ANNALS
OF
DISCRETE
MATHEMATICS

42

Combinatorial Designs

A. HARTMAN

NORTH-HOLLAND

COMBINATORIAL DESIGNS

ANNALS OF DISCRETE MATHEMATICS 42

NORTH-HOLLAND – AMSTERDAM • NEW YORK • OXFORD • TOKYO

COMBINATORIAL DESIGNS— A TRIBUTE TO HAIM HANANI

A. HARTMAN
IBM Israel—Science and Technology
Technion City, Haifa 32000
Israel

1989

NORTH-HOLLAND – AMSTERDAM • NEW YORK • OXFORD • TOKYO

ELSEVIER SCIENCE PUBLISHERS B.V.
Sara Burgerhartstraat 25
P.O. Box 211, 1000 AE Amsterdam, The Netherlands

Distributors for the United States and Canada:

ELSEVIER SCIENCE PUBLISHING COMPANY, INC.
655, Avenue of the Americas
New York, N.Y. 10010, U.S.A.

Reprinted from the Journal *Discrete Mathematics*, Volume 77, Nos. 1–3, 1989.

ISBN: 0 444 88115 8

PRINTED IN NORTHERN IRELAND

SPECIAL VOLUME

COMBINATORIAL DESIGNS – A TRIBUTE TO HAIM HANANI

Guest Editor: A. HARTMAN

CONTENTS

This Page Intentionally Left Blank

Prof. Haim Hanani

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 1–4
North-Holland

COMBINATORIAL DESIGNS - A TRIBUTE TO HAIM HANANI

PREFACE

This volume is dedicated to a mathematician who laid the ground work for the modern study of combinatorial design theory. Haim Hanani pioneered the techniques for constructing designs and the theory of pairwise balanced designs, leading directly to Wilson's Existence Theorems. He also has lead the way in the study of resolvable designs, covering and packing problems, latin squares, 3-designs, and other combinatorial configurations. All this is made more remarkable by the fact that Haim's first paper in design theory (the existence theorem for Steiner quadruple systems) appeared only in 1960. His encylopaedic papers are widely referenced, and his genius for construction is known and respected throughout the design theory community.

Haim Hanani was born in Poland in 1912; he studied mathematics in Vienna and Warsaw from 1929–34, graduating with an M.A. from the University of Warsaw. In 1935 he emigrated to Israel and was awarded the Hebrew University's first Ph.D. in Mathematics in 1938. His dissertation was on the four colour problem. While a student he joined the National Military Organization (IZL), an underground force fighting for the establishment of a Jewish state in the land of Israel. He was imprisoned by the British authorities in 1944 and exiled to Eritrea, and then to Kenya, returning to Israel only in 1949 after Israel's independence. In 1955 he was appointed to the faculty of the Technion in Haifa. During the period from 1969–73 he served as the first rector of Ben Gurion University in Beersheba, and in 1979 he was awarded an honorary doctorate for his work in founding the university. In 1980 he was appointed Professor Emeritus at the Technion. Throughout his career he has held numerous administrative posts in the Technion and in professional and government agencies. He is on the editorial board of *Discrete Mathematics, Journal of Combinatorial Theory* and the *European Journal of Combinatorics.*

I would like to take this opportunity to express my gratitude to Professor Hanani for his contributions to mathematics, and to wish him a long, fruitful and healthy life on his seventy-fifth birthday. This volume of research and survey papers is a fitting tribute to a founding father, from his mathematical sons and daughters.

Alan Hartman
Toronto, Ontario
July, 1988

0012-365X/89/$3.50

ACKNOWLEDGEMENTS

I would like to thank all the people who assisted in the preparation of this volume, particularly the authors and referees of the papers. It is due to the extremely high standard of these people that this volume contains such a wealth of excellent papers. I would like to thank Peter Hammer and the staff at North-Holland for their support of the project.

I would also like to express my thanks to Eric Mendelsohn, and the faculty and staff at the University of Toronto where most of the editorial work was done. Special thanks are due to Karin Smith for her dedicated help in preparing the manuscript.

OBITUARY: SHMUEL SCHREIBER (1920–1988)

It is with great sadness that we note the passing of Shmuel Schreiber. Shmuel's last two papers appear in this volume, and were completed only days before his death. He was born in Romania, arriving in (then) Palestine in 1940. He received his Master's degree from the Hebrew University in 1947. His career was not in academia, so his time for research was limited; nevertheless his papers on Steiner triple systems and finite algebras remain as important works. His presence at combinatorial meetings in Israel was inspiring, his questions and problems always challenging, and his infectious enthusiasm for mathematics was remarkable. He will be greatly missed by the Israeli mathematical community and the combinatorial theorists of the world who had the privilege to know him.

Alan Hartman
Toronto, Ontario
July, 1988

LIST OF PUBLICATIONS by Haim Hanani

1. Über wesentlich unplättbar Kurven im dreidimensionalen Raume, Fundamenta Mathematicae 23 (1934) 135–142.
2. A contribution to the four color problem, thesis for the Ph.D. degree, submitted to the Hebrew University, Jerusalem, 1938 (in Hebrew).
3. A contribution to the four color problem, Am. J. Math. 64 (1942) 36–54.
4. Sur les changements des signes d'une série à termes complexes. Comptes rendus des séances de l'Academie des Sciences 225 (1947) 516–518 (with A. Dvoretzky).
5. On the number of straight lines determined by n points, Riveon Lematematika 5 (1951) 10–11 (in Hebrew, English Summary).
6. On sums of series of complex numbers, Pacific J. Math. 3 (1953) 695–709.
7. On the number of lines and planes determined by d points, Scientific Publications, Technion, I.I.T. Haifa, 6 (1954/5) 58–63.
8. Enumeration of rational numbers, Riveon Lematematika 9 (1955) 23–24 (in Hebrew, English Summary).
9. On the number of monotonic subsequences, Bull. Res. Council Israel 7F (1957/8) 11–13.
10. A generalization of the Banach and Mazur game, Trans Amer. Math. Soc. 94 (1960), 86–102.
11. On quadruple systems, Canad. J. Math. 12 (1960) 145–157.
12. A note on Steiner triple systems, Math. Scandinavica 8 (1960) 154–156.
13. The existence and construction of balanced incomplete block-designs, Annals Math. Statistics 32 (1961) 361–386.
14. Some characterizations of a class of unavoidable compact sets in the game of Banach and Mazur, Pacific J. Math. 11 (1961) 945–959, (with M. Reichbach).
15. On C_l-summability of series, Michigan Math. J. 9 (1962) 1–14 (with P. Erdös).
16. On some tactical configurations, Canad. J. Math. 15 (1963) 702–722.
17. The sphere in the image, Israel J. Math. 1 (1963) 188–195 (with E. Netanyahu and M. Reichaw-Reichbach).
18. On a limit theorem in combinatorial analysis, Publicationes Mathematicae 10 (1963) 10–13 (with P. Erdös).
19. On covering of balanced imcomplete block designs, Canad. J. Math. 16 (1964) 615–625.
20. On the lottery problem, Publications of the Mathematical Institute of the Hungarian Academy of Sciences, 9, series A (1964) 155–158 (with D. Orenstein and V.T. Sós).
21. A balanced incomplete block design, Annals Math. Statistics 36 (1965) 711.
22. Some combinatorial configurations, Trans. N.Y. Acad. Sci., Ser. II, 30 (1968) 421–426.
23. Eigenvalues of infinite matrices, Colloquium Mathematicum 19 (1968) 89–101. (With E. Netanyahu and M. Reichaw).
24. On the number of orthogonal latin squares, J. Combin. Theory 8 (1970) 247–271.
25. On balanced incomplete block designs with large number of elements, Canad. J. Math. 22 (1970) 61–65.
26. Truncated finite planes, Proc. Symposia in Pure Mathematics, A.M.S. 19 (1971) 115–120.
27. On balanced incomplete block designs with blocks having five elements, J. Combin. Theory 12 (1972) 184–201.
28. On resolvable designs, Discrete Math. 3 (1972) 343–357 (with D.K. Ray-Chaudhuri and R.M. Wilson).
29. On resolvable balanced incomplete block designs, J. Combin. Theory 17 (1974) 275–289.
30. On transversal designs, Combinatorics, Proceedings of the NATO Advanced Study Institute (Breukelen, The Netherlands, 1974) 43–53.
31. Balanced incomplete block designs and related designs, Discrete Math. 11 (1975) 255–369.
32. A combinatorial identity, Fibonacci Quarterly 14 (1976) 49–51.
33. Resolvable designs, Colloquio Internazionale sulle Teorie Combinatorie, Atti dei Convegni Lincei, Roma 17 (1976) 249–252.
34. Group divisible designs with block-size four, Discrete Math. 30 (1977) 1–10 (with A.E. Brouwer and A. Schrijver).
35. A class of three-designs, J. Combin. Theory 26 (1979) 1–19.

36. Decomposition of Hypergraphs into Octahedra, Trans. N.Y. Acad. Sci. 319 (1979) 260–264.
37. On three-designs of small order, Discrete Math. 45 (1983) 75–97 (with A. Hartman and E.S. Kramer).
38. On the original Steiner systems, Discrete Math. 51 (1984) 309–310.
39. BIRDs with blocksize 7, this volume.

Discrete Mathematics 77 (1989) 5–20
North-Holland

RESOLVABLE GROUP DIVISIBLE DESIGNS WITH BLOCK SIZE 3

Ahmed M. ASSAF* and Alan HARTMAN
IBM Israel – Haifa Research Group, Technion City, Haifa 32000, Israel

Dedicated to Professor Haim Hanani on the occasion of his 75th birthday.

Let v be a non negative integer, let λ be a positive integer, and let K and M be sets of positive integers. A *group divisible design*, denoted by GD$[K, \lambda, M, v]$, is a triple (X, Γ, β) where X is a set of points, $\Gamma = \{G_1, G_2, \ldots\}$ is a partition of X, and β is a class of subsets of X with the following properties. (Members of Γ are called *groups* and members of β are called *blocks*.)

1. The cardinality of X is v.
2. The cardinality of each group is a member of M.
3. The cardinality of each block is a member of K.
4. Every 2-subset $\{x, y\}$ of X such that x and y belong to distinct groups is contained in precisely λ blocks.
5. Every 2-subset $\{x, y\}$ of X such that x and y belong to the same group is contained in no block.

A group divisible design is *resolvable* if there exists a partition $\Pi = \{P_1, P_2, \ldots\}$ of β such that each part P_i is itself a partition of X. In this paper we investigate the existence of resolvable group divisible designs with $K = \{3\}$, M a singleton set, and all λ. The case where $M = \{1\}$ has been solved by Ray-Chaudhuri and Wilson for $\lambda = 1$, and by Hanani for all $\lambda > 1$. The case where M is a singleton set, and $\lambda = 1$ has recently been investigated by Rees and Stinson. We give some small improvements to Rees and Stinson's results, and give new results for the cases where $\lambda > 1$. We also investigate a class of designs, introduced by Hanani, which we call frame resolvable group divisible designs and prove necessary and sufficient conditions for their existence.

1. Introduction

Let v be a non negative integer, let λ be a positive integer, and let K and M be sets of positive integers. A *group divisible design*, denoted by GD$[K, \lambda, M, v]$, is a triple (X, Γ, β) where X is a set of points, $\Gamma = \{G_1, G_2, \ldots\}$ is a partition of X, and β is a class of subsets of X with the following properties. (Members of Γ are called *groups* and members of β are called *blocks*.)

1. The cardinality of X is v.
2. The cardinality of each group is a member of M.
3. The cardinality of each block is a member of K.

* Department of Algebra, Combinatorics and Analysis, Auburn University, Auburn, Ala. 36849, U.S.A.

4. Every 2-subset $\{x, y\}$ of X such that x and y belong to distinct groups is contained in precisely λ blocks.
5. Every 2-subset $\{x, y\}$ of X such that x and y belong to the same group is contained in no block.

When $M = \{m\}$ or $K = \{k\}$ are singleton sets we shorten the notation for $\mathrm{GD}[K, \lambda, M, v]$ to $\mathrm{GD}[k, \lambda, m, v]$.

A group divisible design is *resolvable* if there exists a partition $\Pi = \{P_1, P_2, \ldots, P_r\}$ of β such that each part P_i is itself a partition of X. The parts P_i are called *parallel classes*, and the partition Π is called a *resolution*. The number r of parallel classes in a resolvable $\mathrm{GD}[k, \lambda, m, v]$ is given by $r = \lambda(v - m)/(k - 1) = \lambda m(u - 1)/(k - 1)$, where u is the number of groups.

Group divisible designs are generalizations of many combinatorial design structures, we give a short list below.

A *pairwise balanced design* $\mathrm{B}(K, \lambda, v)$ is equivalent to a $\mathrm{GD}[K, \lambda, 1, v]$.

A *balanced incomplete block design* $\mathrm{B}(k, \lambda, v)$ is equivalent to a $\mathrm{GD}[k, \lambda, 1, v]$.

A *transversal design* $\mathrm{T}(k, \lambda, m)$ is equivalent to a $\mathrm{GD}[k, \lambda, m, km]$.

The main purpose of this paper is to investigate the existence of resolvable group divisible designs with parameters $\mathrm{GD}[3, \lambda, m, v]$. Note that the existence of group divisible designs with block size 3 has been settled by Hanani [7] who proved the following.

Theorem 1.1. *A group divisible design* $\mathrm{GD}[3, \lambda, m, v]$ *exists if and only if*

$$v \equiv 0 \pmod{m},\ v \neq 2m,$$

$$\lambda(v - m) \equiv 0 \pmod{2},\ \textit{and}$$

$$\lambda v(v - m) \equiv 0 \pmod{6}.$$

For such a design to be resolvable an obvious additional necessary condition on the parameters is that

$$v \equiv 0 \pmod{3}.$$

We shall show that in the majority of cases the above conditions are also sufficient for the existence of resolvable designs $\mathrm{GD}[3, \lambda, m, v]$. However, we do leave some cases where the necessary conditions are satisfied but the existence of the designs is undecided.

We begin by surveying the known existence theorems for resolvable group divisible designs with block size 3. The most celebrated existence problem for resolvable designs was first posed by Kirkman [9] in 1847, and is known as Kirkman's schoolgirl problem. This was solved by Ray-Chaudhuri and Wilson [11] in 1974 when they proved the following.

Theorem 1.2. *A resolvable group divisible design* GD[3, 1, 1, v] *exists if and only if* $v \equiv 3 \pmod 6$.

Another well studied problem for resolvable group divisible designs is the existence of resolvable transversal designs. A resolvable transversal design T(3, 1, m) or resolvable GD[3, 1, m, $3m$] is equivalent to a pair of mutually orthogonal Latin squares of side m, and the following existence theorem was proved by Bose, Parker and Shrikhande [2, 3] in 1960.

Theorem 1.3. *A resolvable group divisible design* GD[3, 1, m, $3m$] *exists if and only if* $m \notin \{2, 6\}$.

Further progress was made on the case $m = 1$ by Hanani [6] when he proved.

Theorem 1.4. *A resolvable group divisible design* GD[3, 2, 1, v] *exists if and only if* $v \equiv 0 \pmod 3$, *and* $v \neq 6$.

An easy consequence of Theorems 1.2 and 1.4 is:

Theorem 1.5. *A resolvable group divisible design* GD[3, λ, 1, v] *exists if and only if*

$$\lambda \equiv 1 \pmod 2, \text{ and } v \equiv 3 \pmod 6, \text{ or}$$
$$\lambda \equiv 0 \pmod 2, \text{ and } v \equiv 0 \pmod 3, \text{ and } v \neq 6, \text{ or}$$
$$\lambda \equiv 0 \pmod 4, \text{ and } v = 6.$$

Proof. Theorems 1.2 and 1.4 cover the cases $\lambda = 1$ and $\lambda = 2$. For $\lambda > 2$ and $v \neq 6$ the designs are constructed by taking copies of the blocks and resolution classes of the designs with $\lambda \leq 2$. For $v = 6$ and $\lambda = 4j$ take j copies of all 3-subsets of a 6-set as blocks, and the resolution classes consist of a block and its complement.

Now let us assume that there exists a resolvable GD[3, $4j + 2$, 1, 6]. We can assume that $X = \{0, 1, 2, 3, 4, 5\}$. Every resolution class contains two blocks, and these two blocks contain either 0 or 4 pairs $\{x, y\}$ such that $x \not\equiv y \pmod 2$ (according to whether the resolution class is $\{\{0, 2, 4\}, \{1, 3, 5\}\}$ or not). There are a total of 9 such pairs, and thus $9(4j + 2)$ is a multiple of 4, a contradiction. □

A resolvable group divisible design GD[3, 1, 2, v] with $m = 2$ and $\lambda = 1$ has been referred to in the literature as a *nearly Kirkman triple system*, and the following existence theorem is mainly due to Baker and Wilson [1] with some final small cases solved in the papers of Brouwer [4] and Rees and Stinson [10]. (Note that a resolvable GD[3, 1, 2, 6] is equivalent to a pair of orthogonal Latin squares of side 2, which do not exist by Theorem 1.3.)

Theorem 1.6. *A resolvable group divisible design* GD[3, 1, 2, v] *exists if and only if* $v \equiv 0 \pmod 6$, *and* $v \geq 18$.

Rees and Stinson also proved the following theorem, which is the state of the art for resolvable group divisible designs with $k = 3$, $\lambda = 1$, and arbitrary m.

Theorem 1.7. *A resolvable group divisible design* GD[3, 1, m, v] *exists if and only if*

$$v \equiv 0 \pmod m,\ v \neq 2m,$$

$$v - m \equiv 0 \pmod 2,$$

$$v \equiv 0 \pmod 3 \text{ and,}$$

$$(m, v) \notin \{(2, 6), (2, 12), (6, 18)\}$$

with the possible exceptions of

$$(m, v) \in \{(6, 66), (18, 198)\}$$

$$m \equiv 6 \text{ or } 30 \pmod{36}, \text{ and } v = 14m$$

$$m \equiv 2 \text{ or } 10 \pmod{12}, \text{ and } v = 6m.$$

In this paper we improve on Rees and Stinson's result by removing the first two classes of exceptions, and some of the third class. We also prove a result similar to Theorem 1.7 with $\lambda > 1$. We denote the set of primes less than or equal to p by D_p. Our main result is the following.

Theorem 1.8. *A resolvable group divisible design $GD[3, \lambda, m, um]$ exists if and only if*

$$u \neq 2,$$

$$\lambda m(u-1) \equiv 0 \pmod 2,$$

$$um \equiv 0 \pmod 3 \text{ and,}$$

$$(\lambda, m, u) \notin \{(2j+1, 2, 3), (1, 2, 6), (1, 6, 3), (4j+2, 1, 6) : j = 0, 1, 2, \ldots\}$$

with the possible exceptions of the cases where $u = 6$ *and* $\lambda \not\equiv 0 \pmod 4$. *Moreover, there exist resolvable* GD[3, λ, m, $6m$] *for all odd* λ *and even* m *such that* $m/2$ *is divisible by a member of* D_7; *and there exist resolvable* GD[3, λ, m, $6m$] *for all* $\lambda \equiv 2 \pmod 4$ *and all* m *divisible by a member of* D_{19}, *except possibly* $m \in \{22, 26, 34, 38\}$.

A further configuration investigated in this paper has appeared in Hanani's paper [6] in a disguised form, and explicitly in Stinson's paper [12]. We have chosen to use the terminology *frame resolvable group divisible design* as a compromise between the terms currently in use. A group divisible design

(X, Γ, β) is said to be *frame resolvable* if there exists a partition $\Pi = \{P_1, P_2, \ldots, P_f\}$ of β such that each P_i is itself a partition of $X \setminus G_j$ for some $G_j \in \Gamma$. The parts P_i are called *frame parallel classes*, and the partition Π is called a *frame resolution*.

Two obvious necessary conditions for the existence of a frame resolvable GD$[k, \lambda, m, v]$ are that $v \neq km$, and $v - m \equiv 0 \pmod{k}$. The number of frame parallel classes, f, is given by

$$f = \frac{\lambda v(v-m)}{k(k-1)} \div \frac{v-m}{k} = \frac{\lambda v}{k-1},$$

and hence an additional necessary condition is that $\lambda v \equiv 0 \pmod{k-1}$. Note that the number of frame parallel classes which partition $X \setminus G_i$ for some fixed group G_i is given by $f - r = \lambda m/(k-1)$ and we shall sometimes use this fact to index the frame resolution as $\Pi = \{P_{ij} : i = 1, 2, \ldots, u; j = 1, 2, \ldots, \lambda m/(k-1)\}$ where u is the number of groups and P_{ij} is a partition of $X \setminus G_i$ for all j.

In the case $k = 3$ Stinson [12] has shown that the necessary conditions stated above are also sufficient when $\lambda = 1$, and his result is stated below.

Theorem 1.9. *A frame resolvable group divisible design* GD$[3, 1, m, v]$ *exists if and only if*

$$v \equiv 0 \pmod{m},\ v \neq 2m, 3m$$
$$v - m \equiv 0 \pmod{3}, \text{ and}$$
$$m \equiv 0 \pmod{2}.$$

Hanani [6] has also shown that the necessary conditions are sufficient when $\lambda = 2$ and $m = 1$. His result is:

Theorem 1.10. *A frame resolvable group divisible design* GD$[3, 2, 1, v]$ *exists if and only if* $v \equiv 1 \pmod{3}$.

In the same paper Hanani also constructs frame resolvable GD$[3, 2, m, v]$ designs with $m \in \{3, 12, 24\}$ and infinitely many values of v. In this paper we extend the above results to prove:

Theorem 1.11. *A frame resolvable group divisible design* GD$[3, \lambda, m, v]$ *exists if and only if*

$$v \equiv 0 \pmod{m},\ v \neq 2m, 3m,$$
$$\lambda(v - m) \equiv 0 \pmod{2},$$
$$v - m \equiv 0 \pmod{3}, \text{ and}$$
$$\lambda v \equiv 0 \pmod{2}.$$

In Section 2 we describe the major constructions necessary to prove Theorems 1.8 and 1.11. In Section 3 we prove these results, and the appendix contains the constructions of resolvable and frame resolvable designs with small parameters needed in the proofs.

2. Recursive constructions

In this section we show how to construct both resolvable and frame resolvable group divisible designs using the existence of designs with smaller values of the various parameters. Throughout the sequel we shall denote the set $\{0, 1, \ldots, n-1\}$ by I_n. The first lemma shows how to increase λ without altering any of the other parameters.

Lemma 2.1 (Addition Lemma). *If there exist a (frame) resolvable* GD$[K, \lambda, m, v]$ *and a (frame) resolvable* GD$[K, \mu, m, v]$ *then there exists a (frame) resolvable* GD$[K, \lambda+\mu, m, v]$.

Proof. Take the union of the two postulated designs. □

In most cases this lemma reduces our problem to consideration of only two cases namely $\lambda = 1$ or 2. The next theorem is multiplicative on the number of points and the index λ. In general we will be using the theorem with $k_1 = k$ thus keeping the block size constant, but we shall also have occasion to set $k_1 \neq k$.

Theorem 2.2 (Multiplication Theorem). *If there exist a (frame) resolvable* GD$[k_1, \lambda, m, v]$ *and a resolvable* GD$[k, \mu, g, k_1 g]$ *then there exists a (frame) resolvable* GD$[k, \lambda\mu, mg, vg]$.

Proof. Let (X, Γ, β) be a (frame) resolvable GD$[k_1, \lambda, m, v]$ with (frame) resolution $\Pi = \{\pi_1, \pi_2, \ldots\}$. We construct a (frame) resolvable GD$[k, \lambda\mu, mg, vg]$ as follows. Let $X' = X \times I_g$. Let $\Gamma' = \{G \times I_g : G \in \Gamma\}$. For each block $B \in \beta$ we construct a resolvable GD$[k, \mu, g, k_1 g]$ with point set $B \times I_g$, groups $\{x\} \times I_g$ for each $x \in B$, block set $\beta(B)$, and resolution $\Pi(B) = \{P(B, j) : j = 1, 2, \ldots\}$. Now let $\beta' = \bigcup_{B \in \beta} \beta(B)$, and construct (frame) parallel classes $P'(i, j) = \bigcup_{B \in \pi_i} P(B, j)$. □

To apply this theorem we generally use Theorem 1.3 which guarantees the existence of resolvable GD$[3, 1, g, 3g]$ for all $g \neq 2, 6$. Thus our problem usually reduces to consideration of the cases where $m = 1, 2, 3$, and 6. The next theorem shows that the set $U = \{u :$ there exists a frame resolvable GD$[k, \lambda, m, mu]\}$ is PBD-closed.

Theorem 2.3 (PBD-closure Theorem). *If there exist a pairwise balanced design* B$[K, 1, v]$ *and for each $u \in K$ there exists a frame resolvable* GD$[k, \lambda, m, mu]$ *then there exists a frame resolvable* GD$[k, \lambda, m, mv]$.

Proof. Let (X, β) be a B$[K, 1, v]$. We construct a frame resolvable GD$[k, \lambda, m, mv]$ as follows. Let $X' = X \times I_m$. Let $\Gamma' = \{\{x\} \times I_m : x \in X\}$. For each block $B \in \beta$ of cardinality u we construct a frame resolvable GD$[k, \lambda, m, mu]$ with point set $B \times I_m$, groups $\{x\} \times I_m$ for each $x \in B$, and block set $\beta(B)$. Its frame resolution $\Pi(B) = \{P(B, x, j) : x \in B, j = 1, 2, \ldots, \lambda m/(k-1)\}$, is indexed so that $P(B, x, j)$ is a partition of $(B \setminus \{x\}) \times I_m$ for all j. Now let $\beta' = \bigcup_{B \in \beta} \beta(B)$, and construct frame parallel classes $P'(x, j) = \bigcup_{x \in B \in \beta} P(B, x, j)$, for all $x \in X$ and all $j = 1, 2, \ldots, \lambda m/(k-1)$. $\square$

With k, λ, and m fixed, this theorem reduces our existence problem for frame resolvable GD$[k, \lambda, m, mu]$ to finitely many values of u, using the known finite generating sets for U. An example of the kind of result we shall use is the following theorem of Drake and Larson [5].

Theorem 2.4. *For all* $v \leq 4$ *there exists a* B$(K, 1, v)$ *where* $K = \{4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 18, 19, 23\}$.

The next theorem is similar to the PBD-closure theorem and it illustrates the interplay between frame resolvable and resolvable group divisible designs.

Theorem 2.5 (FR + 1-closure Theorem). *If there exist a group divisible design* GD$[K, 1, M, v]$ *and for each $g \in M$ there exists a resolvable* GD$[k, \lambda, m, m(g+1)]$ *and for each $u \in K$ there exists a frame resolvable* GD$[k, \lambda, m, mu]$ *then there exists a resolvable* GD$[k, \lambda, m, m(v+1)]$.

Proof. Let (X, Γ, β) be a GD$[K, 1, M, v]$. We construct a resolvable GD$[k, \lambda, m, m(v+1)]$ as follows. Let $X' = (X \cup \{\infty\}) \times I_m$. Let $\Gamma' = \{\{x\} \times I_m : x \in X \cup \{\infty\}\}$. For each group $G \in \Gamma$ of cardinality g we construct a resolvable GD$[k, \lambda, m, m(g+1)]$ with point set $(G \cup \{\infty\}) \times I_m$, groups $\{x\} \times I_m$ for each $x \in G \cup \{\infty\}$, and block set $\beta(G)$. Its resolution $\Pi(G) = \{\pi(G, x, j) : x \in G, j = 1, 2, \ldots, \lambda m/(k-1)\}$, is indexed arbitrarily by the ordered pairs (x, j). This is possible since the number of parallel classes is $\lambda mg/(k-1)$. For each block $B \in \beta$ of cardinality u we construct a frame resolvable GD$[k, \lambda, m, mu]$ with point set $B \times I_m$, groups $\{x\} \times I_m$ for each $x \in B$, and block set $\beta(B)$. Its frame resolution $\Pi(B) = \{P(B, x, j) : x \in B, j = 1, 2, \ldots, \lambda m/(k-1)\}$, is indexed so that $P(B, x, j)$ is a partition of $(B \setminus \{x\}) \times I_m$ for all j. Now let $\beta' = \bigcup_{G \in \Gamma} \beta(G) \cup \bigcup_{B \in \beta} \beta(B)$, and construct the following parallel classes. Let x be a member of X and let G be the unique group in Γ which contains x, now for each $j = 1, 2, \ldots, \lambda m/(k-1)$ define

$$P'(x, j) = \pi(G, x, j) \cup \bigcup_{x \in B \in \beta} P(B, x, j). \quad \square$$

This theorem, together with our results on the existence of frame resolvable designs and standard results on group divisible designs, reduces the existence problem for resolvable group divisible designs to a finite number of values of v.

Note that none of the results in this section are completely new, since variants of these results have appeared in the papers of Hanani, Wilson and others. We have restated and proved the results to make the paper self contained and to have the results in the most convenient form for our purposes.

3. Proofs of the main theorems

We begin this section with a proof that the necessary conditions for existence of frame resolvable group divisible designs with block size 3 are sufficient. We restate the theorem here for the reader's convenience.

Theorem 1.11. *A frame resolvable group divisible design* GD$[3, \lambda, m, v]$ *exists if and only if*

$$v \equiv 0 \pmod m,\ v \neq 2m, 3m,$$
$$\lambda(v-m) \equiv 0 \pmod 2,$$
$$v - m \equiv 0 \pmod 3, \textit{ and}$$
$$\lambda v \equiv 0 \pmod 2.$$

Proof. Let $v = um$. We consider three cases.

Case 1. $\lambda \equiv 1 \pmod 2$.

In this case the necessary conditions reduce to $u \neq 2, 3$, $m \equiv 0 \pmod 2$, and $m(u-1) \equiv 0 \pmod 3$. The existence of these designs follows from Stinson's theorem [12] (Theorem 1.9) and the Addition Lemma.

Case 2. $\lambda \equiv 0 \pmod 2$ and $m \not\equiv 0 \pmod 3$.

In this case the necessary conditions reduce to $u \equiv 1 \pmod 3$. The existence of these designs follows from Stinson's theorem [12] (Theorem 1.9) and the Addition Lemma when m is even. When m is odd existence follows from Hanani's theorem [6] (Theorem 1.10), the Addition Lemma and the Multiplication Theorem, since, by Theorem 1.3, there exist resolvable GD$[3, 1, m, 3m]$ for all odd m.

Case 3. $\lambda \equiv 0 \pmod 2$ and $m \equiv 0 \pmod 3$.

In this case the necessary conditions reduce to $u \neq 2, 3$. When m is even the result follows from Stinson's theorem and the Addition Lemma. When m is odd, by the Addition Lemma and the Multiplication Theorem, it is sufficient to establish the result in the case where $\lambda = 2$ and $m = 3$. When $u \equiv 1 \pmod 3$ and in particular when $u \in \{4, 7, 10, 19\}$ the result follows from Hanani's theorem and the Multiplication Theorem. When $u \in \{5, 8, 9, 11, 12, 15, 23\}$ Hanani [6] has constructed frame resolvable GD$[3, 2, 3, 3u]$ designs. In Hanani's paper the designs are given by developing the frame parallel classes denoted $M_{u,3}(0;0)$ modulo $(u, 3)$. When $u \in \{6, 14, 18\}$ we construct frame resolvable GD[3, 2, 3, $3u$] designs in the Appendix. For all other values of u the result then follows from Drake and Larson's theorem [5] (Theorem 2.4) and the PBD-closure theorem. □

We turn now to resolvable group divisible designs, and we begin by giving a small improvement to Rees and Stinson's theorem [10] (Theorem 1.7).

Theorem 3.1. *There exist resolvable* GD[3, 1, m, $11m$] *and resolvable* GD[3, 1, m, $14m$] *for all* $m \equiv 0 \pmod 6$. *Furthermore, there exist resolvable* GD[3, 1, m, $6m$] *for all* $m \equiv 0 \pmod{10}$, *and for all* $m \equiv 0 \pmod{14}$.

Proof. In the Appendix we construct resolvable designs GD[3, 1, 6, 66], GD[3, 1, 6, 84], GD[3, 1, 10, 60], and GD[3, 1, 14, 84]. Rees and Stinson have constructed resolvable designs GD[3, 1, 12, 132], GD[3, 1, 12, 168], GD[3, 1, 20, 120], and GD[3, 1, 28, 168]. The result then follows from the Multiplication Theorem and the existence of a pair of orthogonal Latin squares of side $n \neq 2, 6$ (Theorem 1.3). □

This result, together with Rees and Stinson's theorem proves our main result, Theorem 1.8, for the case $\lambda = 1$. We now concentrate on $\lambda = 2$. In order to establish our result in this case we use the following theorem due to Hanani, Ray-Chaudhuri and Wilson [8] concerning the existence of resolvable balanced incomplete block designs with block size 4.

Theorem 3.2. *A resolvable* GD[4, 1, 1, v] *exists if and only if* $v \equiv 4 \pmod{12}$.

We also use the following result concerning the existence of three mutually orthogonal Latin squares of side g. This result is due to a combination of authors, see [14] and [13] for a proof.

Theorem 3.3. *A* GD[5, 1, g, $5g$] *exists for all* $g \geq 4$, $g \neq 6$, *with the possible exception of* $g = 10$.

We are now able to state and prove the following.

Theorem 3.4. *A resolvable* GD[3, 2, m, mu] *exists if and only if* $mu \equiv 0 \pmod 3$, $u \neq 2$, *and* $(m, u) \neq (1, 6)$, *with the possible exception of the cases where* $u = 6$. *Moreover, there exists a resolvable* GD[3, 2, m, $6m$] *for all* m *divisible by a member of* D_{19}, *except possibly* $m \in \{22, 26, 34, 38\}$.

Proof. Necessity of these conditions was established in the introduction. To prove sufficiency we consider four cases.

Case 1. $u \equiv 0 \pmod 3$, and $u \neq 6$.

When $m = 1$ this is Hanani's theorem (Theorem 1.4). When $m = 2$ and $u = 3$ we give a direct construction in the Appendix. When $m = 2$ and $u \geq 9$ the result follows from the existence of nearly Kirkman triple systems (Theorem 1.6) and the Addition Lemma. All other values of m then follow from the Multiplication Theorem and the existence of mutually orthogonal Latin squares (Theorem 1.3).

Case 2. $m = 3$ and $u \neq 2$.

When u is odd, we can construct a resolvable GD[3, 1, 3, $3u$] from a Kirkman triple system (which exists by Theorem 1.2) simply by considering one of the parallel classes as the set of groups. Using the Addition Lemma gives a resolvable GD[3, 2, 3, $3u$]. When $u \equiv 0 \pmod 3$, and $u \neq 6$, then the construction is given in Case 1. When $u \in \{4, 6, 8, 10, 14, 22\}$ we give constructions in the Appendix. When $u \equiv 4 \pmod{12}$, we can use the Multiplication Theorem with $k_1 = 4$ and $k = 3$, since resolvable GD[4, 1, 1, u] exist by Theorem 3.2 and we have constructed a resolvable GD[3, 2, 3, 12] in the Appendix.

From the above construction, we have the existence of resolvable GD[3, 2, 3, $3u$] for all $u \leq 30$ with the exceptions of $u = 2, 20, 26$. For $u > 30$ and $u = 20$, or 26 we use induction. Write $u = 4g + n + 1$ where $g \geq 4$, $g \notin \{6, 10\}$, $0 \leq n \leq g$ and $n \neq 1$. By Theorem 3.3 there exists a GD[5, 1, g, $5g$], and deleting $g - n$ points from a single group, and all the blocks containing them yields a GD[{4, 5}, 1, $\{g, n\}$, $4g + n$]. By Theorem 1.11 there exists a frame resolvable GD[3, 2, 3, 12], and a frame resolvable GD[3, 2, 3, 15]. Since $u > g + 1 \geq 5$ and $g + 1 \geq n + 1 \neq 2$ the induction hypothesis gives us the existence of a resolvable GD[3, 2, 3, $3(g + 1)$], and a resolvable GD[3, 2, 3, $3(n + 1)$]. We now apply the FR + 1 Closure Theorem to construct a GD[3, 2, 3, $3u$].

Case 3. $m \equiv 0 \pmod 3$, and $u \neq 2$.

Case 2 handles the case $m = 3$. The cases $m = 6$, 18 are covered by Rees and Stinson's theorem (Theorem 1.7), Theorem 3.1, and the Addition Lemma. All other cases are covered by applying the Multiplication Theorem to the designs constructed in Case 2 and the existence theorem for mutually orthogonal Latin squares (Theorem 1.3).

Case 4. $u = 6$, m is divisible by a member of D_{19}, and $m \notin \{22, 26, 34, 38\}$.

In the Appendix we construct resolvable GD[3, 2, m, $6m$] for all $m \in D_{19}$. The existence of a resolvable GD[3, 2, $6m$, $36m$] follows from Rees and Stinson's theorem. For $m \in D_7$ the existence of a resolvable GD[3, 2, $2m$, $12m$] follows from Rees and Stinson's theorem and Theorem 3.1. The remaining cases follow from the Multiplication Theorem. □

We are now ready to prove our main result which is restated below for the reader's convenience.

Theorem 1.8. *A resolvable group divisible design* GD[3, λ, m, um] *exists if and* *only if*

$$u \neq 2$$
$$\lambda m(u-1) \equiv 0 \pmod 2,$$
$$um \equiv 0 \pmod 3 \textit{ and,}$$
$$(\lambda, m, u) \notin \{(2j+1, 2, 3), (1, 2, 6), (1, 6, 3), (4j+2, 1, 6) : j = 0, 1, 2, \ldots\}$$

with the possible exceptions of the cases where $u = 6$ *and* $\lambda \not\equiv 0 \pmod 4$. *Moreover there exist resolvable* GD[3, λ, m, $6m$] *for all odd* λ *and all even* m *such that* $m/2$ *is divisible by a member of* D_7, *and there exist resolvable* GD[3, λ, m, $6m$] *for all* $\lambda \equiv 2 \pmod 4$ *and all* m *divisible by a member of* D_{19}, *except possibly* $m \in \{22, 26, 34, 38\}$.

Proof. The theorem is true for $\lambda \leqslant 2$ by Rees and Stinson's theorem, Theorem 3.1 and Theorem 3.4. For even values of λ we use the Addition Lemma. For odd values of λ, using the Addition Lemma, it is sufficient to construct a resolvable GD[3, 3, 2, 12] and a resolvable GD[3, 3, 6, 18]. This is done in the Appendix.

It remains to show the non-existence oa a resolvable GD[3, $2j+1$, 2, 6] for any j. Assume that such a design exists with groups $\{0, 1\}$, $\{2, 3\}$, $\{4, 5\}$. There are four possible resolution classes $P_1 = \{\{0, 2, 4\}, \{1, 3, 5\}\}$, $P_2 = \{\{0, 2, 5\}, \{1, 3, 4\}\}$, $P_3 = \{\{0, 3, 4\}, \{1, 2, 5\}\}$, $P_4 = \{\{0, 3, 5\}, \{1, 2, 4\}\}$. Let P_i occur p_i times in the design. Counting occurrences of the pair $\{0, 2\}$ yields $p_1 + p_2 = 2j + 1$, and hence $p_1 \neq p_2$. Similarly considering the pairs $\{0, 4\}$ and $\{3, 4\}$ yields $p_1 + p_3 = 2j + 1$, and $p_2 + p_3 = 2j + 1$, hence $p_1 = p_2$, a contradiction. $\square$

Note added in proof

The proper reference for Theorem 2.4 is A.E. Brouwer, H. Hanani and A. Schrijver, Group divisible designs with block size four, Discrete Math. 30 (1977) 1–10.

References

[1] R.D. Baker and R.M. Wilson, Nearly Kirkman triple systems, Utilitas Math. 11 (1977) 289–296.
[2] R.C. Bose, E.T. Parker and S. Shrikhande, Further results on the construction of mutually orthogonal Latin squares and the falsity of the Euler's conjecture, Can. J. Math. 12 (1960) 189–203.
[3] R.C. Bose and S. Shrikhande, On the construction of sets of mutually orthogonal Latin squares and falsity of a conjecture of Euler, Trans. Amer. Math. Soc. 95 (1960) 191–200.
[4] A.E. Brower, Two nearly Kirkman triple systems, Utilitas Math. 13 (1978) 311–314.
[5] D.A. Drake and J. Larson, Pairwise balanced designs whose line sizes do not divide six, J. Combin. Theory (A) 34 (1983) 266–300.

[6] H. Hanani, On resolvable balanced incomplete block designs, J. Combin. Theory (A) 17 (1974) 275–289.
[7] H. Hanani, Balanced incomplete block designs and related designs, Discrete Math. 11 (1975) 255–369.
[8] H. Hanani, D.K. Ray-Chaudhuri and R.M. Wilson, On resolvable designs, Discrete Math. 3 (1972) 75–97.
[9] T.P. Kirkman, On a problem in combinations, Cambridge and Dublin Math. J. 2 (1847) 191–204.
[10] R. Rees and D.R. Stinson, On resolvable group divisible designs with block size 3, Ars Combinatoria 23 (1987) 107–120.
[11] D.K. Ray-Chaudhuri and R.M. Wilson, Solution of Kirkman's schoolgirl problem, Combinatorics, Proc. Sympos. Pure Math. 19 (1971) 187–203.
[12] D.R. Stinson, Frames for Kirkman triple systems, Discrete Math. 62 (1987) 289–300.
[13] D.T. Todorov, Three mutually orthogonal Latin squares of order 14, Ars Combinatoria 20 (1985) 45–47.
[14] W.D. Wallis, Three orthogonal Latin squares, Congressus Numerantium 42 (1984) 69–86.

Appendix

A frame resolvable GD[3, 2, 3, 18].

$X = Z_{15} \cup \{\infty_0, \infty_1, \infty_2\}$.

$\Gamma = \{\{i, i+5, i+10\}, \{\infty_0, \infty_1, \infty_2\} : i = 0, 1, \ldots, 4\}$.

Frame parallel classes

$\{[4, 7, 8]\ [6, 12, 3]\ [9, 11, \infty_0]\ [14, 1, \infty_1]\ [13, 2, \infty_2]\}$ (mod 15),

$\{[3j+k, 3j+k+7, 3j+k+14]\quad j = 0, 1, \ldots, 4\}\quad k = 0, 1, 2.$

A frame resolvable GD[3, 2, 3, 42].

$X = Z_{39} \cup \{\infty_0, \infty_1, \infty_2\}$.

$\Gamma = \{\{i, i+13, i+26\}, \{\infty_0, \infty_1, \infty_2\} : i = 0, 1, \ldots, 12\}$.

Frame parallel classes

$\{[2, 8, 14]\ [4, 11, 15]\ [9, 17, 19]\ [16, 25, 30]\ [29, 7, 12]\ [10, 28, 31]\ [38, 23, 27]$
$[34, 20, 22]\ [3, 32, 35]\ [6, 36, 37]\ [18, 33, \infty_0]\ [5, 21, \infty_1]\ [1, 24, \infty_2]\}$ (mod 39),

$\{[3j+k, 3j+k+19, 3j+k+38]\quad j = 0, 1, \ldots, 12\}\quad k = 0, 1, 2.$

A frame resolvable GD[3, 2, 3, 54].

$X = Z_{51} \cup \{\infty_0, \infty_1, \infty_2\}$.

$\Gamma = \{\{i, i+17, i+34\}, \{\infty_0, \infty_1, \infty_2\} : i = 0, 1, \ldots, 16\}$.

Frame parallel classes

$\{[2, 10, 18]\ [4, 13, 19]\ [1, 11, 15]\ [3, 14, 16]\ [8, 20, 26]\ [22, 41, 42]\ [27, 49, 5]$
$[7, 30, 35]\ [48, 21, 24]\ [50, 29, 32]\ [12, 43, 47]\ [6, 38, 45]\ [37, 23, 28]\ [44, 31, 33]$
$[39, 9, \infty_0]\ [40, 25, \infty_1]\ [46, 36, \infty_2]\}$ (mod 51), $\{[3j+k, 3j+k+25, 3j+k+50]\quad j = 0, 1, \ldots, 16\}\quad k = 0, 1, 2.$

A resolvable GD[3, 1, 6, 66].

$X = Z_{60} \cup \{\infty_0, \infty_1, \ldots, \infty_5\}$.

$\Gamma = \{\{i + 10j : j = 0, 1, \ldots, 5\}, \{\infty_0, \infty_1, \ldots, \infty_5\} : i = 0, 1, \ldots, 9\}$.

Parallel classes are formed from the orbit of the following base parallel class under the action of the permutation which fixes $\infty_0, \infty_1, \ldots, \infty_5$ and sends $j \to j+2 \pmod{60}$ for all j in Z_{60}.

{[0, 2, 16] [4, 10, 32] [1, 3, 29] [5, 9, 27] [7, 13, 56] [11, 19, 14] [23, 35, 28]
[25, 39, 52] [37, 53, 44] [57, 21, 8] [42, 46, 45] [12, 48, 31] [50, 38, 15] [22, 30, 51]
[18, 36, 59] [40, 6, 41] [34, 49, ∞_0] [20, 47, ∞_1] [24, 55, ∞_2] [54, 33, ∞_3] [58, 43, ∞_4]
[26, 17, ∞_5]}

A resolvable GD[3, 1, 6, 84].

$X = Z_{78} \cup \{\infty_0, \infty_1, \ldots, \infty_5\}$.

$\Gamma = \{\{i + 13j : j = 0, 1, \ldots, 5\}, \{\infty_0, \infty_1, \ldots, \infty_5\} : i = 0, 1, \ldots, 12\}$.

Parallel classes are formed from the orbit of the following base parallel class under the action of the permutation which fixes $\infty_0, \infty_1, \ldots, \infty_5$ and sends $j \to j+2 \pmod{78}$ for all j in Z_{78}.

{[0, 19, 38] [2, 23, 44] [4, 5, 6] [1, 3, 39] [8, 32, 36] [7, 31, 35] [12, 34, 42] [11, 33, 41]
[20, 40, 52] [67, 9, 21] [70, 26, 29] [25, 59, 62] [48, 58, 63] [61, 71, 76] [54, 68, 77]
[51, 65, 74] [30, 46, 57] [75, 13, 24] [10, 28, 45] [37, 55, 72] [18, 43, 49] [69, 16, 22]
[64, 15, ∞_0] [27, 56, ∞_1] [14, 47, ∞_2] [17, 50, ∞_3] [66, 73, ∞_4], [53, 60, ∞_5]}

A resolvable GD[3, 1, 10, 60].

$X = Z_{50} \cup \{\infty_0, \infty_1, \ldots, \infty_9\}$.

$\Gamma = \{\{i + 5j : j = 0, 1, \ldots, 9\}, \{\infty_0, \infty_1, \ldots, \infty_9\} : i = 0, 1, \ldots, 4\}$.

Parallel classes are formed from the orbit of the following base parallel class under the action of the permutation which fixes $\infty_0, \infty_1, \ldots, \infty_9$ and sends $j \to j+2 \pmod{50}$ for all j in Z_{50}.

{[0, 4, 16] [1, 5, 17] [6, 8, 30] [7, 9, 31] [12, 18, 26] [19, 22, 25] [13, 14, 21]
[27, 40, 41] [29, 36, 47] [28, 37, 46] [33, 44, ∞_0] [48, 11, ∞_1] [32, 49, ∞_2] [35, 2, ∞_3]
[34, 3, ∞_4] [23, 42, ∞_5] [24, 45, ∞_6] [39, 10, ∞_7] [20, 43, ∞_8] [15, 38, ∞_9]}

A resolvable GD[3, 1, 14, 84].

$X = Z_{70} \cup \{\infty_0, \infty_1, \ldots, \infty_{13}\}$.

$\Gamma = \{\{i + 5j : j = 0, 1, \ldots, 13\}, \{\infty_0, \infty_1, \ldots, \infty_{13}\} : i = 0, 1, \ldots, 4\}$.

Parallel classes are formed from the orbit of the following base parallel class under the action of the permutation which fixes $\infty_0, \infty_1, \ldots, \infty_{13}$ and sends $j \to j+2 \pmod{70}$ for all j in Z_{70}.

{[0, 2, 14] [1, 3, 15] [4, 8, 30] [5, 9, 31] [10, 18, 42] [11, 19, 43] [6, 22, 40] [13, 16, 29]
[17, 26, 35] [7, 24, 41] [28, 34, 57] [21, 27, 50] [32, 33, 60] [67, 68, 25] [48, 51, ∞_0]
[49, 62, ∞_1] [54, 61, ∞_2] [39, 46, ∞_3] [52, 63, ∞_4] [53, 64, ∞_5] [36, 55, ∞_6] [47, 66, ∞_7]
[44, 65, ∞_8] [37, 58, ∞_9] [38, 69, ∞_{10}] [59, 20, ∞_{11}] [12, 45, ∞_{12}] [23, 56, ∞_{13}]}

A resolvable GD[3, 2, 2, 6].

$X = Z_4 \cup \{\infty_0, \infty_1\}$.

$\Gamma = \{\{i, i+2\}, \{\infty_0, \infty_1\} : i = 0, 1\}$.

Parallel classes

{[0, 1, ∞_0] [2, 3, ∞_1]} (mod 4).

A resolvable GD(3, 2, 3, 12].

$X = Z_3 \times Z_4$

$\Gamma = \{Z_3 \times \{i\} : i \in Z_4\}$

Parallel classes

$\{[(0,0),(1,1),(2,2)] \mod(-,4)\}$ $\{[(0,0),(1,1),(2,3)] \mod(-,4)\}$
$\{[(0,0),(1,2),(2,1)] \mod(-,4)\}$ $\{[(0,0),(1,3),(2,1)] \mod(-,4)\}$
$\{[(0,0),(1,2),(2,3)] \mod(-,4)\}$
$\{[(0,0),(0,2),(0,3)][(1,1),(1,2),(1,3)][(2,0),(2,1),(2,2)][(0,1),(1,0),(2,3)]\}$ mod($-$ 4)

A resolvable GD[3, 2, 3, 18].

$X = Z_{15} \cup \{\infty_0, \infty_1, \infty_2\}$.

$\Gamma = \{\{i, i+5, i+10\}, \{\infty_0, \infty_1, \infty_2\} : i = 0, 1, \ldots, 4\}$.

Parallel classes

$\{[0,1,4]$ $[5,7,14]$ $[9,12,13]$ $[2,11,\infty_0]$ $[3,10,\infty_1]$ $[6,8,\infty_2]\}$ (mod 15).

A resolvable GD[3, 2, 3, 24].

$X = Z_{21} \cup \{\infty_0, \infty_1, \infty_2\}$.

$\Gamma = \{\{i, i+7, i+14\}, \{\infty_0, \infty_1, \infty_2\} : i = 0, 1, \ldots, 6\}$.

Parallel classes

$\{[0,4,5]$ $[2,12,15]$ $[6,8,17]$ $[7,10,16]$ $[13,18,19]$ $[1,14,\infty_0]$ $[3,20,\infty_1]$
$[9,11,\infty_2]\}$ (mod 21).

A resolvable GD[3, 2, 3, 30].

$X = Z_{27} \cup \{\infty_0, \infty_1, \infty_2\}$.

$\Gamma = \{\{i, i+9, i+18\}, \{\infty_0, \infty_1, \infty_2\} : i = 0, 1, \ldots, 8\}$.

Parallel classes

$\{[0,4,6]$ $[1,8,12]$ $[3,11,13]$ $[26,18,21]$ $[23,16,17]$ $[5,19,22]$ $[9,24,25]$
$[10,15,\infty_0]$ $[2,14,\infty_1]$ $[7,20,\infty_2]\}$ (mod 27).

A resolvable GD[3, 2, 3, 42].

$X = Z_{39} \cup \{\infty_0, \infty_1, \infty_2\}$.

$\Gamma = \{\{i, i+13, i+26\}, \{\infty_0, \infty_1, \infty_2\} : i = 0, 1, \ldots, 12\}$.

Parallel classes

$\{[1,2,7]$ $[4,8,28]$ $[16,32,34]$ $[11,19,25]$ $[5,22,37]$ $[10,20,31]$ $[21,24,35]$
$[6,18,23]$ $[27,36,17]$ $[15,12,14]$ $[3,30,38]$ $[9,0,\infty_0]$ $[26,33,\infty_1]$
$[13,29,\infty_2]\}$ (mod 39).

A resolvable GD(3, 2, 3, 66].

$X = Z_{63} \cup \{\infty_0, \infty_1, \infty_2\}$.

$\Gamma = \{\{i, i+21, i+42\}, \{\infty_0, \infty_1, \infty_2\} : i = 0, 1, \ldots, 20\}$.

Parallel classes

$\{[0,10,20]$ $[2,13,21]$ $[4,16,22]$ $[1,14,18]$ $[3,17,19]$ $[8,23,30]$ $[5,28,37]$
$[7,31,38]$ $[9,34,39]$ $[33,59,62]$ $[24,51,52]$ $[46,27,35]$ $[54,36,42]$ $[57,40,44]$
$[61,45,47]$ $[26,60,6]$ $[12,48,53]$ $[55,29,32]$ $[11,49,50]$ $[25,58,\infty_0]$ $[43,15,\infty_1]$
$[56,41,\infty_2]\}$ (mod 63).

A resolvable GD[3, 2, 2, 12].

$X = Z_{10} \cup \{\infty_0, \infty_1\}$.

$\Gamma = \{\{i, i+5\}, \{\infty_0, \infty_1\} : i = 0, 1, \ldots, 4\}$.

Parallel classes

{[0, 1, 9] [2, 5, 8] [3, 7, ∞_0] [4, 6, ∞_1]} (mod 10).

A resolvable GD[3, 2, 5, 30].

$X = Z_{25} \cup \{\infty_0, \infty_1, \ldots, \infty_4\}$.

$\Gamma = \{\{i + 5j : j = 0, 1, \ldots, 4\}, \{\infty_0, \infty_1, \ldots, \infty_4\} : i = 0, 1, \ldots, 4\}$.

Parallel classes

{[1, 2, 4] [7, 14, 16] [12, 18, 5] [13, 21, 0] [20, 3, 6] [9, 10, ∞_0] [15, 19, ∞_1] [17, 23, ∞_2]
[24, 8, ∞_3] [11, 22, ∞_4]} (mod 25).

A resolvable GD[3, 2, 7, 42].

$X = Z_{35} \cup \{\infty_0, \infty_1, \ldots, \infty_6\}$.

$\Gamma = \{\{i + 5j : j = 0, 1, \ldots, 6\}, \{\infty_0, \infty_1, \ldots, \infty_6\} : i = 0, 1, \ldots, 4\}$.

Parallel classes

{[0, 4, 6] [1, 9, 13] [3, 12, 14] [2, 18, 21] [5, 22, 23] [7, 28, 31] [10, 32, 33] [17, 24, ∞_0]
[30, 8, ∞_1] [15, 29, ∞_2] [25, 16, ∞_3] [19, 11, ∞_4] [34, 27, ∞_5] [26, 20, ∞_6]} (mod 35).

A resolvable GD[3, 2, 11, 66].

$X = Z_{55} \cup \{\infty_0, \infty_1, \ldots, \infty_{10}\}$.

$\Gamma = \{\{i + 5j : j = 0, 1, \ldots, 10\}, \{\infty_0, \infty_1, \ldots, \infty_{10}\} : i = 0, 1, \ldots, 4\}$.

Parallel classes

{[0, 7, 13] [2, 10, 14] [6, 15, 17] [1, 18, 24] [3, 21, 25] [8, 27, 29] [4, 28, 35] [5, 31, 34]
[9, 36, 37] [11, 47, 50] [16, 53, 54] [12, 26, ∞_0] [30, 46, ∞_1] [42, 19, ∞_2] [45, 23, ∞_3]
[43, 22, ∞_4] [52, 38, ∞_5] [33, 20, ∞_6] [44, 32, ∞_7] [51, 40, ∞_8] [48, 39, ∞_9] [49, 41, ∞_{10}]}
(mod 55).

A resolvable GD[3, 2, 13, 78].

$X = Z_{65} \cup \{\infty_0, \infty_1, \ldots, \infty_{12}\}$.

$\Gamma = \{\{i + 5j : j = 0, 1, \ldots, 12\}, \{\infty_0, \infty_1, \ldots, \infty_{12}\} : i = 0, 1, \ldots, 4\}$.

Parallel classes

{[0, 11, 19] [2, 14, 20] [4, 17, 21] [8, 22, 24] [1, 23, 29] [3, 26, 30] [7, 31, 33]
[5, 34, 41] [6, 37, 40] [10, 42, 43] [9, 48, 55] [12, 53, 56] [15, 57, 58] [27, 35, ∞_0]
[16, 25, ∞_1] [18, 39, ∞_2] [13, 50, ∞_3] [59, 32, ∞_4] [46, 28, ∞_5] [61, 44, ∞_6] [54, 38, ∞_7]
[63, 49, ∞_8] [60, 47, ∞_9] [64, 52, ∞_{10}] [62, 51, ∞_{11}] [45, 36, ∞_{12}]} (mod 65).

A resolvable GD[3, 2, 17, 102].

$X = Z_{85} \cup \{\infty_0, \infty_1, \ldots, \infty_{16}\}$.

$\Gamma = \{\{i + 5j : j = 0, 1, \ldots, 16\}, \{\infty_0, \infty_1, \ldots, \infty_{16}\} : i = 0, 1, \ldots, 4\}$.

Parallel classes

$\{[0, 11, 19]$ $[2, 14, 20]$ $[4, 17, 21]$ $[8, 22, 24]$ $[5, 26, 34]$ $[1, 23, 29]$ $[9, 32, 36]$ $[7, 31, 33]$ $[3, 35, 46]$ $[6, 39, 48]$ $[10, 44, 51]$ $[13, 49, 52]$ $[16, 53, 54]$ $[12, 60, 69]$ $[15, 64, 71]$ $[25, 76, 79]$ $[28, 80, 81]$ $[27, 58, \infty_0]$ $[18, 62, \infty_1]$ $[37, 83, \infty_2]$ $[68, 30, \infty_3]$ $[70, 43, \infty_4]$ $[73, 47, \infty_5]$ $[74, 50, \infty_6]$ $[61, 38, \infty_7]$ $[67, 45, \infty_8]$ $[63, 42, \infty_9]$ $[75, 56, \infty_{10}]$ $[77, 59, \infty_{11}]$ $[57, 40, \infty_{12}]$ $[82, 66, \infty_{13}]$ $[55, 41, \infty_{14}]$ $[78, 65, \infty_{15}]$ $[84, 72, \infty_{16}]\}$ (mod 85).

A resolvable GD[3, 2, 19, 114].

$X = Z_{95} \cup \{\infty_0, \infty_1, \ldots, \infty_{18}\}.$

$\Gamma = \{\{i + 5j : j = 0, 1, \ldots, 18\}, \{\infty_0, \infty_1, \ldots, \infty_{18}\} : i = 0, 1, \ldots, 4\}.$

Parallel classes

$\{[0, 12, 23]$ $[2, 15, 24]$ $[4, 18, 25]$ $[1, 17, 20]$ $[9, 26, 27]$ $[3, 30, 41]$ $[5, 33, 42]$ $[7, 36, 43]$ $[6, 37, 40]$ $[13, 45, 46]$ $[8, 47, 59]$ $[11, 52, 60]$ $[14, 56, 62]$ $[10, 53, 57]$ $[19, 63, 65]$ $[16, 72, 80]$ $[21, 78, 84]$ $[28, 86, 90]$ $[22, 81, 83]$ $[31, 55, \infty_0]$ $[32, 58, \infty_1]$ $[35, 87, \infty_2]$ $[29, 82, \infty_3]$ $[34, 88, \infty_4]$ $[67, 38, \infty_5]$ $[76, 48, \infty_6]$ $[66, 39, \infty_7]$ $[70, 44, \infty_8]$ $[85, 61, \infty_9]$ $[91, 68, \infty_{10}]$ $[71, 49, \infty_{11}]$ $[75, 54, \infty_{12}]$ $[69, 50, \infty_{13}]$ $[92, 74, \infty_{14}]$ $[94, 77, \infty_{15}]$ $[89, 73, \infty_{16}]$ $[93, 79, \infty_{17}]$ $[64, 51, \infty_{18}]\}$ (mod 95).

A resolvable GD[3, 3, 2, 12].

$X = Z_{10} \cup \{\infty_0, \infty_1\}.$

$\Gamma = \{\{i, i + 5\}, \{\infty_0, \infty_1\} : i = 0, 1, \ldots, 4\}.$

Parallel classes

$\{[0, 4, 6]$ $[5, 7, 8]$ $[1, 3, \infty_0]$ $[2, 9, \infty_1]\}$ (mod 10)

$\{[0, 3, 4]$ $[5, 8, 9]$ $[1, 2, \infty_0]$ $[6, 7, \infty_1]\} + i,$ $i = 0, 1, \ldots, 4.$

A resolvable GD[3, 3, 6, 18].

$X = Z_{15} \cup \{\infty_0, \infty_1, \infty_2\}.$

$\Gamma = \{\{\infty_i, i + 3j : j = 0, 1, \ldots, 4\} : i = 0, 1, 2\}.$

Parallel classes are formed from the orbits of the following base parallel classes under the action of the permutation of which sends $\infty_i \to \infty_{i+1}$ (reducing subscripts modulo 3), and sends $i \to i + 1$ (mod 15) for all i in Z_{15}. Note that the first base parallel class has an orbit of length 3, and the second has an orbit of length 15.

$\{[\infty_0, \infty_1, \infty_2]$ $[3i, 3i + 10, 3i + 5] : i = 0, 1, \ldots, 4\}$

$\{[\infty_0, 13, 11]$ $[3, \infty_1, 2]$ $[9, 10, \infty_2]$ $[0, 7, 14]$ $[6, 4, 8]$ $[12, 1, 5]\}.$

Discrete Mathematics 77 (1989) 21–27
North-Holland

MINIMALLY PROJECTIVELY EMBEDDABLE STEINER SYSTEMS*

Lynn Margaret BATTEN
University of Winnipeg, 515 Portage Avenue, Canada R3B 2E9

Dedicated to Haim Hanani on his seventy-fifth birthday.

We study Steiner systems which embed "in a minimal way" in projective planes, and consider connections between the automorphism group of the Steiner systems and corresponding planes. Under certain conditions we are able to show (see Theorem 2) that such Steiner systems are either blocking sets or maximal arcs.

1. Introduction

A *Steiner system* $S = S(2, k, v)$ is an ordered pair (P, B) where P is a finite set of v elements called *points*, B is a set of subsets of size $k \geq 2$, of P, called *blocks*, such that two points are on a unique block. S is *trivial* if $|B| \leq 1$.

Let $b = |B|$ and let r be the number of blocks per point. It follows that $v - 1 = r(k-1)$ and $vr = bk$. Thus a necessary condition for the existence of Steiner systems $S(2, k, v)$ is that $v - 1 \equiv 0 \pmod{k-1}$ and $v(v-1) \equiv 0 \pmod{k(k-1)}$ [9]. Hanani proved that these congruences are together sufficient in case $k = 3$, 4 or 5 [10, 11].

A *projective plane* is a Steiner system $S(2, q+1, q^2+q+1)$ for $q \geq 2$. Here q is called the *order* of the projective plane. If S is a projective plane, we normally refer to its blocks as *lines*.

It appears to be the case that the majority of Steiner systems embed in projective planes [2]. In this article, we are interested in those Steiner systems which embed in a 'minimal' way, as defined in the next section, and in the resulting relationships between the automorphism groups acting on the two structures. Clearly, if a Steiner system S embeds in a projective plane Π which in turn embeds in a second projective plane Π', there need be no connection whatsoever between the automorphism groups of S and Π'. Thus some notion of Π 'lying minimally' in S is crucial if we expect to be able to say anything at all about the connections between the two structures.

We shall need the following definitions.

A subset of the points of a projective plane Π which is met by every line of Π but which itself contains no line of Π, is called a *blocking set*.

* Research supported by NSERC grant A3485.

A subset of the points of a projective plane Π which is met by every line of Π in either 0 or a constant k points, but which contains more than k points of Π, is called a *maximal arc*. It is obvious that a maximal arc forms a non-trivial Steiner system $S(2, k, v)$ and that a Steiner system in Π is a maximal arc if and only if $r = q + 1$, where q is the order of Π.

For more information on blocking sets and maximal arcs, we refer the reader to the book [14] by Hirschfeld.

Our main results are presented in Theorems 1, 2 and 3.

2. The setting

We wish to consider the situation of a Steiner system embedded in a 'smallest possible' projective plane. The definition we give below assumes conditions on a Steiner system S which allow us to construct such a projective plane on S.

A Steiner system $S = S(2, k, v)$ is *minimally projectively embeddable* (an *mpe-system*) if for some integer q,

(i) S is equipped with a non-empty family $\mathscr{F}$ of sets of blocks, each containing a set of $\geqslant 2$ mutually non-intersecting blocks such that any two non-intersecting blocks of S occur in precisely one element of $\mathscr{F}$. If $L \in F \in \mathscr{F}$, we write $F \in L$ and say that F "belongs to", "is in", or "is on", L;

(ii) $|\mathscr{F}| + v = q^2 + q + 1$;

(iii) for any distinct elements x and y of $\mathscr{F} \cup P$, there is a unique set X of $q + 1$ elements of $\mathscr{F} \cup P$ including x and y, with the property that for each block L of S, precisely one of the following holds: $L \subseteq X$; there is a unique element of X on L.

If S is an mpe-system, we shall often refer to it more precisely as the pair $(S, \mathscr{F})$, where $\mathscr{F}$ is the family described in (i).

We say $(S, \mathscr{F})$ *embeds minimally* in the projective plane Π if S is an mpe-system which is a restriction of Π to some subset of its point set, and if for all points $x \in \Pi \backslash S$, there is a unique element $F \in \mathscr{F}$ such that the blocks of F are precisely the restrictions of the lines of Π on x to the points of S.

The following facts are immediate from the above definitions: S contains non-intersecting blocks and so if S embeds minimally in Π, S is non-trivial and S cannot equal Π; every point of $\Pi \backslash S$ is on at least two lines of Π which have restrictions to blocks of S.

Proposition 1. *Let Π be a projective plane of order q and $S = (P, B)$ a Steiner system which is a restriction of Π to a point-set P of Π. Suppose that each point of $\Pi \backslash S$ is on at least two lines which restricted to S are blocks of S. Then S is an mpe-system provided with the family $\mathscr{F}$ corresponding to the points of $\Pi \backslash S$, and $(S, \mathscr{F})$ embeds minimally in Π.*

Theorem 1. *Let $(S, \mathcal{F})$ be an mpe-system for some integer q. Then there is up to isomorphism a unique projective plane Π of order q such that S embeds minimally in Π.*

Proof. Consider the system $\Pi = (\mathcal{F} \cup P, \mathcal{L})$, where $\mathcal{L}$ is the set of all $(q+1)$-sets defined in (iii). Clearly Π is a Steiner system $S(2, q+1, q^2+q+1)$ and so a projective plane of order q. We need to check that the restriction to P of a line of Π which contains at least two points of P is a block of S. Let x and y be points of the line ℓ in Π which are also in P. Then there is a block L of S on x and y. By (iii), $L \subseteq \ell$. Conversely, using (iii), any block L of S is a subset of a unique line ℓ of Π.

To show that π is unique, suppose $(S, \mathcal{F})$ embeds minimally in both Π_1 and Π_2. Define a map ϕ from Π_1 to Π_2 as follows. We may identify S in both planes, so that $\phi(x) = x$ for all $x \in S$. This induces a map on blocks of S and so on lines of Π_1 which have restrictions to blocks of S. So for $x \in \Pi_1 \setminus S$, since by (i), x is on at least two elements of some $F \in \mathcal{F}$, we may define $\phi(x)$ to be the intersection in Π_2 of the image of the elements of F. Thus ϕ is well-defined on all points of Π_1. It remains only to check that for an arbitrary line ℓ of Π_1, the set $\{\phi(x), x \in \ell\}$ is a line of Π_2. But this follows easily from the definition given in (iii). Thus ϕ is an isomorphism between Π_1 and Π_2. $\square$

We call the plane Π of Theorem 1 the *minimal projective extension* of $(S, \mathcal{F})$.

If $(S, \mathcal{F})$ embeds minimally in Π, and ℓ is a line of Π, we call ℓ respectively a *secant, tangent,* or *exterior line,* if it has k, 1 or 0 points in common with S.

Examples

1. Any maximal arc different from Π embeds minimally in Π. In particular, if S is an affine plane this is well known. If Π has order q and S is a $(q+1)$-arc (oval) in Π if q is odd, or a $(q+2)$-arc (hyperoval) in Π if q is even [14], then S embeds minimally in Π by Proposition 1.
2. $S = \mathrm{AG}(2,3)$ embeds minimally in $\Pi = \mathrm{PG}(2,4)$ in such a way that each point of $\Pi \setminus S$ is the intersection of precisely two secants of Π [17].

In each of the above examples, the elements of $\mathcal{F}$ have the same size. When this is the case, it is possible to compute this constant as a function of q, r and k, as we show in the next proposition.

Proposition 2. *Let $(S, \mathcal{F})$ embed minimally in Π such that each point of $\Pi \setminus S$ is on the same number c of secants of Π. Then $c = (r(q+1-k)(rk-r+1))/(k(q^2+q-rk+r))$. In particular, S is a maximal arc if and only if $c = v/k = q+1-q/k$; thus, in this case, $k \mid q$.*

Proof. Counting in two ways flags (p, ℓ), p a point of $\Pi \setminus S$ and ℓ a secant, gives

$b(q+1-k)=c(q^2+q+1-v)$. Then using $vr=bk$ and $v-1=r(k-1)$ gives the value for c. Since S is a maximal arc precisely when $r=q+1$, substituting this value in the equation for c yields $c=v/k=q+1-q/k$. □

3. Automorphisms

In this section, we shall concentrate on the connections between the groups of automorphisms acting on S and those acting on Π, where S embeds minimally in Π. It is clear that interesting results will be obtained only when we consider automorphisms of S which can be extended to automorphisms of Π. In order to ensure that this is the case, we shall subject $(S, \mathcal{F})$ to the following condition.

(E) Let $(S, \mathcal{F})$ be an mpe-system, and let G be a subgroup of Aut(S). Then for all $F \in \mathcal{F}$ and $g \in G$ we have $g(F) \in \mathcal{F}$.

Proposition 3. *Let $(S, \mathcal{F})$ be an mpe-system satisfying (E) for some subgroup G of* Aut(S). *Then G extends to a subgroup G^* of* Aut(Π), *where Π is the minimal projective extension of $(S, \mathcal{F})$, such that each element of G^* restricted to S is an element of G.*

Proof. Let $g \in G$. Define $g^* = g$ on points of S. For $x \in \Pi \setminus S$ such that x corresponds to $F \in \mathcal{F}$, define $g^*(x)$ to be the point of $\Pi \setminus S$ corresponding to $g(F) \in \mathcal{F}$. By (E), g^* is well-defined. Let ℓ be an arbitrary line of Π, and consider $g^*(\ell) = \{g^*(x) \mid x \in \ell\}$. To show that $g^*(\ell)$ is a line of Π, it suffices by the proof of Theorem 1 and by (iii) to show that for any secant $\mathscr{k}$ of Π, either $\mathscr{k} = g^*(\ell)$ or $|\mathscr{k} \cap g^*(\ell)| = 1$. But $\{g(L) \mid L \text{ a block of } S\} = \{L \mid L \text{ a block of } S\}$, and since for any secant $\mathscr{k}$ of Π, either $\mathscr{k} = \ell$ or $|\mathscr{k} \cap \ell| = 1$, the result follows. □

It is now trivial to show that $G^* = \{g^* \mid g \in G\}$ forms a group.

A number of results exist in the literature classifying Steiner systems with automorphism groups satisfying certain kinds of transitivity conditions. We mention two of the important ones here, commenting on minimal embeddability and whether or not (E) holds for some subgroups of Aut(S). The reader is referred to [1, 2,7] for more results on transitivity of Steiner systems, as well as the pertinent definitions.

Kantor [15]. If S is a Steiner system with automorphism group 2-transitive on points, then S is one of

(a) a Desarguesian affine or projective space (in the latter case, two points per line are allowed),

(b) an Hermitian or Ree unital,

(c) the Hering affine plane of order 27 [12] or the near-field affine plane of order 9,

(d) one of two Steiner systems $S(2, 9, 9^3)$ due to Hering [13].

For a discussion of and examples of projective and therefore also affine spaces embedded (not necessarily minimally) in projective planes, we refer the reader to [3].

Any Hermitian unital $H = S(2, q+1, q^3+1)$ embeds minimally in $\mathrm{PG}(2, q^2)$ and forms a blocking set there. The number of secants of each point of $\Pi \setminus H$ is $q^2 - q$ [4]. It is known that the Ree unitals $S(2, q+1, q^3+1)$ cannot be embedded in any projective plane of order q^2 [16].

The affine planes of (c) are of course, minimally projectively embeddable. We know nothing about minimal embeddability of the systems in (d).

Delandtsheer [8]. If S is a Steiner system with automorphism group transitive on pairs of intersecting lines and transitive on pairs of non-intersecting lines, then S is a Desarguesian affine plane, a Desarguesian projective space, or a complete graph.

We shall see in Theorem 2 of the next section that if S is an mpe-system satisfying (E) and the conditions of Delandtsheer's theorem, then S is either a maximal arc or a blocking set. If S is an affine or Desarguesian subspace of Π, we again refer to [3]. If S is a complete graph and $r = q+1$, then S is a hyperoval as in Example 2. S cannot be both a complete graph and a blocking set in Π.

It is clear that there is a connection between the way an automorphism of S acts on non-intersecting blocks of S and the way an extension of this automorphism to a projective plane Π on S would act on the point of intersection of these two blocks in Π. In fact, we have easily the following result.

Proposition 4. *Let G be a subgroup of* $\mathrm{Aut}(S)$, $(S, \mathcal{F})$ *an mpe-system embedding minimally in Π, and satisfying (E). Then* $v_{G^*} = v_G + |\{\text{orbits of } G \text{ on unordered pairs of non-intersecting blocks of } S\}|$, *where v_G denotes the number of point orbits of G in S, and v_{G^*} denotes the number of point orbits of G^* in Π.*

Corollary. *Let G satisfy the conditions of Proposition 4, and in addition, be homogeneous on pairs of non-intersecting blocks of S. Then $v_{G^*} = v_G + 1$.*

For the proof of the next theorem we use the following result Block [5]. Let G be a subgroup of $\mathrm{Aut}(S)$, S a Steiner system. Let v_G and b_G be respectively the number of point and of line orbits of S under G. Then $v_G \leqslant b_G$. Moreover, Brauer [6], if $v = b$ then $v_G = b_G$. For proofs of these results see [4].

Theorem 2. *Let G be a subgroup of* $\mathrm{Aut}(S)$, $(S, \mathcal{F})$ *minimally embeddable in Π and satisfying (E). Suppose also that G is transitive on blocks of S and homogeneous on pairs of non-intersecting blocks of S. Then $v_{G^*} = b_{G^*} = 2$ and S is either a maximal arc or a blocking set.*

Proof. G line transitive implies G point transitive by Block's result. So $v_G = b_G = 1$. By the corollary to Proposition 4 and again using Brauer, $v_{G^*} = b_{G^*} = 2$.

Thus the lines of Π fall into two orbits under G^*. Clearly secants form a single orbit. The other orbit therefore consists either entirely of tangents or entirely of exterior lines. In the former case, S is a blocking set; in the latter, $r = q + 1$ and S is a maximal arc. □

Delandtsheer [8] proved as a preliminary step in her result mentioned above, that if G is a subgroup of Aut(S) for a Steiner system S which is transitive on pairs of intersecting blocks and on pairs of non-intersecting blocks, then G is 2-transitive on points of S. A major question is what can be said with *only* the assumption of transitivity on pairs of (non-) intersecting blocks.

If in addition to the assumptions of Theorem 2, the numbers of points of S and Π are coprime, we are able to say more, as we show in the final result.

Theorem 3. *Let S and G satisfy the conditions of Theorem 2. Suppose in addition that $(v, q^2 + q + 1) = 1$, q the order of Π. Then G is flag-transitive on S, and S is not a blocking set.*

Proof. Let $p \in S$ and consider the stabilizer G_p^* of p in Π. For $x \notin S$, we have $|G^*| = |\{g(p) \mid g \in G^*\}| \cdot |G_p^*| = v\,|G_p^*| = v\,|\Omega|\,|G_{p,x}^*|$, where Ω is the orbit under G_p^* of x in Π.

Similarly, $|G^*| = (q^2 + q + 1 - v)\,|G_x^*| = (q^2 + q + 1 - v)\,|\Delta|\,|G_{x,p}^*|$, where Δ is the orbit of p under G_x^* in Π.

So $v\,|\Omega| = (q^2 + q + 1 - v)\,|\Delta|$. But $(v, q^2 + q + 1) = 1$ implies $|\Omega| = q^2 + q + 1 - v$, and so $\Omega = \Pi \setminus S$. Thus G_p^* is transitive on $\Pi \setminus S$.

Now consider flags (p, L) and (p', L') of S. Since $k = q + 1$ would contradict $S \neq \Pi$, we know that each block of S has at least one point in $\Pi \setminus S$. It follows from the above that for any $p \in S$, G_p^* is transitive on lines through p. Hence there exist maps $g_1 \in G_p^*$ taking (p, L) to (p, pp'), pp' the line on p and p', $g_2 \in G^*$ taking (p, pp') to $(p', g_2(pp'))$, where $g_2(pp')$ is a line on p', and $g_3 \in G_{p'}^*$, taking $(p', g_2(pp'))$ to (p', L'). The composition of these three maps gives the desired result.

Suppose now that S is a blocking set. Then, since there are no exterior lines, counting lines of Π in two different ways yield $q^2 + q + 1 = b + v(q + 1 - r) = v(r/k + q + 1 - r)$. So $(v, q^2 + q + 1) = 1$ implies $q^2 + q + 1 \mid r + qk + k - rk$. If $r = q + 1$, then S is a maximal arc and hence not a blocking set. So $r \leq q$. If $k = q$, then also $r = q$ and we get $q^2 + q + 1 \mid 2q$, a contradiction. So $k \leq q - 1$, implying $q^2 + q + 1 \leq q^2 + q - 1 - rk$, again a contradiction. □

References

[1] L.M. Batten, Transitivity on finite linear spaces, Technical Report 69, Seminario di Geometrie Combinatorie, University of Rome, 1987.
[2] L.M. Batten and A. Beutelspacher, The Theory of Finite Linear Spaces: Combinatorics of Points and Lines, Cambridge University Press, to appear.
[3] L.M. Batten, J.M.N. Brown and M.J. de Resmini, Steiner systems in finite projective planes, submitted.
[4] T. Beth, D. Jungnickel and H. Lenz, Design theory (Cambridge University Press, Cambridge, New York, 1986).
[5] R.E. Block, On the orbits of collineation groups, *Math. Zeit.* 96 (1967) 33–49.
[6] R. Brauer, On the connections between the ordinary and the modular characters of groups of finite order, Ann. Math. 42 (1941) 926–935.
[7] F. Buekenhout, A. Delandtsheer and J. Doyen, Finite linear spaces with flag-transitive groups, submitted.
[8] A. Delandtsheer, Transitivity on ordered pairs of lines in finite linear spaces, Abh. Math. Sem. Univ. Hamburg 54 (1984) 107–110.
[9] M. Hall, Jr., Combinatorial Theory, 2nd ed. (John Wiley & Sons, New York, 1986).
[10] H. Hanani, The existence and construction of balanced incomplete block designs. Ann. Math. Statist. 32 (1961) 361–386.
[11] H. Hanani, On balanced incomplete block designs with blocks having five elements, J. Combin. Theory 12 (1972) 184–201.
[12] C. Hering, Eine nicht-desarguessche zweifach transitive affine Ebene der Ordnung 27, Abh. Math. Sem. Univ. Hamburg 34 (1969) 203–208.
[13] C. Hering, Two new sporadic doubly transitive linear spaces, Finite Geometries, Lecture Notes in Pure and Applied Mathematics, 103 (ed. C.A. Baker and L.M. Batten) (Marcel Dekker, New York, 1985) 127–129.
[14] J.W.P. Hirschfeld, Projective Geometries over Finite Fields (Clarendon Press, Oxford, 1979).
[15] W.M. Kantor, Homogeneous designs and geometric lattices, J. Combin. Theory (A) 38 (1985) 66–74.
[16] H. Lüneburg, Some remarks concerning the Ree groups of type (G_2), J. Algebra 3 (1966) 256–259.
[17] T.G. Ostrom and F.A. Sherk, Finite projective planes with affine subplanes, Can. Math. Bull. 7 (1964) 549–559.
[18] T.G. Ostrom and A. Wagner, On projective and affine planes with transitive collineation groups, Math. Zeit. 71 (1959) 186–199.

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 29–50
North-Holland

THE SPECTRA OF A VARIETY OF QUASIGROUPS AND RELATED COMBINATORIAL DESIGNS

F.E. BENNETT*
Department of Mathematics, Mount Saint Vincent University, Halifax, Nova Scotia, B3M 2J6 Canada

A quasigroup is an ordered pair $(Q, \cdot)$, where Q is a set and $(\cdot)$ is a binary operation on Q such that the equations $ax = b$ and $ya = b$ are uniquely solvable for every pair of elements a, b in Q. It is well-known that the multiplication table of a quasigroup defines a Latin square, and to each quasigroup are associated six (not necessarily distinct) conjugate quasigroups. The spectrum of the two-variable quasigroup identity $u(x, y) = v(x, y)$ is the set of all integers n such that there exists a quasigroup of order n satisfying the identity $u(x, y) = v(x, y)$. Trevor Evans has provided a collection of two-variable quasigroup identities, which imply that two conjugates are orthogonal and which are conjugate-equivalent to "short conjugate-orthogonal identities". These identities include the familiar Stein identity, $x(xy) = yx$, which has been given a considerable amount of attention. Apart from being associated with conjugate orthogonal Latin squares, some of the identities have been used in the description of other types of combinatorial designs, such as BIBDs, Mendelsohn designs, certain classes of graphs, and orthogonal arrays with interesting conjugacy properties. We shall briefly survey the known results and in some cases we present new results concerning the spectra of the short conjugate-orthogonal identities, which have not been previously investigated. The emphasis will be on the constructions and uses of pairwise balanced designs (PBDs) and related combinatorial structures.

1. Introduction

A *quasigroup* is an ordered pair $(Q, \cdot)$, where Q is a set and $(\cdot)$ is a binary operation on Q such that the equations $ax = b$ and $ya = b$ are uniquely solvable for every pair of elements a, b in Q. It is fairly well-known (see, for example, [24]) that the multiplication table of a quasigroup defines a *Latin square*, that is, a Latin square can be considered as the multiplication table of a quasigroup with the headline and sideline removed. We shall be concerned mainly with finite quasigroups (Latin squares). A quasigroup $(Q, \cdot)$ is called *idempotent* if the identity $x^2 = x$ holds for all x in Q.

The *spectrum* of the two-variable quasigroup identity $u(x, y) = v(x, y)$ is the set of all integers n such that there exists a quasigroup of order n satisfying the identity $u(x, y) = v(x, y)$. It is particularly useful to study the spectrum of certain two-variable quasigroup identities, since such identities are quite often instrumental in the construction or algebraic description of combinatorial designs. For example, it is well-known (see [22]) that an *idempotent totally symmetric*

* Research supported by the Natural Sciences and Engineering Research Council of Canada under Grant A-5320.

0012-365X/89/$3.50

quasigroup $(Q, \cdot)$ (commonly called a *Steiner quasigroup*), $\{x^2 = x, x(xy) = y, (xy)y = x\}$, corresponds to a *Steiner triple system*, where $\{x, y, z\}$ is a triple if and only if $x \cdot y = z$, where x, y, z are distinct and $x^2 = x$ for all x. Similarly, an *idempotent semisymmetric quasigroup* $(Q, \cdot)$, $\{x^2 = x, (xy)x = y, x(yx) = y\}$, corresponds to a *Mendelsohn triple system* (see [52]), with (x, y, z) as a cyclically ordered triple if and only if $x \cdot y = z$, where x, y, z are distinct and $x^2 = x$ for all x. A quasigroup $(Q, \cdot)$ satisfying both the *Stein identity*, $x(xy) = yx$, *and* the *Schröder identity*, $(xy)(yx) = x$, corresponds to a $(2, 4)$—*Steiner system*, the blocks of size 4 being the 2-generator subquasigroups (see [66]). Indeed, most of the two-variable identities, which we shall investigate in this paper, have been used in the description and construction of combinatorial structures, such as $(2, k)$-Steiner systems, Mendelsohn designs, certain classes of graphs, Latin squares, and orthogonal arrays with interesting conjugacy properties. For more details, the interested reader may wish to consult the references.

If $(Q, \otimes)$ is a quasigroup, we may define on the set Q six binary operations $\otimes(1,2,3)$, $\otimes(1,3,2)$, $\otimes(2,1,3)$, $\otimes(2,3,1)$, $\otimes(3,1,2)$ and $\otimes(3,2,1)$ as follows: $a \otimes b = c$ if and only if

$$a \otimes (1,2,3)b = c, \qquad a \otimes (1,3,2)c = b, \qquad b \otimes (2,1,3)a = c$$
$$b \otimes (2,3,1)c = a, \qquad c \otimes (3,1,2)a = b, \qquad c \otimes (3,2,1)b = a.$$

These six (not necessarily distinct) quasigroups $(Q, \otimes(i, j, k))$, where $\{i, j, k\} = \{1, 2, 3\}$, are called the *conjugates* of $(Q, \otimes)$ (see Stein [65]). If the multiplication table of a quasigroup $(Q, \otimes)$ defines a Latin square L, then the six Latin squares defined by the multiplication tables of its conjugates $(Q, \otimes(i, j, k))$ are called the conjugates of L. It is well-known (see, for example, [49]) that the number of distinct conjugates of a quasigroup (Latin square) is always 1, 2, 3 or 6. The interested reader may wish to refer to the book of Dénes and Keedwell [24] for more details pertaining to Latin squares.

Two quasigroup identities $u_1(x, y) = u_2(x, y)$ and $v_1(x, y) = v_2(x, y)$ are said to be *conjugate-equivalent* if when $(Q, \cdot)$ is a quasigroup satisfying one of them, then at least one conjugate of $(Q, \cdot)$ satisfies the other. For example, the Stein identity $x(xy) = yx$ is conjugate-equivalent to the identity $(yx)x = xy$, since the latter can be obtained by taking the $(2,1,3)$-conjugate (usually called *transpose*) of the Stein quasigroup.

Two quasigroups $(Q, \cdot)$ and $(Q, *)$ defined on the same set Q are said to be *orthogonal* if the pair of equations $x \cdot y = a$ and $x * y = b$, where a and b are any two given elements of Q, are satisfied simultaneously by a unique pair of elements from Q. Equivalently, we say that $(Q, \cdot)$ and $(Q, *)$ are orthogonal if $x \cdot y = z \cdot t$ and $x * y = z * t$ together imply $x = z$ and $y = t$. We remark that when the two quasigroups $(Q, \cdot)$ and $(Q, *)$ are orthogonal then their corresponding Latin squares are also orthogonal in the usual sense.

It is perhaps worth mentioning that the above definition of orthogonality between quasigroups can be extended to more general algebraic systems, such as groupoids, as was done by Trevor Evans in [27]. If we adapt the notation of [27], where the functional notation $a(x, y)$ is conveniently used in place of the infix notation $x * y$ for the operation, then we say that the two binary operations $a(x, y)$ and $b(x, y)$ defined on the same set Q are *orthogonal operations*, briefly written $a \perp b$, if $|\{(x, y): a(x, y) = i, b(x, y) = j\}| = 1$ for every ordered pair i, j in Q.

A quasigroup (Latin square) which is orthogonal to its (i, j, k)-conjugate is called *(i, j, k)-conjugate orthogonal.* A $(2, 1, 3)$-conjugate orthogonal quasigroup (Latin square) is more commonly called *self-orthogonal.* Orthogonality relations between pairs of conjugates of quasigroups (Latin squares) have been studied quite extensively (see, for example, [2, 4, 5, 7, 12, 17, 27, 37, 46, 61, 65]).

In [27] Trevor Evans introduced the concept of "short conjugate-orthogonal identity", which is perhaps best described in light of the following result.

Theorem 1.1 (Trevor Evans [27]). *Let $a(x, y)$ and $b(x, y)$ be conjugate operations on Q. Then $a \perp b$ if and only if there is a quasigroup word $w(x, y)$ such that $w(a(x, y), b(x, y)) = x$ holds identically.*

As Trevor Evans subsequently remarked, Theorem 1.1 provides a method of producing many quasigroup identities which imply that two conjugates are orthogonal. He called an identity of the type described in Theorem 1.1 where $w(x, y)$ is a word of length two a *short conjugate-orthogonal identity.* A simplified description of all such identities to within conjugacy-equivalence was given by Trevor Evans in [27, Theorem 6.2] which we state below. Note that, through private communication [30] with Trevor Evans, the identities $(y \cdot yx)y = x$ and $(y \cdot xy)y = x$ have replaced the identities $(y \cdot yx)x = x$ and $(y \cdot xy)x = x$ respectively, which, for example, are satisfied by Steiner quasigroups and inadvertently appeared as a result of a typographical error.

Theorem 1.2 (Trevor Evans [27, 30]). *Any non-trivial short conjugate-orthogonal identity is conjugate-equivalent to one of the following:*

(i)	$xy \cdot yx = x$	(ii)	$yx \cdot xy = x$
(iii)	$(x \cdot yx)y = x$	(iv)	$(x \cdot xy)y = x$
(v)	$(xy \cdot x)y = x$	(vi)	$(y \cdot yx)y = x$
(vii)	$(y \cdot xy)y = x$	(viii)	$(yx \cdot x)y = x$
(ix)	$(yx \cdot y)y = x$	(x)	$(xy \cdot y)y = x$
(xi)	$x \cdot xy = yx$	(xii)	$xy \cdot y = x \cdot xy$
(xiii)	$(xy \cdot y)x = xy$	(xiv)	$yx \cdot y = x \cdot yx$

Before proceeding, we wish to point out that, to within conjugacy-equivalence, the list of identities in Theorem 1.2 can further be reduced. For convenience and future reference, we formally state the following:

Proposition 1.3. *Any identity listed in Theorem* 1.2 *is conjugate-equivalent to one of the following*:

(1) $xy \cdot yx = x$	(2) $yx \cdot xy = x$
(3) $(xy \cdot y)y = x$	(4) $x \cdot xy = yx$
(5) $(yx \cdot y)y = x$	(6) $(xy \cdot x)y = x$
(7) $xy \cdot y = x \cdot xy$	(8) $yx \cdot y = x \cdot yx$

Proof. First of all, it should be mentioned that the identities (vii) and (ix) of Theorem 1.2 are actually equivalent. By replacing x by xy in $(yx \cdot y)y = x$, we get $((y \cdot xy)y)y = xy$, and by cancellation, we have $((y \cdot xy)y = x$. Conversely, the identity $(y \cdot xy)y = x$ implies $yx \cdot y = (y((y \cdot xy)y))y = y \cdot xy$, that is, the identity $(y \cdot xy)y = x$ implies $(yx \cdot y)y = x$. Secondly, the identities (vi) and (ix) of Theorem 1.2 are conjugate equivalent. For if a quasigroup satisfies the identity $(y \cdot yx)y = x$, then its transpose will satisfy $y(xy \cdot y) = x$ which, by replacing x by yx, implies $y((yx \cdot y)y) = yx$ and, by cancellation, $(yx \cdot y)y = x$. In a similar manner, one can verify the additional conjugacy-equivalence among the following pairs of identities in Theorem 1.2:

(a) The $(1, 3, 2)$-conjugate of a quasigroup satisfying the identity (ii) $yx \cdot xy = x$ will satisfy the identity (iii) $(x \cdot yx)y = x$.
(b) The $(1, 3, 2)$-conjugate of a quasigroup satisfying (xi) $x \cdot xy = yx$ will satisfy (iv) $(x \cdot xy)y = x$.
(c) The $(2, 3, 1)$-conjugate of a quasigroup satisfying the identity (xi) $x \cdot xy = yx$ will satisfy (xiii) $(xy \cdot y)x = xy$.
(d) The $(3, 2, 1)$-conjugate of a quasigroup satisfying the identity (ix) $(yx \cdot y)y = x$ will satisfy (viii) $(yx \cdot x)y = x$.

This essentially completes the proof of the proposition. □

C.C. Lindner and E. Mendelsohn [45] extended the concept of a conjugate of a quasigroup to that of a conjugate of an $n^2 \times k$ orthogonal array, which is obtained by permuting the columns of the array. We define an $n^2 \times k$ *orthogonal array* based on an n-set, say $S = \{1, 2, \ldots, n\}$, to be a rectangular array of n^2 rows and k columns where, for any two distinct columns, the set of ordered pairs occurring in these two columns and the n^2 rows is precisely the set of all n^2 distinct ordered pairs from S. Evidently, a quasigroup $(Q, \cdot)$ of order n is equivalent to an $n^2 \times 3$ orthogonal array, where (x, y, z) is a row of the array if and only if $x \cdot y = z$. Lindner and Mendelsohn also defined the *conjugate invariant subgroup* for an $n^2 \times k$ orthogonal array to be the group of all permutations on $\{1, 2, \ldots, k\}$ which yield conjugates equal to the original array. For the cases $k = 3$ and 4, the interested reader may refer to the survey paper of Lindner [39]. For more detailed results, refer to [45, 47, 48, 49], where a complete characterization of the groups which can be conjugate invariant subgroups for $n^2 \times 3$ and $n^2 \times 4$ orthogonal arrays is given.

Example 1.4. Below we give an example of a quasigroup of order 4 and its associated $4^2 \times 3$ orthogonal array which has the cyclic group $C_3 = \langle (1\,2\,3) \rangle$ as conjugate invariant subgroup. Note that the quasigroup is idempotent and semisymmetric, and it corresponds to a Mendelsohn triple system of order 4.

Quasigroup $(Q, \cdot)$

$\cdot$	1	2	3	4
1	1	3	4	2
2	4	2	1	3
3	2	4	3	1
4	3	1	2	4

Orthogonal Array

(1, 1, 1)
(1, 2, 3)
(1, 3, 4)
(1, 4, 2)
(2, 1, 4)
(2, 2, 2)
(2, 3, 1)
(2, 4, 3)
(3, 1, 2)
(3, 2, 4)
(3, 3, 3)
(3, 4, 1)
(4, 1, 3)
(4, 2, 1)
(4, 3, 2)
(4, 4, 4)

It is fairly evident that, disregarding the level at which the rows occur, the above orthogonal array remains invariant under cyclic permutation of its columns.

The main purpose of this paper is to focus attention on the spectrum of each of the identities listed in Proposition 1.3. Some of these identities have been given a considerable amount of attention by various authors, while others remain to be investigated. We shall very briefly survey the known results and, in particular, give some improvements on the spectrum of a variety of the familiar Stein quasigroups. We shall also present some new results on the spectra of some of the other identities which have not been previously investigated. We shall employ both direct and recursive methods for constructing quasigroups, where the emphasis will be on the constructions and uses of pairwise balanced designs (PBDs) and other related combinatorial designs. In view of Proposition 1.3, this paper presents fairly conclusive results regarding the spectra of most of the identities listed by Trevor Evans in Theorem 1.2.

2. Finite models and recursive constructions of quasigroups

In what follows, we shall be concerned mainly with finite quasigroups. We shall describe some of the techniques for constructing quasigroups which satisfy some particular two-variable identity $u(x, y) = v(x, y)$.

The most direct method of constructing finite models of a quasigroup $(Q, \cdot)$ satisfying $u(x, y) = v(x, y)$ is to look for a model of the identity of the form $x \cdot y = \lambda x + \mu y$, where the elements lie in a finite field (or finite near field). This technique is fairly well-known and has been used quite extensively (see, for example, [29, 47, 51, 54, 65]). In particular, for idempotent models, we shall look for models of the identity of the form $x \cdot y = \lambda x + (1 - \lambda)y$ in $\mathrm{GF}(q)$, where q is a prime power and $\lambda \neq 0$ or 1. This will require finding a solution to some polynomial equation $f(\lambda) = 0$ in $\mathrm{GF}(q)$, depending on the identity being investigated. We present the following useful example.

Example 2.1. Consider the identity $(yx \cdot y)y = x$ (identity (5) of Proposition 1.3). This identity does not imply the idempotent law $x^2 = x$. If, however, we are interested in idempotent models of $(yx \cdot y)y = x$, we may look for models of the identity of the form $x \cdot y = \lambda x + (1 - \lambda)y$, where $\lambda \neq 0$ or 1 and the polynomial equation $f(\lambda) = \lambda^3 - \lambda^2 + 1 = 0$ is satisfied in $\mathrm{GF}(p)$. If $f(\lambda)$ has a root in $\mathrm{GF}(p)$, then this value of λ yields a solution in $\mathrm{GF}(p)$, and hence an idempotent model of the identity in $\mathrm{GF}(p)$. For example, $\lambda = 2$ yields an idempotent model in GF(5), while $\lambda = 4$ yields an idempotent model in GF(7). If $f(\lambda)$ does not have a root in $\mathrm{GF}(p)$, then there is an extension field $\mathrm{GF}(p^3)$ in which $f(\lambda)$ has a root, and this root yields an idempotent model in $\mathrm{GF}(p^3)$. For example, there are idempotent models in $\mathrm{GF}(2^3)$ and $\mathrm{GF}(3^3)$. In other words, there is an *idempotent* quasigroup satisfying $(yx \cdot y)y = x$ for orders 5, 7, 8 and 27. In actual fact, for all primes $p < 300$, it can readily be verified that $f(\lambda)$ has a root in $\mathrm{GF}(p)$ (and hence produces an idempotent model in $\mathrm{GF}(p)$) except for $p \in \{2, 3, 13, 29, 31, 47, 71, 73, 127, 131, 151, 163, 179, 193, 197, 233, 239, 257, 269, 277\}$. Our investigation will continue in subsequent sections.

Having found models of the two-variable quasigroup identity $u(x, y) = v(x, y)$ using finite fields (or finite near fields), one may recursively construct other models by various techniques. In what follows, we shall describe some of these techniques.

Let $(P, \cdot)$ and $(Q, *)$ be two quasigroups. On the set $P \times Q$ we can define a binary operation $\otimes$ as follows:

$$(p, x) \otimes (q, y) = (p \cdot q, x * y), \quad \text{if} \quad p, q \in P \quad \text{and} \quad x, y \in Q.$$

Then it is easy to see that $(P \times Q, \otimes)$ is a quasigroup, called the *direct product* of $(P, \cdot)$ and $(Q, *)$. The following result is fairly well-known and can be readily verified.

Theorem 2.2. *Let $(P, \cdot)$ and $(Q, *)$ be two quasigroups satisfying the identity $u(x, y) = v(x, y)$, where $|P| = m$ and $|Q| = n$. Then their direct product $(P \times Q, \otimes)$ is a quasigroup of order mn satisfying $u(x, y) = v(x, y)$. Moreover, if $(P, \cdot)$ and $(Q, *)$ are idempotent, so is $(P \times Q, \otimes)$.*

Example 2.3. Using the fact that there are idempotent quasigroups of orders 5, 7 and 8 satisfying the identity $(yx \cdot y)y = x$ (see Example 2.1), we can apply Theorem 2.2 to get idempotent models of $(yx \cdot y)y = x$ of orders $5^r \cdot 7^s \cdot 8^t$, where r, s, t are non-negative integers.

Our next construction is a generalized form of the above direct product construction for quasigroups, and it is originally due to Sade [63] who called it "produit direct-singulier". This construction was subsequently generalized and used extensively in various ways by C.C. Lindner (see, for example, [40–43]). We shall adapt the definition of Lindner in the description which follows.

Let $(V, \cdot)$ be an idempotent quasigroup and $(Q, *)$ a quasigroup containing a subquasigroup $(P, *)$. Let $\bar{P} = Q - P$ and let $(\bar{P}, \otimes)$ be a quasigroup, where $\otimes$ is not necessarily related to $*$. On the set $S = P \cup (\bar{P} \times V)$ define a binary operation $\oplus$ as follows:

(1) $p \oplus q = p * q$, if $p, q \in P$,

(2) $p \oplus (q, v) = (p * q, v)$, if $p \in P$, $q \in \bar{P}$,

(3) $(q, v) \oplus p = (q * p, v)$, if $p \in P$, $q \in \bar{P}$,

(4) $(p, v) \oplus (q, v) = p * q$, if $p * q \in P$
$= (p * q, v)$, if $p * q \in \bar{P}$

(5) $(p, v) \oplus (q, w) = (p \otimes q, v \cdot w)$, if $v \neq w$.

The quasigroup $(S, \oplus)$ so constructed is called the *singular direct product* of V and Q.

Unlike the direct product construction, two-variable quasigroup identities are not necessarily preserved by the singular direct product construction. However, C.C. Lindner [41] has obtained some fairly general results on identities which are preserved by the singular direct product for quasigroups. Before stating the result, we need to adapt some of the terminology used in [41]. Let $F(x, y)$ be the free groupoid on two generators x and y. The *components* of a word $w(x, y)$ of $F(x, y)$ are defined as follows:

(1) if the length of $w(x, y)$ is 1, the only component of $w(x, y)$ is $w(x, y)$, and

(2) if the length of $w(x, y)$ is greater than 1, the components of $w(x, y)$ are $w(x, y)$ itself and the components of $u(x, y)$ and $v(x, y)$, where $w(x, y) = u(x, y)v(x, y)$.

Let $(Q, \cdot)$ be any quasigroup (written multiplicatively) such that if $t(x, y) = t_1(x, y)t_2(x, y)$ is any component of $w(x, y)$ of length at least 2 and $a \neq b$ are any two elements of Q, then $t_1(a, b) \neq t_2(a, b)$. Such a quasigroup is called a *discrete* $w(x, y)$*-quasigroup*. If $(Q, \cdot)$ is a discrete $w(x, y)$ and $v(x, y)$-quasigroup and satisfies the identity $w(x, y) = v(x, y)$, we call $(Q, \cdot)$ a *discrete* $w(x, y) = v(x, y)$*-quasigroup*. We now state:

Theorem 2.4 (C.C. Lindner [41]). *Let $(V, \cdot)$ be a discrete $w(x, y) = v(x, y)$-idempotent quasigroup. Further let $(Q, *)$ be a quasigroup satisfying $w(x, y) = v(x, y)$ and containing a subquasigroup $(P, *)$. Let $\bar{P} = Q - P$ and suppose it is possible to define on $\bar{P}$ a binary operation $\otimes$ (not necessarily related to $*$) so that*

$(\bar{P}, \otimes)$ is a quasigroup satisfying $w(x, y) = v(x, y)$. Then the singular direct product $(S, \oplus)$ of V and Q defined above satisfies the identity $w(x, y) = v(x, y)$. Moreover, if $|V| = v$, $|Q| = q$, $|P| = p$ and $|\bar{P}| = q - p$, then $|S| = v(q - p) + p$.

We wish to remark, as Lindner himself has pointed out, that in the statement of Theorem 2.4 only the quasigroup $(V, \cdot)$ need be idempotent and also $(V, \cdot)$ is the only quasigroup that is required to be a discrete $w(x, y) = v(x, y)$-quasigroup. Of course, if $(Q, *)$ is an idempotent quasigroup, then the singular direct product $(S, \oplus)$ of V and Q will also be an idempotent quasigroup.

Example 2.5. Let $(V, \cdot)$ be an idempotent quasigroup of order 7 satisfying the identity $(yx \cdot y)y = x$. Let $(Q, *)$ be an idempotent quasigroup of order 5 satisfying the identity $(yx \cdot y)y = x$ based on the set $Q = \{1, 2, 3, 4, 5\}$. Let $P = \{5\}$ and on $\bar{P} = Q - P = \{1, 2, 3, 4\}$ define the binary operation $\otimes$ using the multiplication table given below.

$\otimes$	1	2	3	4
1	1	3	4	2
2	3	1	2	4
3	4	2	1	3
4	2	4	3	1

Now it is readily checked that $(\bar{P}, \otimes)$ is a quasigroup of order 4 satisfying the identity $(yx \cdot y)y = x$. It is also easy to verify that $(V, \cdot)$ is an idempotent *discrete* $(yx \cdot y)y = x$ quasigroup and the singular direct product $(S, \oplus)$ of V and Q is an *idempotent* quasigroup of order $29 = 7(5 - 1) + 1$ satisfying $(yx \cdot y)y = x$. Note that this is an addition to the list given in Example 2.1, where constructions using finite fields were used.

While the direct product and singular direct product constructions are useful tools in the construction of quasigroups satisfying two-variable identities, it is fairly obvious that there are limitations with respect to their ability to determine the spectrum. In general, the most effective recursive method of construction in investigating the spectra of two-variable quasigroup identities makes use of the concept of pairwise balanced designs (PBDs) and related combinatorial designs. In what follows, we shall describe the techniques involved. However, the interested reader may wish to refer to [16, 33, 71] for more detailed results on PBDs and related designs.

Definition 2.6. Let K be a set of positive integers. A *pairwise balanced design* (*PBD*) of index unity $B(K, 1; v)$ is a pair $(X, \mathbb{B})$ where X is a v-set (of *points*) and $\mathbb{B}$ is a collection of subsets of X (called *blocks*) with sizes from K such that every pair of distinct points of X is contained in exactly one block of $\mathbb{B}$. The number $|X| = v$ is called the *order* of the PBD.

Now let $(Q, \mathbb{B})$ be a PBD $B(K, 1; v)$ and for each block $B \in \mathbb{B}$ let $\circ(B)$ be a binary operation on B so that $(B, \circ(B))$ is an idempotent quasigroup. Define a binary operation $(\cdot)$ on Q by $x \cdot x = x$ for all $x \in Q$, and $x \cdot y = x \circ(B)\, y$, where $x \neq y$ and B is the unique block in $\mathbb{B}$ containing x and y. It is well-known and easy to see that $(Q, \cdot)$ is an idempotent quasigroup of order v (see [71]). More important is the fact that PBDs can be used to investigate the spectrum of certain collections of two-variable quasigroup identities. The following theorem is now well-known (see, for example, [28, 31, 66]) and has been used quite extensively.

Theorem 2.7. *Let V be a variety (more generally universal class) of algebras which is idempotent and which is based on two-variable identities. Suppose that there is a PBD $B(K, 1; v)$ such that for each block of size $k \in K$ there is a model of V of order k, then there is a model of V of order v.*

We shall denote by $B(K)$ the set of all integers v for which there exists a PBD $B(K, 1; v)$. We briefly denote by $B(k_1, k_2, \ldots, k_r)$ the set of all integers v for which there is a PBD $B(\{k_1, k_2, \ldots, k_r\}, 1; v)$. A set K is said to be *PBD-closed* if $B(K) = K$. R.M. Wilson's remarkable theory concerning the structure of PBD-closed sets (see [72–74]) often provides us with some form of asymptotic results in the following theorem.

Theorem 2.8 (R.M. Wilson [72–74]). *Let K be a set of positive integers and define the two parameters*:

$$\alpha(K) = g \cdot c \cdot d\{k - 1 : k \in K\},$$

$$\beta(K) = g \cdot c \cdot d\{k(k - 1) : k \in K\}.$$

Then there exists a constant C (depending on K) such that, for all integers $v > C$, $v \in B(K)$ if and only if $v - 1 \equiv 0 \pmod{\alpha(K)}$ and $v(v - 1) \equiv 0 \pmod{\beta(K)}$.

Example 2.9. Using finite fields in Example 2.1, we constructed idempotent quasigroups of orders 5, 7 and 8 satisfying the identity $(yx \cdot y)y = x$. If we let $K = \{5, 7, 8\}$ in Theorem 2.8, then $\alpha(K) = 1$ and $\beta(K) = 2$, and consequently the theorem guarantees $v \in B(5, 7, 8)$ for *all sufficiently large values of v*. Theorem 2.7 then further guarantees the existence of idempotent quasigroups satisfying $(yx \cdot y)y = x$ for all sufficiently large orders, where the term "sufficiently large" is unspecified.

As already mentioned, the identity $(yx \cdot y)y = x$ does not imply the idempotent identity $x^2 = x$. Consequently, while Theorem 2.7 usually has a dramatic effect in investigating the spectrum of certain collections of two-variable identities, the requirement that the variety V be idempotent is a definite drawback in some cases. To get around this, we sometimes use the notion of a *group divisible design* (GDD).

Definition 2.10. Let K and M be sets of positive integers. A *group divisible design* (GDD) $GD(K, 1, M; v)$ is a triple $(X, \mathbb{G}, \mathbb{B})$, where

(i) X is a v-set (of *points*),
(ii) $\mathbb{G}$ is a collection of non-empty subsets of X (called *groups*) with sizes in M and which partition X,
(iii) $\mathbb{B}$ is a collection of subsets of X (called *blocks*), each with size at least two in K,
(iv) no block meets a group in more than one point, and
(v) each pairset $\{x, y\}$ of points not contained in a group is contained in exactly one block.

The *group-type* (or *type*) of the GDD $(X, \mathbb{G}, \mathbb{B})$ is the multiset $\{|G| : G \in \mathbb{G}\}$ and we usually use the "exponential" notation for its description: a group-type $1^i 2^j 3^k \cdots$ denotes i occurrences of groups of size 1, j occurrences of groups of size 2, and so on.

Now let $(Q, \mathbb{G}, \mathbb{B})$ be a GDD $GD(K, 1, M; v)$ and for each group $G \in \mathbb{G}$ let $\circ(G)$ be a binary operation on G so that $(G, \circ(G))$ is a quasigroup (not necessarily idempotent). Further, for each block $B \in \mathbb{B}$, let $\circ(B)$ be a binary operation on B so that $(B, \circ(B))$ is an idempotent quasigroup. Define on Q the binary operation $(*)$ by $x * y = x \circ(G) y$ if x and y belong to the group $G \in \mathbb{G}$ (in particular, $x * x = x \circ(G) x$ for all $x \in Q$, where G is the group in $\mathbb{G}$ containing x), and $x * y = x \circ(B) y$, if $x \neq y$ and the pairset $\{x, y\}$ belongs to the block $B \in \mathbb{B}$. It is readily checked that $(Q, *)$ is a quasigroup of order v (cf. [71]). Unfortunately, this construction of quasigroups using GDDs does not necessarily preserve two-variable identities as C.C. Lindner has pointed out in [44]. However, Lindner [44] (see also Ganter [31]) for a generalization) was able to use the concept of a discrete model of a two-variable identity to obtain the following result.

Theorem 2.11. *Let $(Q, \mathbb{G}, \mathbb{B})$ be a GDD and $(Q, *)$ a quasigroup constructed from $(Q, \mathbb{G}, \mathbb{B})$ such that the quasigroup $(G, \circ(G))$ constructed on each group G in $\mathbb{G}$ satisfies the identity $u(x, y) = v(x, y)$ and the quasigroup $(B, \circ(B))$ constructed for each block B in $\mathbb{B}$ is an idempotent discrete model of $u(x, y) = v(x, y)$. Then the quasigroup $(Q, *)$ satisfies the identity $u(x, y) = v(x, y)$.*

We wish to remark that in the statement of Theorem 2.11 only the quasigroups $(B, \circ(B))$ defined on the blocks of $\mathbb{B}$ need be discrete models of the identity $u(x, y) = v(x, y)$, and that the quasigroups $(G, \circ(G))$ defined on the groups of $\mathbb{G}$

need only satisfy the identity $u(x, y) = v(x, y)$. We also have the following easy generalization of Theorem 2.11, which is a GDD analog of the singular direct product construction result in Theorem 2.4.

Theorem 2.12. *Let $(X, \mathbb{G}, \mathbb{B})$ be a GDD $GD(K, 1, M; v)$ and let P be a set of order p disjoint from X. Suppose for each block B in $\mathbb{B}$ it is possible to define a binary operation $\circ(B)$ on B so that $(B, \circ(B))$ is an idempotent discrete model of the identity $u(x, y) = v(x, y)$. Also suppose that for each group G in $\mathbb{G}$, there is a binary operation $\circ(G_p)$ on the set $G \cup P$ which converts it into a $u(x, y) = v(x, y)$-quasigroup containing P as a common subquasigroup. Then there exists a quasigroup $(X \cup P, *)$ of order $v + p$ satisfying the identity $u(x, y) = v(x, y)$.*

Proof. We define the operation $(*)$ on $X \cup P$ as follows:

(1) $x * y = x \circ(B) y$, if $x \neq y$ and the pairset $\{x, y\}$ is contained in the block $B \in \mathbb{B}$;

(2) $x * y = x \circ(G_P) y$, if $x, y \in G$, or $x \in G$ and $y \in P$, or $x \in P$ and $y \in G$, where $G \in \mathbb{G}$;

(3) $x * y = x \cdot y$, if $x, y \in P$ and $(P, \cdot)$ is a quasigroup satisfying the identity $u(x, y) = v(x, y)$.

The verification that $(X \cup P, *)$ is a quasigroup satisfying $u(x, y) = v(x, y)$ is fairly straightforward. □

The following theorem is a slight modification of Theorem 2.12 and its proof is very similar.

Theorem 2.13. *Let $(X, \mathbb{G}, \mathbb{B})$ be a GDD $GD(K, 1, M; v)$ and let P be a set of order p disjoint from X. Suppose that for each block B in $\mathbb{B}$ it is possible to define a binary operation $\circ(B)$ on B so that $(B, \circ(B))$ is an idempotent discrete model of the identity $u(x, y) = v(x, y)$. Suppose that $\mathbb{G} = \{G_1, G_2, \ldots, G_m\}$ and for each group G_i, $i = 1, 2, \ldots, m-1$, there is a binary operation $\circ(G_{iP})$ on the set $G_i \cup P$ which converts it into a $u(x, y) = v(x, y)$-quasigroup containing P as a common subquasigroup. Further suppose that there is a binary operation $(\cdot)$ on the set $G_m \cup P$ which converts it into a $u(x, y) = v(x, y)$-quasigroup. Then there exists a quasigroup $(X \cup P, *)$ of order $v + p$ satisfying the identity $u(x, y) = v(x, y)$.*

Proof. We define the operation $(*)$ on $X \cup P$ as follows:

(1) $x * y = x \circ(B) y$, if $x \neq y$ and the pairset $\{x, y\}$ is contained in the block $B \in \mathbb{B}$;

(2) $x * y = x \circ(G_{iP}) y$, if $x, y \in G_i$, or $x \in G_i$ and $y \in P$, or $x \in P$ and $y \in G_i$, where $i = 1, 2, \ldots, m-1$.

(3) $x * y = x \cdot y$, if $x, y \in G_m \cup P$.

Then $(X \cup P, *)$ is a quasigroup satisfying $u(x, y) = v(x, y)$. □

3. Quasigroup identities and orthogonal arrays

As we have already mentioned, some of the identities listed in Proposition 1.3 have been used in the construction and description of orthogonal arrays with interesting conjugacy properties. Indeed, the most conclusive results we have to date regarding the spectra of short conjugate orthogonal identities pertain to those identities associated with certain classes of $n^2 \times 4$ orthogonal arrays. In this section, we shall give only a brief summary of the known results concerning the identities (1), (2) and (3) of Proposition 1.3, and the reader may consult the references for more details. Henceforth, we let $J(u(x, y) = v(x, y))$ denote the spectrum of the identity $u(x, y) = v(x, y)$.

Quasigroups satisfying the identity $xy \cdot yx = x$, called the *Schröder identity*, are known to be self-orthogonal and a necessary condition for $n \in J(xy \cdot yx = x)$ is $n \equiv 0$ or $1 \pmod 4$. Several authors investigated $J(xy \cdot yx = x)$ including D.A. Norton and S.K. Stein [58], S.K. Stein [66], R.D. Baker [1], C.C. Lindner, N.S. Mendelsohn and S.R. Sun [47]. The most conclusive result was obtained by Lindner, Mendelsohn and Sun in the following theorem.

Theorem 3.1 (Lindner, Mendelsohn and Sun [47]). *$J(xy \cdot yx = x)$ contains precisely the set of all positive integers $n \equiv 0$ or $1 \pmod 4$ except $n = 5$, and possibly excepting $n = 12$ and 21.*

More recently, C.J. Colbourn and D.R. Stinson [23] have proved the following:

Theorem 3.2. *There exists an idempotent Schröder quasigroup of order n for all positive integers $n \equiv 0$ or $1 \pmod 4$ except $n = 5$ and 9, and possibly excepting $n = 12, 24, 33, 45, 69, 105, 117$.*

Combining Theorems 3.1 and 3.2, we now have

Theorem 3.3. *$J(xy \cdot yx = x)$ contains precisely the set of all positive integers $n \equiv 0$ or $1 \pmod 4$ except $n = 5$, and possibly excepting $n = 12$.*

From the results of [47], we are able to use Theorem 3.3 to determine that the spectrum of $n^2 \times 4$ orthogonal arrays having K_4 (the Klein 4-group) as conjugate invariant subgroup contains precisely the same set of values of n given in Theorem 3.3. This result also applies to the spectrum of Latin squares which have simultaneously the properties of being orthogonal to their transposes and have the Weisner property (see [47] for more details).

A quasigroup satisfying the identity $yx \cdot xy = x$, called *Stein's third law*, is known to be self-orthogonal. Moreover, a necessary condition for $n \in J(yx \cdot xy = x)$ is $n \equiv 0$ or $1 \pmod 4$. In [48], Lindner, Mullin and Hoffman established a correspondence between quasigroups satisfying the identity $yx \cdot xy = x$ and $n^2 \times 4$ orthogonal arrays having C_4 (the cyclic group of order 4) as conjugate invariant subgroup (briefly denoted by COA in [48]). They essentially proved:

Theorem 3.4 (Lindner, Mullin and Hoffman [48]). *$J(yx \cdot xy = x)$ contains precisely the set of all positive integers $n \equiv 0$ or $1 \pmod 4$ except possibly $n = 12$ and 48.*

However, the possible exception $n = 48$ can now be removed and we can obtain the following theorem.

Theorem 3.5. *$J(yx \cdot xy = x)$ contains precisely the set of all positive integers $n \equiv 0$ or $1 \pmod 4$ except possibly $n = 12$.*

Proof. We need only remove the possible exception $n = 48$ from Theorem 3.4. First of all, the result of Brouwer [20] can be used to establish the existence of a $\{5\}$-GDD of group-type 8^6 (see, for example, [67, Example 3.4]). If v is a prime power and $v \equiv 1 \pmod 4$, then [48, Lemma 6.6] guarantees the existence of an *idempotent* quasigroup of order v satisfying the identity $yx \cdot xy = x$. Thus in particular, we can define an idempotent *discrete* model of the identity $yx \cdot xy = x$ on the blocks of size 5 of the above mentioned GDD, and on each group of order 8, we define a model of $yx \cdot xy = x$. We then apply Theorem 2.11 to get $48 \in J(yx \cdot xy = x)$. Alternatively, we may use the $\{5\}$-GDD of group-type 8^6 and apply the result contained in [48, Lemma 6.5]. □

We wish to remark that, apart from COAs, there are some correspondences between *idempotent* models of $yx \cdot xy = x$ and other types of combinatorial structures (see, for example, [1, 51]). Note that the identity $(x \cdot yx)y = x$ ((iii) of Theorem 1.2), which was studied by N.S. Mendelsohn in [51]), is conjugate equivalent to the identity $yx \cdot xy = x$. Obviously, $J((x \cdot yx)y = x) = J(yx \cdot xy = x)$. In this connection, it is worth mentioning that the combined result of Bennett [5] and the more recent result of Zhang [75] on $(v, 4, 1)$-perfect Mendelsohn designs establishes the following:

Theorem 3.6. *There exists an idempotent quasigroup of order n satisfying Stein's third law for all positive integers $n \equiv 0$ or $1 \pmod 4$ except $n = 4$, and possibly excepting $n = 8, 12, 33$.*

Remark. K. Heinrich [private communication] has informed the author that an exhaustive computer search established the non-existence of a $(8, 4, 1)$-perfect Mendelsohn design. Hence, $n = 8$ is a definite exception in Theorem 3.6.

In [3], the author established a correspondence between quasigroups satisfying the identity $(xy \cdot y)y = x$ and $n^2 \times 4$ orthogonal arrays having C_3 (the cyclic group of order 3) as conjugate invariant subgroup. As a corollary to the results contained in [48, Theorem 5.1], the following result was obtained.

Theorem 3.7 (Bennett [3]). *$J((xy \cdot y)y = x)$ contains precisely the set of all positive integers $n \equiv 0$ or $1 \pmod 3$ except $n = 6$.*

A quasigroup satisfying the identity $(xy \cdot y)y = x$ is known to be $(3, 2, 1)$-conjugate orthogonal. Also, idempotent models of $(xy \cdot y)y = x$ correspond to a class of resolvable Mendelsohn triple systems (see, for example, [10]). It was also shown [3] that idempotent models of $(xy \cdot y)y = x$ exist only for orders $n \equiv 1 \pmod 3$.

4. Stein quasigroups

A quasigroup satisfying the identity $x \cdot xy = yx$ is called a *Stein quasigroup*. Stein quasigroups are necessarily idempotent and self-orthogonal. The Stein identity $x \cdot xy = yx$ ((4) of Proposition 1.3) is perhaps the most extensively studied of the two-variable identities listed in Proposition 1.3. Following S.K. Stein's original interest in the identity in 1957 (see [65]), several authors have given it a considerable amount of attention (see, for example, [11, 27, 40, 51, 59, 60, 65, 66]). Stein had hoped to use quasigroups satisfying the constraint $x \cdot xz = y \cdot yz$ implies $x = y$ to construct counter-examples to the Euler conjecture concerning orthogonal Latin squares. Obviously, a quasigroup satisfying the identity $x \cdot xy = yx$ became a suitable candidate for his investigation. However, most of the current results we have relating to the spectrum $J(x \cdot xy = yx)$ came long after the disproof of the Euler conjecture and, in fact, after the spectrum for self-orthogonal Latin squares was determined to contain all positive integers $n \neq 2, 3$ or 6 (see [17]). Undoubtedly, Stein quasigroups are of special interest in their own right. Stein [65] and Mendelsohn [51] used Galois fields to show that $J(x \cdot xy = yx)$ contained all positive integers of the form $4^k m$, where the square-free part of m does not contain any prime $p \equiv 2$ or $3 \pmod 5$. Later on, Stein [66] used BIBDs to show that the spectrum contained all numbers of the form $12k + 1$, $12k + 4$, $20k + 1$, and $20k + 5$. Lindner [40] further enlarged the spectrum by using the singular direct product construction. In two subsequent papers [59, 60], Pelling and Rogers showed that if $n \in \{2, 3, 6, 7, 8, 10, 12, 14\}$, then $n \notin J(x \cdot xy = yx)$ and they used PBDs in conjunction with the singular direct product to show that $n \in J(x \cdot xy = yx)$ for all $n > 1042$. This bound was later improved by Bennett and Mendelsohn in [11]. The main result was established on the basis of the following two lemmas.

Lemma 4.1. *$B(4, 5, 9, 11, 19, 31) \subseteq J(x \cdot xy = yx)$.*

Lemma 4.2 (see [11, Theorems 4.3–4.6, 4.8–4.10]). *If* $v \geq 4$ *and* $v \notin \{6, 7, 8, 10, 12, 14, 15, 18, 22, 23, 26, 27, 30, 34, 35, 38, 39, 42, 43, 46, 50, 54, 62, 66, 70, 74, 78, 82, 90, 98, 102, 106, 110, 114, 126, 130, 142, 158, 162, 174, 178, 190\}$, *then* $v \in B(4, 5, 9, 11, 19, 31)$.

Theorem 4.3 (Bennett and Mendelsohn [11]). $v \in J(x \cdot xy = yx)$ *holds for all positive integers* v *except* $v \in \{2, 3, 6, 7, 8, 10, 12, 14\}$ *and possibly excepting* $v \in \{15, 18, 22, 23, 26, 27, 30, 34, 35, 38, 39, 42, 43, 46, 50, 54, 62, 66, 70, 74, 78, 82, 90, 98, 102, 106, 110, 114, 126, 130, 142, 158, 162, 174, 178, 190\}$.

In [8] the author improved the result of Lemma 4.2 and obtained the following theorem:

Theorem 4.4. *For all integers* $v \geq 4$, $v \in B(4, 5, 9, 11, 19, 31)$ *holds with the exception of* $v \in \{6, 7, 8, 10, 12, 14, 15, 18, 22, 23, 26, 27, 30, 34\}$ *and with the possible exception of* $v \in \{38, 42, 43, 46, 50, 54, 62, 66, 70, 74, 78, 82, 90, 98, 102, 114, 126\}$.

As a consequence of Lemma 4.1 and Theorem 4.4, we readily obtain the following improvement of Theorem 4.3.

Theorem 4.5. $v \in J(x \cdot xy = yx)$ *holds for all positive integers* v *except* $v \in \{2, 3, 6, 7, 8, 10, 12, 14\}$ *and possibly excepting* $v \in \{15, 18, 22, 23, 26, 27, 30, 34, 38, 42, 43, 46, 50, 54, 62, 66, 70, 74, 78, 82, 90, 98, 102, 114, 126\}$.

The result of Theorem 4.4 also allows us to enlarge the spectrum of certain classes of Stein systems (see [11, 59, 60]). If a Stein system S contains a proper subsystem T, then it is known that $|S| \geq 3|T| + 1$ (see, for example, [60]). The case where equality holds is of special interest. If, as in [11, 59], we write $Q(n)$ whenever there is a Stein system of order n which is a subsystem of one of order $3n + 1$, then we have the following improvement of results contained in [11, 59].

Theorem 4.6. *If* $n \equiv 1 \pmod 3$, *then* $Q(n)$ *holds for all* $n \geq 4$ *except* $n = 7, 10$ *and possibly excepting* $n \in \{22, 34, 43, 46, 70, 82\}$.

Proof. We need only remove the possible exceptions $n = 106, 130, 142, 178, 190$ from [11, Theorem 5.1]. We now use the fact that, if $k > 1$, then $9k + 4 \in B(4, (3k + 1)^*)$ holds from [18, Lemma 7]. Combining this with the fact that we have $\{106, 130, 142, 178, 190\} \subseteq J(x \cdot xy = yx)$, we get the desired result with $k \in \{35, 43, 47, 59, 63\}$ and an application of Theorem 2.7. □

An *extended medial Stein system* is a Stein system with the property that every 2-element generated subsystem satisfies the medial law $(xy)(zt) = (xz)(yt)$.

Extended medial Stein systems were originally investigated by Pelling and Rogers [59, 60] and later studied in [11]. Since it is known that a medial Stein system of order n exists for $n \in \{4, 5, 9, 11, 19, 31\}$, we can use the result of Theorem 4.4 to further improve that contained in [11, Theorem 5.2]. We essentially have the following theorem.

Theorem 4.7. *An extended medial Stein system of order n exists for all integers $n \geq 4$ except $n \in \{6, 7, 8, 10, 12, 14\}$ and possibly excepting $n \in \{15, 18, 22, 23, 26, 27, 30, 34, 38, 42, 43, 46, 50, 54, 62, 66, 70, 74, 78, 82, 90, 98, 102, 114, 126\}$.*

Remark. D.G. Rogers [private communication] has recently shown that there is no Stein quasigroup of order 18. Hence, 18 is an exception in both Theorems 4.5 and 4.7.

5. The spectrum of $(yx \cdot y)y = x$ and Mendelsohn designs

We have already seen in the proof of Proposition 1.3 that the identity $(yx \cdot y)y = x$ is equivalent to $(y \cdot xy)y = x$, and it is also conjugate equivalent to the identities $(y \cdot yx)y = x$ and $(yx \cdot x)y = x$. Consequently, the spectrum of each of these identities ((vi), (vii), (viii), and (ix) of Theorem 1.2) is the same. A quasigroup satisfying the identity $(yx \cdot y)y = x$ has the interesting property of being orthogonal to its (2, 3, 1)-, (3, 1, 2)-, and (3, 2, 1)-conjugate. In particular, *idempotent* models of $(yx \cdot y)y = x$ can be associated with a class of resolvable Mendelsohn designs which we briefly describe below. For more details, the reader is referred to [5, 6, 10, 36, 37, 51–53].

A $(v, K, 1)$-*Mendelsohn design* (briefly $(v, K, 1)$-MD) is a pair $(X, \mathbb{B})$, where X is a v-set (of *points*) and $\mathbb{B}$ is a collection of cyclically ordered subsets of X (called *blocks*) with sizes in the set K such that every ordered pair of points of X are consecutive in exactly one block of $\mathbb{B}$.

If $(X, \mathbb{B})$ is a $(v, K, 1)$-MD with $X = \{1, 2, \ldots, v\}$ and $K = \{k_1, k_2, \ldots, k_s\}$, where $\sum_{1 \leq i \leq s} k_i = v - 1$, then $(X, \mathbb{B})$ is called *loosely resolvable* if its blocks can be separated into v parallel classes such that the set theoretic union of the elements in the blocks of the jth parallel class is $X - \{j\}$. If each parallel class contains one block of each of the sizes $k_1, k_2, \ldots, k_s$, then $(X, \mathbb{B})$ is called *precisely resolvable.* The $(v, K, 1)$-MD is called *r-fold perfect* if each ordered pair of points of X appears t-apart in exactly one block of $\mathbb{B}$ for all $t = 1, 2, \ldots, r$. If $K = \{k\}$ and $r = k - 1$, the design is called *perfect.*

Let $|Q| = v$ and suppose $(Q, \cdot)$ is an *idempotent* quasigroup satisfying $(yx \cdot y)y = x$. Then $(Q, \cdot)$ will be orthogonal to its (3, 2, 1)-conjugate, say $(Q, *)$. We can then define the blocks of a 2-fold perfect loosely resolvable $(v, K, 1)$-MD as follows. For the block containing a of the xth parallel class, the right-hand neighbour of a is $a \cdot x$ and the left-hand neighbour of a is $a * x$. This construction produces well-defined blocks of size $k \geqslant 3$ in K and it can be verified that the resulting design is a 2-fold perfect loosely resolvable $(v, K, 1)$-MD (see, for example, [5, 37]).

In Example 2.9, we are essentially guaranteed the existence of a constant C such that for all $n > C$, there exists an *idempotent* quasigroup of order n satisfying the identity $(yx \cdot y)y = x$. In [9], the author carried out an investigation of $J((yx \cdot y)y = x)$ with some emphasis on finding a concrete upper bound for the constant C. Example 2.1 was employed in conjunction with the recursive constructions of Section 2 and the notion of a quasigroup with "holes" (see, for example, [13, 14, 25]). The main result of [9] pertaining to the spectrum of the identity $(yx \cdot y)y = x$ can be summarized in the following theorems:

Theorem 5.1. *For every integer $n \geqslant 1$ with the exception of $n = 2, 3, 4, 6$, and the possible exception of $n \in \{9, 10, 12, 13, 14, 15, 16, 18, 20, 22, 24, 26, 28, 30, 34, 38, 39, 42, 44, 46, 51, 52, 58, 60, 62, 66, 68, 70, 72, 74, 75, 76, 86, 87, 90, 94, 96, 98, 99, 100, 102, 106, 108, 110, 114, 116, 118, 122, 132, 142, 146, 154, 158, 164, 170, 174\}$, there exists an idempotent quasigroup of order n satisfying the identity $(yx \cdot y)y = x$.*

Theorem 5.2. *$J((yx \cdot y)y = x)$ contains every integer $n \geqslant 1$ with the exception of $n = 2, 6$, and possibly excepting $n = 10, 14, 18, 26, 30, 38, 42, 158$.*

6. Miscellaneous results and summary

In the preceding sections of this paper, we have been able to present fairly conclusive results regarding the spectrum of most of the identities listed by Trevor Evans in Theorem 1.2. However, the last three identities of Proposition 1.3 remain to be investigated, namely, (6) $(xy \cdot x)y = x$ ((v) of Theorem 1.2), (7) $xy \cdot y = x \cdot xy$ ((xii) of Theorem 1.2), and (8) $yx \cdot y = x \cdot yx$ ((xiv) of Theorem 1.2). For the most part, the current results on the spectrum of each of these identities are still somewhat inconclusive, and we shall provide only a brief summary in this section.

Lemma 6.1. *Each of the identities in $\{(xy \cdot x)y = x,\ xy \cdot y = x \cdot xy,\ yx \cdot y = x \cdot yx\}$ implies the idempotent law.*

Proof. We first consider the identity $(xy \cdot x)y = x$. If $(xy \cdot x)y = x$ holds, then, replacing x by xy, we obtain $(((xy)y)(xy))y = xy$ which implies $((xy)y)(xy) = x$. On the other hand, $((x(xy))x)(xy) = x$ also holds. Hence we have $((x(xy))x)(xy) = ((xy)y)(xy)$ and, by cancellation, $(x(xy))x = (xy)y$ holds. In particular, we must have $(x(x^2))x = (x^2)x$ which implies $x \cdot x^2 = x^2$, which further implies $x^2 = x$. Next, we consider the identity $xy \cdot y = x \cdot xy$. If $xy \cdot y = x \cdot xy$ holds, then $ay = a$

implies that $a^2 = a \cdot ay = ay \cdot y = ay = a$. Finally, we consider the identity $yx \cdot y = x \cdot yx$. If $yx \cdot y = x \cdot yx$ holds, then $ax = a$ implies that $a^2 = ax \cdot a = x \cdot ax = xa$ which, by cancellation, implies $a = x$, that is, $a^2 = a$. This completes the proof of the lemma. $\square$

In what follows, we shall make use of a result due to Mullin et al. [56].

Lemma 6.2. *A* $B(\{5, 9, 13, 17, 29, 49\}, 1; v)$ *exists for all positive integers* $v \equiv 1 \pmod 4$ *with the possible exception of* $v = 33, 57, 93, 133$.

A quasigroup satisfying the identity $(xy \cdot x)y = x$ is $(3, 2, 1)$-conjugate orthogonal and, moreover, the identity itself is $(3, 2, 1)$-conjugate invariant. Consequently, *any* quasigroup of order v satisfying the identity $(xy \cdot x)y = x$ can always be associated with some 2-fold perfect loosely resolvable $(v, K, 1)$-MD as described in the previous section. There are models of the identity $(xy \cdot x)y = x$ in $\mathrm{GF}(q)$ for all prime powers $q \equiv 1 \pmod 4$. In particular, there are models of the identity of order n, where $n \in \{5, 9, 13, 17, 29, 49\}$. By using the result of Lemma 6.2 and applying Theorem 2.7, we readily obtain the following result.

Theorem 6.3. $J((xy \cdot x)y = x)$ *contains all positive integers* $v \equiv 1 \pmod 4$, *except possibly* $v = 33, 57, 93,$ *and* 133.

It is still an open problem to determine more precisely $J((xy \cdot x)y = x)$. It is not difficult to check that 2, 3, 4, and 6 do not belong to $J((xy \cdot x)y = x)$.

The identity $xy \cdot y = x \cdot xy$ is conjugate invariant, and a quasigroup satisfying this identity is $(3, 2, 1)$- and $(1, 3, 2)$-conjugate orthogonal. Hence these quasigroups can be associated with 2-fold perfect loosely resolvable Mendelsohn designs. There are models of the identity $xy \cdot y = x \cdot xy$ in $\mathrm{GF}(2^k)$ for all $k \geqslant 2$. In particular, there are models of the identity of orders 4 and 8. If we utilize a result of Hanani [33], we readily obtain models of the identity of all orders $v \equiv 1$ or $4 \pmod{12}$, and, more generally, if we appeal to Wilson's result in Theorem 2.8 with $K = \{4, 8\}$, we easily obtain

Theorem 6.4. $J(xy \cdot y = x \cdot xy)$ *contains all sufficiently large integers* v, *where* $v \equiv 0$ *or* $1 \pmod 4$.

It can be shown that $J(xy \cdot y = x \cdot xy)$ does not contain 2, 3, 5, 6 or 7, and it is possible to be more specific about the term "sufficiently large" in Theorem 6.4. However, more conclusive results are being sought by the author.

Quasigroups satisfying the identity $yx \cdot y = x \cdot yx$ are $(3, 1, 2)$ (and $(2, 3, 1)$)-conjugate orthogonal, and there are models of the identity in $\mathrm{GF}(q)$ for all prime powers $q \equiv 1 \pmod 4$. Consequently, it is possible to obtain a result similar to that of Theorem 6.3, that is, we have

Theorem 6.5. *$J(yx \cdot y = x \cdot yx)$ contains all positive integers $v \equiv 1 \pmod 4$, except possibly $v = 33$, 57, 93 and 133.*

In summary, the author has attempted to provide an up to date account of what is known regarding the spectrum of each of the identities in Theorem 1.2. I would like to reiterate that only a brief survey of the known results is given in this paper. However, I have made a concerted effort to include many references to the earlier investigations in the bibliography, and the interested reader should find plenty of details therein.

Note added in proof. Since this paper was accepted for publication, the author has discovered the following:

(1) The quasigroup identities $(xy \cdot x)y = x$ and $yx \cdot y = x \cdot yx$, namely, (6) and (8), respectively, cf. Proposition 1.3, are conjugate-equivalent. Consequently, the spectrum is the same for each of these identities and the list of identities in Proposition 1.3 can further be reduced to seven.

(2) There exists a $(33, 4, 1)$-perfect Mendelsohn design and the possible exception $n = 33$ can be eliminated from Theorem 3.6.

(3) W.H. Mills has recently shown that $\{70, 82\} \subseteq B(4, 19^*)$. Consequently, the numbers 70 and 82 can be removed from the list of possible exceptions in Theorems 4.4, 4.5, 4.6 and 4.7.

References

[1] R.D. Baker, Quasigroups and tactical systems, Aequationes Math. 18 (1978) 296–303.

[2] F.E. Bennett, Latin squares with pairwise orthogonal conjugates, Discrete Math. 36 (1981) 117–137.

[3] F.E. Bennett, On a class of $n^2 \times 4$ orthogonal arrays and associated quasigroups, Congressus Numerantium 39 (1983) 117–122.

[4] F.E. Bennett, On conjugate orthogonal idempotent Latin squares, Ars Combinatoria 19 (1985) 37–50.

[5] F.E. Bennett, Congugate orthogonal Latin squares and Mendelsohn designs, Ars Combinatoria 19 (1985) 51–62.

[6] F.E. Bennett, On r-fold perfect Mendelsohn designs, Ars Combinatoria 23 (1987) 57–68.

[7] F.E. Bennett, Pairwise balanced designs with prime power block sizes exceeding 7, Annals Discrete Math. 34 (1987) 43–64.

[8] F.E. Bennett, Concerning pairwise balanced designs with prime power block sizes, Contemporary Math., to appear.

[9] F.E. Bennett, Quasigroup identities and Mendelsohn designs, Canad. J. Math., to appear.

[10] F.E. Bennett, E. Mendelsohn and N.S. Mendelsohn, Resolvable perfect cyclic designs, J. Combin. Theory (A) 29 (1980) 142–150.

[11] F.E. Bennett and N.S. Mendelsohn, On the spectrum of Stein quasigroups, Bull. Austral. Math. Soc. 21 (1980) 47–63.

[12] F.E. Bennett and N.S. Mendelsohn, Conjugate orthogonal Latin square graphs, Congressus Numerantium 23 (1979) 179–192.
[13] F.E. Bennett, Lisheng Wu and L. Zhu, Conjugate orthogonal Latin squares with equal-sized holes, Annals Discrete Math. 34 (1987) 65–80.
[14] F.E. Bennett, Lisheng Wu and L. Zhu, On the existence of COLS with equal-sized holes, Ars Combinatoria 26B (1988) 5–36.
[15] F.E. Bennett, Lisheng Wu and L. Zhu, Further results on incomplete (3, 2, 1)-conjugate orthogonal idempotent Latin squares, Discrete Math., to appear.
[16] Th. Beth, D. Jungnickel and H. Lenz, Design Theory (Bibliographisches Institut, Zurich, 1985).
[17] R.K. Brayton, D. Coppersmith and A.J. Hoffman, Self-orthogonal Latin squares of all orders $n \neq 2$, 3 or 6, Bull. Amer. Math. Soc. 80 (1974) 116–118.
[18] A.E. Brouwer, Optimal packings of K_4's into a K_n, J. Combin. Theory (A) 26 (1979) 278–297.
[19] A.E. Brouwer, The number of mutually orthogonal Latin squares – a table up to order 10000, Research Report ZW123/79, Mathematisch Centrum, Amsterdam, 1979.
[20] A.E. Brouwer, Four MOLS of order 10 with a hole of order 2, J. Statist. Planning and Inference 10 (1984) 203–205.
[21] A.E. Brouwer, H. Hanani and A. Schrijver, Group divisible designs with block-size four, Discrete Math. 20 (1977) 1–10.
[22] R.H. Bruck, What is a loop?, in: Studies in Modern Algebra, A.A. Albert, ed (Prentice-Hall, Englewood Cliffs, 1963).
[23] C.J. Colbourn and D.R. Stinson, Edge-coloured designs with block size four, Research Report CORR 87-25, July 1987.
[24] J. Dénes and A.D. Keedwell, Latin Squares and Their Applications (Academic Press, New York and London, 1974).
[25] J.H. Dinitz and D.R. Stinson, MOLS with holes, Discrete Math. 44 (1983) 145–154.
[26] D.A. Drake and J.A. Larson, Pairwise balanced designs whose line sizes do not divide six, J. Combin. Theory (A) 34 (1983) 266–300.
[27] T. Evans, Algebraic structures associated with Latin squares and orthogonal arrays, Proc. Conf. Algebraic Aspects of Combinatorics, Congressus Numerantium 13 (1975) 31–52.
[28] T. Evans, Universal-algebraic aspects of combinatorics, Proc. Internat. Conf. Universal Algebra, Janos Bolyai Math. Soc. (North-Holland, Amsterdam, 1980).
[29] T. Evans, Finite representations of two-variable identities or Why are finite fields important in combinatorics? Annals Discrete Math. 15 (1982) 135–141.
[30] T. Evans, private communication.
[31] B. Ganter, Combinatorial designs and algebras, Preprint Nr. 270, Technische Hochschule, Darmstadt, 1976.
[32] B. Ganter and H. Werner, Equational classes of Steiner systems, Algebra Universalis 5 (1975) 125–140.
[33] H. Hanani, Balanced incomplete block designs and related designs, Discrete Math. 11 (1975) 255–369.
[34] H. Hanani, D.K. Ray-Chaudhuri and R.M. Wilson, On resolvable designs, Discrete Math. 3 (1972) 343–357.
[35] J.D. Horton, Sub-Latin squares and incomplete orthogonal arrays, J. Combin. Theory (A) 16 (1974) 23–33.
[36] D.F. Hsu and A.D. Keedwell, Generalized complete mappings, neofields, sequenceable groups and block designs. II, Pacific J. Math. 117 (1985) 291–312.
[37] A.D. Keedwell, Circuit designs and Latin squares, Ars Combinatoria 17 (1984) 79–90.
[38] J.F. Lawless, Pairwise balanced designs and the construction of certain combinatorial systems, Proc. of the Second Louisiana Conf. on Combinatorics, Graph Theory, and Computing, Baton Rouge (1971) 353–366.
[39] C.C. Lindner, Quasigroup identities and orthogonal arrays, in: Surveys in Combinatorics, E.K. Lloyd, ed., London Math. Soc. Lecture Notes Ser. 82 (Cambridge Univ. Press, 1983) 77–105.
[40] C.C. Lindner, Construction of quasigroups satisfying the identity $x(xy) = yx$, Canad. Math. Bull. 14 (1971) 57–59.

[41] C.C. Lindner, Identities preserved by the singular direct product, Algebra Universalis 1 (1971) 86–89.
[42] C.C. Lindner, Identities preserved by the singular direct product II, Algebra Universalis 2 (1972) 113–117.
[43] C.C. Lindner, Construction of quasigroups using the singular direct product, Proc. Amer. Math. Soc. 29 (1971) 263–266.
[44] C.C. Lindner, Identities preserved by group divisible designs, unpublished manuscript.
[45] C.C. Lindner and E. Mendelsohn, On the conjugates of an $n^2 \times 4$ orthogonal array, Discrete Math. 20 (1977) 123–132.
[46] C.C. Lindner, E. Mendelsohn, N.S. Mendelsohn and B. Wolk, Orthogonal Latin square graphs, J. Graph Theory 3 (1979) 325–338.
[47] C.C. Lindner, N.S. Mendelsohn and S.R. Sun, On the construction of Schroeder quasigroups, Discrete Math. 32 (1980) 271–280.
[48] C.C. Lindner, R.C. Mullin and D.G. Hoffman, The spectra for the conjugate invariant subgroups of $n^2 \times 4$ orthogonal arrays, Canad. J. Math. 32 (1980) 1126–1139.
[49] C.C. Lindner and D. Steedly, On the number of conjugates of a quasigroup, Algebra Universalis 5 (1975) 191–196.
[50] H.F. MacNeish, Euler squares, Ann. Math. 23 (1922) 221–227.
[51] N.S. Mendelsohn, Combinatorial designs as models of universal algebras, in: Recent Progress in Combinatorics (Academic Press, New York and London, 1969) 123–132.
[52] N.S. Mendelsohn, A natural generalization of Steiner triple systems, in: Computers in Number Theory, A.O.L. Atkin and B.J. Birch, eds (Academic Press, New York, 1971) 323–338.
[53] N.S. Mendelsohn, Perfect cyclic designs, Discrete Math. 20 (1977) 63–68.
[54] N.S. Mendelsohn, Algebraic construction of combinatorial designs, Proc. Conf. Algebraic Aspects of Combinatorics, Congressus Numerantium 13 (1975) 157–168.
[55] R.C. Mullin, A generalization of the singular direct product with application to skew Room squares, J. Combin. Theory (A) 29 (1980) 306–318.
[56] R.C. Mullin, P.J. Schellenberg, S.A. Vanstone and W.D. Wallis, On the existence of frames, Discrete Math. 37 (1981) 79–104.
[57] R.C. Mullin and D.R. Stinson, Pairwise balanced designs with odd block sizes exceeding 5, Discrete Math., to appear.
[58] D.A. Norton and S.K. Stein, Cycles in algebraic systems, Proc. Amer. Math. Soc. 7 (1956) 999–1004.
[59] M.J. Pelling and D.G. Rogers, Stein quasigroups I: combinatorial aspects, Bull. Austral. Math. Soc. 18 (1978) 221–236.
[60] M.J. Pelling and D.G. Rogers, Stein quasigroups II: algebraic aspects, Bull. Austral. Math. Soc. 20 (1979) 321–334.
[61] K.T. Phelps, Conjugate orthogonal quasigroups, J. Combin. Theory (A) 25 (1978) 117–127.
[62] D.K. Ray-Chaudhuri and R.M. Wilson, Solution of Kirkman's schoolgirl problem, Amer. Math. Soc. Symp. Pure Math. 19 (1971) 187–203.
[63] A. Sade, Produit direct-singulier de quasigroupes orthogonaux et anti-abéliens, Ann. Soc. Sci. Bruxelles Sér. I 74 (1960) 91–99.
[64] E. Seiden, A method of construction of resolvable BIBD, Sankhya (A) 25 (1963) 393–394.
[65] S.K. Stein, On the foundations of quasigroups, Trans. Amer. Math. Soc. 85 (1957) 228–256.
[66] S.K. Stein, Homogeneous quasigroups, Pacific J. Math. 14 (1964) 1091–1102.
[67] D.R. Stinson, The equivalence of certain incomplete transversal designs and frames, Ars Combinatoria 22 (1986) 81–87.
[68] D.R. Stinson and L. Zhu, On the existence of MOLS with equal-sized holes, Aequationes Math. 33 (1987) 96–105.
[69] D.T. Todorov, Three mutually orthogonal Latin squares of order 14, Ars Combinatoria 20 (1985) 45–48.
[70] R.M. Wilson, Concerning the number of mutually orthgonal Latin squares, Discrete Math. 9 (1974) 181–198.

[71] R.M. Wilson, Constructions and uses of pairwise balanced designs, Mathematical Centre Tracts 55 (1974) 18–41.

[72] R.M. Wilson, An existence theory for pairwise balanced designs I, J. Combin. Theory (A) 13 (1972) 220–245.

[73] R.M. Wilson, An existence theory for pairwise balanced designs II, J. Combin. Theory (A) 13 (1972) 246–273.

[74] R.M. Wilson, An existence theory for pairwise balanced designs III, J. Combin. Theory (A) 18 (1975) 71–79.

[75] Zhang Xuebin, On the existence of $(v, 4, 1)$-PMD, Ars Combinatoria, to appear.

Discrete Mathematics 77 (1989) 51–53
North-Holland

NOTE

NEW CYCLIC (61, 244, 40, 10, 6) BIBDs

Elizabeth J. BILLINGTON
Department of Mathematics, University of Queensland, St. Lucia 4067, Australia

Dedicated to Haim Hanani on the occasion of his 75th birthday.

Design number 1115 in the list of BIBD parameters given by Mathon and Rosa [2] is listed as unknown; the parameters are (61, 244, 40, 10, 6). Using techniques of cyclotomy (see [4] for instance) the following four initial blocks were found, by hand, to generate such a design. The cyclotomic classes C_i, $0 \leqslant i \leqslant 11$, are with respect to $e = 12$; the primitive root used in GF[61] was 2. (The classes C_i were quickly obtained from Jacobi's tables [1].)

Initial blocks:

$$C_0 \cup C_1 = \{1, 9, 20, 58, 34, 2, 18, 40, 55, 7\},$$
$$C_3 \cup C_4 = \{8, 11, 38, 37, 28, 16, 22, 15, 13, 56\},$$
$$C_1 \cup C_3 = \{2, 18, 40, 55, 7, 8, 11, 38, 37, 28\},$$
$$C_4 \cup C_6 = \{16, 22, 15, 13, 56, 3, 27, 60, 52, 41\}.$$

Cyclotomic numbers of order 12 are known in general (Whiteman [5]). A check of Whiteman's Table 5 [5, page 72] shows that for *any* odd prime $p = 12f + 1$, f odd, where $p = A^2 + 3B^2 = x^2 + 4y^2$, with $m' \equiv 2 \pmod 4$, $c = 1$ and $m \equiv 1 \pmod 6$ (see [5]), provided

$$2A - B - 4y = 0 \tag{1}$$

and

$$3A + 2 - x - 6y = 0, \tag{2}$$

the four sets $C_0 \cup C_1$, $C_4 \cup C_6$, $C_1 \cup C_3$ and $C_3 \cup C_4$ form a supplementary difference set.

Since $A^2 + 3B^2 = x^2 + 4y^2$, we have from (1) and (2) that

$$\left(\frac{x-2}{3} + 2y\right)^2 + 3(\tfrac{2}{3}(x-2))^2 = x^2 + 4y^2,$$

which becomes $x^2 + x(3y - 13) + (13 - 6y) = 0$. Hence

$$x = \frac{13 - 3y \pm \sqrt{(3y-9)^2 + 36}}{2}, \text{ and so}$$

$$(3y - 9)^2 + 36 = n^2, \text{ say.} \tag{3}$$

Clearly n is divisible by 3; letting $n = 3M$ reduces (3) to

$$M^2 - (y-3)^2 = 4. \tag{4}$$

The only solution to (4) in integers is $M = \pm 2$ and $y = 3$; thus $n = \pm 6$ and $y = 3$, so that $x = 5$ or -1. Since $x \equiv 1 \pmod 4$, we have $x = 5$. Therefore $p = x^2 + 4y^2 = 25 + 4.9 = 61$, and so the prime 61 is an isolated case here.

Calling the four initial blocks (respectively) A, B, C and D, three of these at a time were taken, and a fourth initial block was generated by computer, using a program originally written by Peter Robinson [3]. The resulting designs were not always isomorphic, as was easy to check by investigating block intersection numbers. In this way 10 non-isomorphic cyclic designs were found with parameters (61, 244, 40, 10, 6). (See table.) There are probably many more than 10 cyclic designs with these parameters; the search was by no means exhaustive. Note that design number 10 contains 61 repeated blocks.

The existence of a design with parameters (61, 122, 20, 10, 3) (number 255 in [2]) remains open.

	Initial block										
A:	0	1	6	8	17	19	33	39	54	57	$=(C_0 \cup C_1) - 1$
B:	0	10	12	13	19	24	38	49	53	57	$=(C_4 \cup C_6) - 3$
C:	0	5	6	9	16	26	35	36	38	53	$=(C_1 \cup C_3) - 2$
D:	0	3	5	7	8	14	20	29	30	48	$=(C_3 \cup C_4) - 8$
E:	0	1	3	5	8	21	39	40	49	55	$D=(-E)+8$
F:	0	1	5	8	23	29	43	45	54	56	$A=(-F)+1$
G:	0	5	8	24	25	34	35	38	49	57	$=(C_3 \cup C_6) - 3$
H:	0	1	3	21	26	33	45	47	51	55	
J:	0	2	6	14	25	30	38	42	49	53	

Design number	*Initial blocks*
1	$ABCD$
2	$ABCE$
3	$BCDF$
4	$BCEF$
5	$ADGH$
6	$DFGH$
7	$AEGH$
8	$CDEJ$
9	$EFGH$
10	$CEEJ$

Note added in proof. All ten of the designs listed above appear to be irreducible, thanks to a program written by Peter J. Robinson.

References

[1] C.G.J. Jacobi, Canon Arithmeticus (Akademie-Verlag, Berlin, 1956).
[2] R. Mathon and A. Rosa, Tables of parameters of BIBDs with $r \leqslant 41$ including existence, enumeration, and resolvability results, Annals Discrete Math. 26 (1985) 275–308.
[3] P.J. Robinson, private communication (1983).
[4] T. Storer, Cyclotomy and Difference Sets (Markham Pub. Co., Chicago, 1967).
[5] A.L. Whiteman, The cyclotomic numbers of order twelve, Acta Arith. 6 (1960) 53–76.

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 55–56
North-Holland

NOTE

A UNITAL IN THE HUGHES PLANE OF ORDER NINE

A.E. BROUWER
Dept. of Math., Techn. Univ. Eindhoven, Eindhoven, The Netherlands

Eight years ago I found four nonisomorphic 2-(28, 4, 1) designs embedded in the Hughes plane of order nine, using a computer. This note gives an algebraic description of one of them.

1. Rosati's unital

In [1] and [2] I described the construction of 138 nonisomorphic Steiner systems $S(2, 4, 28)$, 11 of which could be embedded in a projective plane of order 9 (of which 4 in the Hughes plane).

Recently, Rosati [4] constructed a unital (2-$(q^3+1, q+1, 1)$ design, i.e. Steiner system $S(2, q+1, q^3+1)$) in each Hughes plane of order q^2, and raised the question whether his unital coincided in case $q=3$ with one of the four I had found earlier. This turns out not to be the case. Statistics for Rosati's unital are:

$s[3:7]=(0, 1152, 552, 72, 15)$, not resolvable, uniquely embeddable in a projective plane of order nine, self-dual, automorphism group of order 48, point orbits of sizes $4+12+12$, block orbits of sizes $3+6+6+24+24$, the binary code spanned by the blocks has dimension 23 and the weight enumerator of its dual has coefficients $a_{10}=8$, $a_{12}=7$, $a_{14}=0$.

(Here s_i is the number of maximal (partial) spreads of size i; see also [1, 2].)

Applying the process described in [1] to Rosati's unital one finds 15 more unitals, so that as far as I know 154 nonisomorphic Steiner systems $S(2, 4, 28)$ are known today, 12 of which embed in a projective plane.

2. My unital E.8

Seeing Rosati's unital made me wonder whether one of my unitals has a reasonable algebraic description. In this note I shall describe the one with the largest group.

Consider the Hughes plane $\Pi=(\boldsymbol{P}, \boldsymbol{L})$ of order 9 defined over the "mini-quaternion" nearfield of order 9 (cf. [3]). Its group of automorphisms is isomorphic to $\mathrm{PGL}(3,3)\times \mathrm{Sym}(3)$ where the first factor is the group of projectivities, and the second factor the automorphism group of the nearfield. This group stabilizes a unique Baer subplane $\Pi_0=(\boldsymbol{P}_0, \boldsymbol{L}_0)$ of Π.

Choose a nonincident point-line pair x, L in Π_0. The subgroup G of $\mathrm{Aut}\,\Pi$ fixing both x and L is isomorphic to $\mathrm{GL}(2,3)\times \mathrm{Sym}(3)$ and has orbits of sizes

0012-365X/89/$3.50

$1+4+8+6+24+48$ on points and lines. (Namely: the point x, the 4 points of $L \cap \boldsymbol{P}_0$, the 8 remaining points of $\boldsymbol{P}_0$, the 6 remaining points of L, the 24 points of $\boldsymbol{P} \backslash \boldsymbol{P}_0$ that are on a line $M \in \boldsymbol{L}_0$ containing x and meeting $L \cap \boldsymbol{P}_0$, and the remaining 48 points. Dually for the lines.)

Let S be a Sylow 2-subgroup (of order 16) of GL(2, 3) and let T be the unique cyclic group of order 8 contained in S. Put $H=(T \times \mathrm{Alt}(3)) \cup ((S \backslash T) \times (\mathrm{Sym}(3) \backslash \mathrm{Alt}(3)))<G$. Then $H \cong \boldsymbol{Z}_{24}.2$ has order 48 and orbits of sizes $1+4+8+6+24_a+24_b$ on points and lines. Our unital has as points those in orbits $4+24_a$, and then its lines are those in orbits $1+6+8+24+24_b$. This unital is self-dual, but not the set of fixed points of a polarity.

An explicit description of the unital independent of the plane can be given as follows: Let $X=\{a\} \times \boldsymbol{Z}_{24} \cap \{b\} \times \boldsymbol{Z}_4$ and take as blocks the five blocks $\{a_0, a_6, a_{12}, a_{18}\}$, $\{a_0, a_3, a_4, a_{13}\}$, $\{a_1, a_3, a_8, b_0\}$, $\{a_0, a_8, a_{16}, b_2\}$, $\{b_0, b_1, b_2, b_3\}$, and their cyclic shifts (mod 24).

Note that also

$$(a_{2i}, a_{2i+1}, b_{2j}, b_{2j-1}) \mapsto (a_{-2i}, a_{11-2i}, b_{2j}, b_{2j+1})$$

is an automorphism.

Remains the question whether this construction can be generalized to Hughes planes of order q^2 for arbitrary odd q.

References

[1] A.E. Brouwer, Some unitals on 28 points and their embeddings in projective planes of order 9, Math. Centre Report ZW155/81, Amsterdam, March 1981.

[2] A.E. Brouwer, Some unitals on 28 points and their embeddings in projective planes of order 9, pp. 183–188 in: Geometries and Groups (Proceedings Berlin 1981) ed. M. Aigner & D. Jungnickel, Springer Lecture Notes in Math. 893 (Springer, Heidelberg, 1981).

[3] T.G. Room and P.B. Kirkpatrick, Miniquaternion geometry, Cambridge tracts in Math. and Math. Phys. 60 (Cambridge Univ. Press, Cambridge, 1971).

[4] L.A. Rosati, Disegni unitari nei piani di Hughes, preprint (1987).

Discrete Mathematics 77 (1989) 57–63
North-Holland

PERCENTAGES IN PAIRWISE BALANCED DESIGNS

Charles J. COLBOURN and Vojtech RŐDL
Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada

To Professor Haim Hanani on the occasion of his seventy-fifth birthday.

Let $K = \{k_1, \ldots, k_m\}$ be a set of block sizes, and let $\{p_1, \ldots, p_m\}$ be nonnegative numbers with $\sum_{i=1}^m p_i = 1$. We prove the following theorem: for any $\epsilon > 0$, if a $(v, K, 1)$ pairwise balanced design exists and v is sufficiently large, then a $(v, K, 1)$ pairwise balanced design exists in which the fraction of pairs appearing in blocks of size k_i is $p_i \pm \epsilon$ for every i. We also show that the necessary conditions for a pairwise balanced design having precisely the fraction p_i of its pairs in blocks of size k_i for each i are asymptotically sufficient.

1. Preliminaries

Let $K = \{k_1, \ldots, k_m\}$ be a (finite) set of positive integers greater than one. A *pairwise balanced design* $(V, \mathcal{B})$ is a set V of v elements, and a collection $\mathcal{B}$ of subsets of V with the properties that the size of each set of $\mathcal{B}$ is an integer in K, and every 2-subset of V appears in precisely one set of $\mathcal{B}$. Such a pairwise balanced design has *order* v, *index* one, and *blocksizes* K, and is termed a $(v, K, 1)$ PBD. When $K = \{k\}$, the PBD is a $(v, k, 1)$ *block design.* When $c \notin K$, a PBD with exactly one block of size c and all other block sizes from K is termed a $(v, K \cup \{c^*\}, 1)$ PBD. See Hanani [5] for further definitions and background.

For a $(v, K, 1)$ PBD to exist, two congruence conditions are necessary. Define

$$\alpha(K) = \gcd\{k_1 - 1, k_2 - 1, \ldots, k_m - 1\}, \quad \text{and}$$
$$\beta(K) = \gcd\{k_1(k_1 - 1), k_2(k_2 - 1), \ldots, k_m(k_m - 1)\}.$$

Then we must have $v - 1 \equiv 0 \pmod{\alpha(K)}$, and $v(v - 1) \equiv 0 \pmod{\beta(K)}$. Wilson [6] proved that these conditions are asymptotically sufficient:

Theorem A [6]. *For K a set of positive integers, there is a constant N_K so that if $v > N_K$, $v - 1 \equiv 0 \pmod{\alpha(K)}$ and $v(v - 1) \equiv 0 \pmod{\beta(K)}$, then a $(v, K, 1)$ pairwise balanced design exists.*

Wilson's theorem guarantees the existence of some PBD with the required block-sizes, but does not control the number of blocks of each size in any way. In certain applications, however, it is important to ensure that "most" blocks are of one size. In this context, one can view the Erdős–Hanani theorem [4] as establishing the existence of $(v, \{k, 2\}, 1)$ PBDs with almost all blocks of size k. Another context in which a majority of blocks of one size is required appears in

0012-365X/89/$3.50

[3]; there, $(v, \{6, 7\}, 1)$ PBDs are constructed in which almost all blocks have size 6, for *all* orders which are sufficiently large and for which a $(v, \{6, 7\}, 1)$ PBD exists at all.

In this paper, we use Wilson's theorem extensively to prove a general theorem in this direction. Informally, we show that one can prescribe the fraction of blocks of each size, and provided that the order is sufficiently large and the necessary conditions are met, there is a PBD with the required fraction of blocks of each size. More formally, we prove two theorems along these lines:

Theorem 1. *Let $\epsilon > 0$. Let $K = \{k_1, \ldots, k_m\}$ be a set of block sizes. Then there is a constant $C_{K,\epsilon}$ so that if $v \geq C_{K,\epsilon}$, $v - 1 \equiv 0 \pmod{\alpha(K)}$, and $v(v-1) \equiv 0 \pmod{\beta(K)}$, there is a $(v, K, 1)$ PBD in which the fraction of the blocks having size k_1 exceeds $1 - \epsilon$.*

Theorem 2. *Let $\epsilon > 0$. Let $K = \{k_1, \ldots, k_m\}$ be a set of block sizes. Let $\{p_1, \ldots, p_m\}$ be nonnegative numbers with $\sum_{i=1}^{m} p_i = 1$. Then there is a constant $P_{K,\epsilon}$ so that if $v \geq P_{K,\epsilon}$, $v - 1 \equiv 0 \pmod{\alpha(K)}$ and $v(v-1) \equiv 0 \pmod{\beta(K)}$, there is a $(v, K, 1)$ PBD in which, for each $1 \leq i \leq m$, the fraction of pairs appearing in blocks having size k_i is in the range $[p_i - \epsilon, p_i + \epsilon]$.*

The proof of these theorems relies on constructing a large (but finite) collection of PBDs in which blocks of one size predominate. In addition to Wilson's theorem, we require a theorem due to Chowla, Erdős and Straus [2] (see also Wilson [7] and Beth [1]):

Theorem B. *For every $k \geq 1$, there is a constant L_k so that a transversal design $\mathrm{TD}(k, v)$ exists for all $v \geq L_k$.*

A question related to that settled in Theorem 2 is to settle the existence of pairwise balanced designs having exactly the fraction p_i of its pairs covered by blocks of size k_i. In addition to the basic necessary conditions for the PBD to exist, we then have the additional necessary condition for each $1 \leq i \leq m$:

$$p_i v(v-1) \equiv 0 \pmod{k_i(k_i - 1)}. \tag{$*$}$$

We prove the following:

Theorem 3. *Let K be a set of block sizes, and let $\{p_1, \ldots, p_m\}$ be nonnegative fractions with $\sum_{i=1}^{m} p_i = 1$. Then there is a constant C so that for every $v > C$ satisfying $v - 1 \equiv 0 \pmod{\alpha(K)}$, $v(v-1) \equiv 0 \pmod{\beta(K)}$, and $(*)$, there is a $(v, K, 1)$ PBD in which, for every i, blocks of size k_i contain the fraction p_i of all pairs.*

To prove this theorem, we employ a generalization of Theorem A to graph designs established by Wilson [8]:

Theorem C. *Let $\mathcal{G}$ be a graph with e edges. Let $\alpha(\mathcal{G})$ be the greatest common divisor of all vertex degrees in $\mathcal{G}$, and let $\beta(\mathcal{G}) = 2e$. Then there exists a constant $C_{\mathcal{G}}$ such that for all $v > C_{\mathcal{G}}$, if $v - 1 \equiv 0 \pmod{\alpha(\mathcal{G})}$ and $v(v-1) \equiv 0 \pmod{\beta(\mathcal{G})}$, the complete graph K_v can be decomposed into edge-disjoint subgraphs, each isomorphic to $\mathcal{G}$.*

In the remainder of the paper, we use Theorems A, B and C to prove theorems 1, 2 and 3.

2. Proof of Theorem 1

The strategy of the proof is to construct PBDs $\mathcal{D}_i$ of orders $z + k_i$ (where z is an appropriately chosen positive integer), and a PBD $\mathcal{D}_0$, of order $z + 1$, each of which has all but ϵ fraction of its pairs in blocks of size k_1. To do this, we first construct PBDs $\mathcal{B}_i$ of orders $c + k_i$; we then construct PBDs $\mathcal{C}_i$ of orders $y + c + k_i$ and $y + c + 1$, and many apply a product construction (see Fig. 1) to form PBDs $\mathcal{D}_i$ of orders $xy + c + k_i$ and $xy + c + 1$ with the required fraction of blocks of size k_1. Appropriate choices for the integers x, y and c are given.

Finally applying Theorem A to PBDs with block sizes $|\mathcal{D}_i|$ for $0 \leq i \leq m$, we will infer Theorem 1.

Now we give a more detailed description of the proof. Choose c sufficiently large so that we can form a collection $\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_m$ of PBDs with block sizes from K, with $\mathcal{B}_0$ having order $c_0 = c + 1$ and $\mathcal{B}_i$, $i > 0$, having order $c_i = c + k_i$ (c can be chosen to be an appropriate multiple of $\prod_{i=1}^{m} k_i(k_i - 1)(k_i - 2)$). Let y be a multiple of $\prod_{i=0}^{m} c_i(c_i - 1)$, large enough so that a $(y + c_i, c_i, 1)$ block design exists

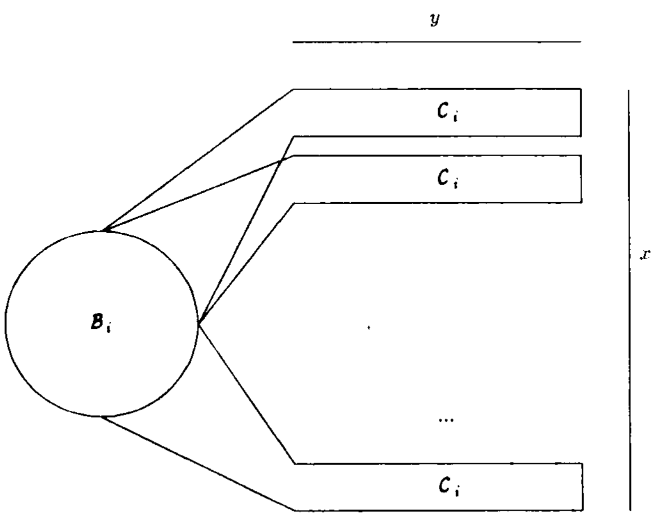


Fig. 1. $\mathcal{D}_i$.

for each i, and a TD(k_1, y) exists. Theorems A and B ensure that such a selection is possible. Replace all but one blocks in a $(y+c_i, c_i, 1)$ block design to form a $(y+c_i, K \cup \{c_i^*\}, 1)$ PBD $\mathscr{C}_i$ (i.e. $\mathscr{C}_i$ contains exactly one blocks of size c_i).

Now choose a value $x \equiv 1 \pmod{\beta(K)}$ for which an $(x, k_1, 1)$ block design exists, and

$$\epsilon y^2\binom{x}{2} > x\binom{y}{2} + \binom{c_i}{2} + xyc_i,$$

for every i, which exists by Theorem A. Let $\mathscr{A}$ be an $(x, k_1, 1)$ block design.

From $\mathscr{A}$ and $\mathscr{C}_i$, we form a $(v, K, 1)$ PBD $\mathscr{D}_i$ on $d_i = xy + c_i$ elements as follows. Let V be the element set of $\mathscr{A}$. The element set of $\mathscr{D}_i$ is then $V \times \{1, \ldots, y\} \cup \{\infty_1, \ldots, \infty_{c_i}\}$. First, for $j = 1, \ldots, x$, we place a copy of $\mathscr{C}_i$ on the elements $V \times \{j\} \cup \{\infty_1, \ldots, \infty_{c_i}\}$, so that the (unique) block of size c_i is on the elements $\{\infty_1, \ldots, \infty_{c_i}\}$. Next, whenever $A \in \mathscr{A}$, place a copy of a TD(k_1, y) on the elements $A \times \{1, \ldots, y\}$, with groups of the transversal design on classes of elements having the same second coordinate. Finally, replace the block of size c_i on $\{\infty_1, \ldots, \infty_{c_i}\}$ by the blocks of $\mathscr{B}_i$. The result, $\mathscr{D}_i$, is a $(v, K, 1)$ PBD in which the fraction of pairs in blocks of size k_1 exceeds $1 - \epsilon$.

Let $D = \{d_0, \ldots, d_m\}$. We want to apply Theorem A again to produce PBDs with block sizes from D for all sufficiently large orders satisfying the necessary condition for a PBD with block sizes from K to exist. To this end, we must verify that $\alpha(D) = \alpha(K)$ and $\beta(D) = \beta(K)$. Since $\prod_{i=1}^{m} k_i(k_i-1)(k_i-2)$ divides both c and y, and $d_i = xy + c + k_i$ holds, we infer that $\alpha(D) \geq \alpha(K)$ and $\beta(D) \geq \beta(K)$. Now we verify the opposite inequalities.

Since $\alpha(D)$ divides both $d_0 - 1 = xy + c$ and $d_i - 1 \times xy + c + k_i - 1$ for $i = 1, \ldots, m$, $\alpha(D)$ must divide their difference. That is, $\alpha(D)$ divides $k_i - 1$ for all $i = 1, \ldots, m$, and hence $\alpha(D) \leq \alpha(K)$.

Now we show that $\beta(D) \leq \beta(K)$. Let γ be a prime power dividing $\beta(D)$. Set $z = xy + c$. Then we have $d_0 = z + 1$ and $d_i = z + k_i$ for $i = 1, \ldots, m$. For every $i = 0, \ldots, m$, γ divides $d_i(d_i - 1)$ and hence γ divides the difference

$$d_i(d_i-1) - d_0(d_0-1) = 2(k_i-1)z + k_i^2 - k_i. \tag{2.1}$$

On the other hand, γ divides $d_0(d_0 - 1)$, and hence

$$\text{either } \gamma \mid z \quad \text{or} \quad \gamma \mid (z+1). \tag{2.2}$$

We show that the latter case is impossible. Suppose to the contrary that γ divides $z + 1$. Note that $z = xy + c$ is a multiple of $\prod_{i=1}^{m} k_i(k_i-1)(k_i-2)$ and hence γ does not divide $k_i - 1$ or $k_i - 2$ for any i. Rewriting (2.1), we obtain

$$\gamma \mid 2(k_i-1)(z+1) + (k_i-1)(k_i-2),$$

which implies that $\gamma \mid (k_i-1)(k_i-2)$, a contradiction.

Thus γ cannot divide $z + 1$, and hence by (2.2) must divide z. Together with (2.1), this implies that $\gamma \mid k_i(k_i - 1)$, proving that $\gamma \mid \beta(K)$ and hence also $\beta(D) \geq \beta(K)$. $\square$

Let v meet the necessary conditions for a $(v, K, 1)$ PBD, and $v > N_D$. Then a $(v, D, 1)$ PBD exists. Replacing each block of size d_i by a copy of $\mathscr{D}_i$ yields a $(v, K, 1)$ PBD in which the fraction of pairs in blocks of size k_1 exceeds $1 - \epsilon$.

3. Proof of Theorem 2

Let δ be small enough that

$$(p_i - \delta)\frac{(1-\delta)}{(1+\delta)} \geqslant p_i - \epsilon, \quad \text{and} \tag{3.1}$$

$$(p_i + \delta)(1+\delta) + \delta \leqslant p_i + \epsilon \tag{3.2}$$

holds for every $i = 1, \ldots, m$.

Using Theroem 1, produce a collection of PBDs with block sizes from K, $\{\mathscr{B}_{ij} : 0 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant m\}$, so that for each j, $1 \leqslant j \leqslant m$, $\mathscr{B}_{ij}$ has all but $(1-\delta)$ of its pairs in blocks of size k_j; the orders of $\mathscr{B}_{0j}, \ldots, \mathscr{B}_{mj}$ are $b_0, \ldots, b_m$, which are chosen as follows. Let z be a (sufficiently large) multiple of $\prod_{i=1}^{m} k_i(k_i - 1)(k_i - 2)$, so that we can produce all of the designs required above with orders $b_0 = z + 1$, and for $1 \leqslant i \leqslant m$, $b_i = z - k_i$. Moreover, we require that z is large enough that $b_i(b_i - 1) \leqslant (1+\delta)b_r(b_r - 1)$ for all $1 \leqslant i,\ r \leqslant n$.

Let $S = \{b_1, \ldots, b_m\}$. We have $\alpha(K) = \alpha(S)$ and $\beta(K) = \beta(S)$, as in the proof of Theorem 1. For v sufficiently large with $v - 1 \equiv 0 \pmod{\alpha(K)}$ and $v(v-1) \equiv 0 \pmod{\beta(K)}$, Theorem A ensures that a $(v, S, 1)$ PBD $\mathscr{D}$ exists. In addition, for v sufficiently large, we can ensure that the blocks of $\mathscr{D}$ can be partitioned into m classes so that $|\mathscr{D}_i|/|\mathscr{D}|$ is in the range $[p_i - \delta, p_i + \delta]$. For $j = 1, \ldots, m$, replace each block in $\mathscr{D}_j$ of size b_i by a copy of $\mathscr{B}_{ij}$. The PBD $\mathscr{C}$ which results is a $(v, K, 1)$ PBD. If λ_i is the number of pairs in $\mathscr{C}$ which are in blocks of size k_i, then we have for each $i = 1, \ldots, m$ that

$$\frac{\lambda_i}{\binom{v}{2}} > \frac{|\mathscr{D}_i|}{|\mathscr{D}|}\frac{(1-\delta)}{(1+\delta)} \geqslant (p_i - \delta)\frac{(1-\delta)}{(1+\delta)}$$

and

$$\frac{\lambda_i}{\binom{v}{2}} < \frac{|\mathscr{D}_i|}{|\mathscr{D}|}(1+\delta) + \delta \leqslant (p_i + \delta)(1+\delta) + \delta.$$

Therefore by (3.1) and (3.2), $\mathscr{C}$ satisfies the requirements of the theroem. □

4. Proof of Theorem 3

Write the fraction p_i of pairs in blocks of size k_i in the form f_i/b, so that gcd $\{f_1, \ldots, f_m\} = 1$. The necessary condition $(*)$ states then that for all i,

$$v(v-1)f_i \equiv 0 \pmod{bk_i(k_i - 1)}.$$

We construct a PBD with the prescribed fraction of pairs in blocks of each size whenever these necessary conditions are met. To do this, form a graph G consisting of disjoint complete subgraphs; G has r_i components isomorphic to K_{k_i}, so that

$$\frac{r_i k_i(k_i-1)}{\sum_{j=1}^{m} r_j k_j(k_j-1)} = \frac{f_i}{b},$$

for each i. Moreover, we ensure that $\gcd\{r_1, \ldots, r_m\} = 1$. Letting e be the number of edges of G, we can simplify to

$$r_i b k_i(k_i-1) = 2ef_i.$$

Hence the necessary condition becomes

$$v(v-1)r_i \equiv 0 \pmod{2e}.$$

Since the $\{r_j\}$ are relatively prime, we have

$$v(v-1) \equiv 0 \pmod{2e}.$$

By Theorem C, the necessary conditions are asymptotically sufficient for the existence of a decomposition of K_v into graphs isomorphic to G; such a decomposition trivially gives a PBD with the required fraction of pairs in each block size.

5. Closing remarks

The theorems proved here are to a large extent straightforward consequences of Wilson's theorems. Nevertheless, they allow finer control of the distribution of block sizes, and hence are useful for extremal questions in design theory, such as that studied in [3].

Acknowledgements

Thanks to Alex Rosa for suggesting this problem, and to Kevin Phelps for helpful discussions. Research of the first author is supported by NSERC Canada under grant A0579.

References

[1] T. Beth, Ein Bemerkung zur Abschatzung der Anzahl orthogonaler lateinischer Quadrate mittels Siebverfahren, Abh. Math. Sem. Hamburg 53 (1983) 284–288.

[2] S. Chowla, P. Erdős and E.G. Straus, On the maximal number of pairwise orthogonal Latin squares of a given order, Canad. J. Math. 12 (1960) 204–208.

[3] C.J. Colbourn, W.R. Polleyblank and A. Rosa, Cubic feedback sets and hybrid triple systems, Graphs and Combinatorics, 5 (1989) 15–28.
[4] P. Erdős and H. Hanani, On a limit theorem in combinatorial analysis, Publ. Math. Debrecen 10 (1963) 10–13.
[5] H. Hanani, Balanced incomplete block designs and related designs, Discrete Math. 11 (1975) 255–369.
[6] R.M. Wilson, An existence theory for pairwise balanced designs II. The structure of PBD closed sets and the existence conjectures, J. Combin. Theory A13 (1972) 246–273.
[7] R.M. Wilson, Concerning the number of mutually orthogonal Latin squares, Discrete Math. 9 (1974) 181–198.
[8] R.M. Wilson, Decompositions of complete graphs into subgraphs isomorphic to a given graph, in: Proc. Fifth British Combinatorial Conference (1975) 647–659.

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 65–73
North-Holland

ON COMPLETE ARCS IN STEINER SYSTEMS $S(2,3,v)$ AND $S(2,4,v)$

Marialuisa J. de RESMINI
Dipartimento di Matematica, Università di Roma 'La Sapienza', 00185 Rome, Italy

To Professor Haim Hanani on his seventy-fifth birthday.

A lower bound is provided for the size of complete arcs in an $S(2, k, v)$ and examples are exhibited for $k=3$ and 4 which show that the lower bound can be attained. Partitions are examined of $S(2, 4, v)$'s into complete arcs.

1. Introduction

The well established facts that both $S(2, 3, v)$'s and $S(2, 4, v)$'s exist for all v's in their spectra and that the number of non-isomorphic systems increases with v raise several questions. One is the classification of such Steiner systems. However, in such general terms this problem seems hopeless. Hence, additional conditions and more information are needed on the inner structure of STS's and $S(2, 4, v)$'s. Basically, there are two possible approaches to the investigation of such inner structures. One of them appeals to possible automorphism groups admitted by the Steiner system. This method recently produced many new Steiner systems and enabled the classification of some of them, see e.g. [2, 4, 14, 21, 27, 28, 35, 36, 37]. The other approach looks at possible nice subsets of the point set and/or at configurations formed by the blocks. Also from this standpoint our knowledge is constantly increased by new results, see e.g. [9, 17, 18]. The inner structure of a certain design is the design itself. This was the case in the very first constructions [20] and since then it has been investigated focusing on different objects. In particular, it is worth recalling that looking at possible generating triangles enabled the classification of STS's as planes, degenerate planes and spaces [11, 34].

Here we shall present some results concerning the smallest possible size for a complete arc in an $S(2, k, v)$ and give some examples of $S(2, 3, v)$'s and $S(2, 4, v)$'s containing complete arcs whose sizes attain the lower bounds. Furthermore, we examine the inner structure of some $S(2, 4, v)$'s by looking for possible partitions of the point set into complete arcs. Twenty-seven years ago Hanani's famous paper [15] appeared in which the existence was proved, by construction, of an $S(2, 4, v)$ for any $v \equiv 1$ or $4 \pmod{12}$. Since then many other

$S(2, 4, v)$'s were constructed so that it seems interesting to devise properties which might enable one to determine when two systems of the same order are inequivalent.

We assume that the reader is familiar with the Steiner system terminology and we refer him to [1, 19] for background and to [12, 13] for literature on the subject, our references being far from exhaustive.

2. Complete arcs in Steiner systems $S(2, k, v)$

An s-arc in an $S(2, k, v)$ is a set of s points of the system no three of which are on a block. Thus an arc is met by any block in 0, 1, or 2 points. Moreover, an arc is complete if any point of the $S(2, k, v)$ lies on at least one secant block. A tangent (secant) block is briefly called a tangent (secant).

If there are no tangents, then the arc takes its maximum possible size, i.e. $r + 1 = (v - 1)/(k - 1) + 1$, and is referred to as a hyperoval. Hyperovals have been thoroughly investigated in STS's and results are known for any k [9, 22]. Furthermore, their use in the construction of $S(2, 3, v)$'s goes back to Kirkman [20] and Reiss [32].

Since the spectrum of $S(2, k, v)$'s containing hyperovals is not the whole spectrum of these systems [9], it makes sense to consider the next possible size for a complete arc. More precisely, we require that there is a unique tangent to the arc at each of its points. Such a complete arc is called an oval and clearly has r points. Again, results are known on STS's containing ovals of some particular types, not necessarily complete [23, 38].

By an oval in an $S(2, k, v)$ we always mean a complete r-arc with a unique tangent at each point. This definition is suggested by the behaviour of ovals in any odd order projective plane and is motivated by the fact that we are interested in complete arcs.

An easy counting argument shows that the number of secants to an oval through each exterior point equals the number of exterior blocks on that point. Moreover, the number of tangents on an exterior point has the same parity as r. Therefore, a necessary condition for an oval to admit interior points, i.e. points on no tangent, is $r \equiv 0 \pmod 2$.

It is well known [16] that in a projective plane Π of odd order q the $q + 1$ tangents to an oval Ω, i.e. a complete $(q + 1)$-arc, form an oval in the dual plane. This means that each point in $\Pi \setminus \Omega$ lies on either two or zero tangents to Ω. This is a consequence of the fact that any two lines in Π always meet. On the other hand, such a result is not true in a Steiner system $S(2, k, v)$ with $b > v$, since there exist parallel blocks.

The next example shows an oval in an $S(2, 3, 13)$, that is a complete 6-arc with a unique tangent at each point. Notice that we started with the points on the oval to construct the STS(13). The points of the oval are $1, 2, \ldots, 6$. Then the secants are:

$$\begin{array}{ccccc} 1\ 2\ \ 7 & 1\ 5\ 12 & 2\ 4\ 12 & 3\ 4\ \ 9 & 4\ 5\ 10 \\ 1\ 3\ 11 & 1\ 6\ \ 9 & 2\ 5\ \ 9 & 3\ 5\ 13 & 4\ 6\ \ 7 \\ 1\ 4\ \ 8 & 2\ 3\ \ 8 & 2\ 6\ 13 & 3\ 6\ 10 & 5\ 6\ \ 8. \end{array}$$

Moreover, the tangents are 1 10 13, 2 10 11, 3 7 12, 4 11 13, 5 7 11, 6 11 12 and the exterior blocks are 7 9 13, 8 12 13, 9 10 12, 7 8 10, 8 9 11. This oval has two interior points, namely 8 and 9, and 11 is a point on four tangents. The remaining points off the arc all are on two tangents. (Ovals in the two nonisomorphic STS(13)'s are thoroughly investigated in [39].)

Therefore, in looking for ovals in an $S(2, k, v)$ one can add some conditions on the oval, for instance the existence of a prescribed number of interior points and/or a certain behaviour of the tangents. For STS's this approach is used in [23, 38].

We observe that the existence of an oval in an $S(2, k, v)$ does not yield any arithmetic condition on v. It depends on the structure of the Steiner system under consideration only.

As we already remarked, the existence of hyperovals gives arithmetic conditions on v [9] which are $v \equiv 3$ or 7 (mod 12) for an STS and $v \equiv 4$ (mod 12) for an $S(2, 4, v)$ (for any k, see Propositions 3 and 4 in [9]). If we delete one point from a hyperoval in an $S(2, k, v)$, we obtain an r-arc all of whose tangents pass through the deleted point. Such an arc is not complete, so we do not consider it as an oval as is done in [38]. Therefore, when an $S(2, k, v)$ contains hyperovals it can contain ovals too and none of these ovals is contained in a hyperoval.

Again, the situation is different from that occurring in projective planes. In fact, any projective plane of even order q can contain hyperovals, but no oval as the $q+1$ tangents to a $(q+1)$-arc all pass through a point which completes the arc to a hyperoval. This is an easy consequence of two facts; namely, the number of tangents to the $(q+1)$-arc on a point off it must be odd, as q is even, and any two lines meet [16].

Next, we turn to the problem of the minimum possible size for a complete arc in an $S(2, k, v)$. We observe that such a lower bound is an open question for projective planes which is settled only for small orders [6, 16]. On the other hand, the following result shows that for $S(2, k, v)$'s with $b > v$ the solution is easier.

Proposition 2.1. *The minimum possible size s for a complete arc in an $S(2, k, v)$, say S, satisfies*

$$s^2(k-2) - s(k-4) - 2v = 0. \tag{2.2}$$

Proof. If γ is a complete s-arc in S, then any point of $S \setminus \gamma$ lies on one secant at least. Therefore, the minimum possible size for γ is attained when each point of

$S\backslash\gamma$ lies on exactly one secant block. This condition yields

$$\frac{s(s-1)}{2}(k-2)+s=v$$

from which (2.2) follows. □

Notice that Proposition 2.1 provides necessary conditions on v, since equation (2.2) must have an integral solution.

Corollary 2.3. *The minimum possible size for a complete arc in an $S(2,3,v)$ is $s=(-1+\sqrt{1+8v})/2$. Furthermore, a necessary condition for an STS to contain a complete arc of the minimum possible size is that v takes one of the following forms:*

$$v=72y^2\pm 18y+1, \quad y\geqslant 1, \tag{2.4}$$

$$v=6m+3, \text{ where } m=(a_j^2-25)/48 \text{ and } a_j \text{ is recursively defined by } a_1=11,\ a_{j+1}=a_j+2(2j-1), \quad j=1,2,\ldots \tag{2.5}$$

Proof. The first part of the statement immediately follows from Proposition 2.1. Thus a necessary existence condition is provided by $1+8v$ being a square.

Suppose $v\equiv 1 \pmod 6$, i.e. $v=6m+1$. Then $1+8v=48m+9$. For this to be a square, $m=3w$. So $16w+1$ must be a square. Thus $16w+1=(8y\pm 1)^2$ which implies that $w=y(4y\pm 1)$ and gives (2.4). Furthermore, $s=12y+1$ for the former value of v and $s=12y-2$ for the latter.

Next, assume $v\equiv 3 \pmod 6$, i.e. $v=6m+3$. Thus, $8v+1=48m+25=a^2$. Therefore, $m=(a^2-25)/48$ must be an integer. The smallest value of a for which this occurs is $a_1=11$. We claim that m is an integer for $a=a_j$, where a_j is recursively defined as in the statement. By induction, we show that $48 \mid a_j^2-25$ implies $48 \mid a_{j+1}^2-25$. This means that we have to prove that $12 \mid (2j-1)(a_j+2j-1)$. On the other hand, this easily follows from the observations below which can all be proved by induction.

$j\equiv 1 \pmod 3 \Rightarrow a_j\equiv 2 \pmod 3$, $j\equiv 0$ or $2 \pmod 3 \Rightarrow a_j\equiv 1 \pmod 3$,
$j\equiv 0 \pmod 2 \Rightarrow a_j\equiv 1 \pmod 4$, $j\equiv 1 \pmod 2 \Rightarrow a_j\equiv 3 \pmod 4$.

To prove the necessity of the above form for m, we begin by observing that $a^2-25\equiv 0 \pmod{48}$ implies $a^2\equiv 1 \pmod 6$. Therefore, $a\equiv 1$ or $5 \pmod 6$. If $a=6z+1$, then $(a^2-25)/48=(3z^2+z-2)/4$. For this to be an integer, $z\equiv 2$ or $3 \pmod 4$. Consequently, $a\equiv 13$ or $19 \pmod{24}$. If $a=6z+5$, then $(a^2-25)/48=z(3z+5)/4$ which is an integer for $z\equiv 0$ or $1 \pmod 4$ only. Thus $a\equiv 5$ or $11 \pmod{24}$. Therefore, necessary conditions for $(a^2-25)/48$ to be an integer are $a\equiv 5$, 11, 13 or $19 \pmod{24}$ and $a>5$ to avoid a trival case. The solutions of these congruences are precisely the above defined a_j's. □

By Corollary 2.3, $v=15$ is an admissible order for complete arcs to exist of the smallest possible size. In this case the size is 5. The next example shows an $S(2,3,15)$ containing a complete 5-arc.

Take the STS(15) no. 21 in [26] whose blocks are given below:

1 2 3	1 4 5	1 6 7	1 8 9	1 10 11	1 12 13	1 14 15
2 4 6	2 5 7	2 8 10	2 9 12	2 11 14	2 13 15	3 4 7
3 5 6	3 8 11	3 9 13	3 10 15	3 12 14	4 8 12	4 9 14
4 10 13	4 11 15	5 8 13	5 9 15	5 10 14	5 11 12	6 8 14
6 9 10	6 11 13	6 12 13	7 8 15	7 9 11	7 10 12	7 13 14.

Then it is easy to check that the points 1 9 10 12 14 form a complete 5-arc. Notice that this STS(15) contains a subsystem (on the points $1, 2, \ldots, 7$); hence, it contains a hyperoval on $8, 9, \ldots, 15$. Moreover, the points 1 3 7 9 10 14 yield a complete 6-arc. Two other complete 6-arcs are 1 5 7 8 12 14 and 1 3 5 7 9 14.

Take now the STS(15) no. 19 [26]. Its blocks are:

1 2 3	1 4 5	1 6 7	1 8 9	1 10 11	1 12 13	1 14 15
2 4 6	2 5 7	2 8 10	2 9 11	2 12 14	2 13 15	3 4 7
3 5 6	3 8 12	3 9 14	3 10 13	3 11 15	4 8 15	4 9 12
4 10 14	4 11 13	5 8 13	5 9 10	5 11 14	5 12 15	6 8 11
6 9 15	6 10 12	6 13 14	7 8 14	7 9 13	7 10 15	7 11 12.

This $S(2, 3, 15)$ contains a unique subsystem, that on the points $1, \ldots, 7$. thus it contains a hyperoval on $8, 9, \ldots, 15$ [9, 20]. It also contains an oval whose points are 1 3 4 6 11 12 14. This oval admits no interior point. The points 8, 9 and 15 are on three tangents whereas the remaining ones are on one tangent only. Also this STS(15) contains a complete 5-arc, namely the one on the points 7 9 12 14 15.

We observe that the STS(15) given by PG(3, 2), no. 1 in [26], obviously contains a complete 5-arc. It is provided by an ovoid in the projective 3-space [16]. Moreover, PG(3, 2) has a partition into three ovoids.

The next admissible order is $v = 21$ (Corollary 2.3) and the corresponding smallest possible size for a complete arc is 6. So there might exist an STS(21) containing a complete 6-arc. There are many known STS(21)'s [4, 26, 27, 28] and no exhaustive search has been carried out to find those containing complete 6-arcs. The author picked at random a couple of $S(2, 3, 21)$'s in each of the quoted papers and tried to uncover, by hand, some complete 6-arc. These very few trials turned out to be unsuccessful.

The proof to Proposition 2.1 suggests a construction of Steiner systems $S(2, k, v)$ containing a complete arc of minimum possible size provided that the necessary conditions on v are satisfied. The construction requires one to start with the arc together with its secants (pairs of points) and complete the pairs to blocks by taking into account that no two secant blocks meet outside the arc. A general procedure has not been devised yet. It is quite obvious that the solution is not going to be easy when $k \geq 4$. However, a general construction is presently under investigation of STS's admitting a complete arc of minimum possible size.

Corollary 2.6. *The minimum possible size for a complete arc in an $S(2, 4, v)$ is $\sqrt{v}$. A necessary condition for such an arc to exist is that v has one of the following* *forms*:

$$v = (6w+1)^2, \qquad v = (6w+5)^2, \qquad v = 4(3w+1)^2, \qquad v = 4(3w+2)^2.$$

Proof. The size of the arc comes from Proposition 2.1. The expressions for v follow from the fact that v must be a square. Recall that $v \equiv 1$ or 4 (mod 12). □

In [9] it was shown that an STS can be embedded in an $S(2, 4, v)$ with two intersection numbers 1 and 3, i.e. with no exterior block, provided that $v \equiv 4$ (mod 24) and v is a square. Under these assumptions, the order of the embedded STS is $(v \pm \sqrt{v})/2$. We observe that in case $v = 4(3w+1)^2$, the above conditions are satisfied. Moreover, the possible complete $(6w+2)$-arc in the $S(2, 4, v)$ might also be a complete $(6w+2)$-arc in the embedded STS of order $18w^2+15w+3$ (Corollary 2.3). Such a complete arc is of minimum possible size both in the $S(2, 4, v)$ and in the embedded STS. The smallest value of v for which such a situation can occur is $v = 100$ in which case the STS has order 55 and the complete arc is a 10-arc.

Notice that Corollary 2.6 suggests the existence of $S(2, 4, v)$'s, v a square, admitting a partition into $\sqrt{v}$ complete $(\sqrt{v})$-arcs. Steiner systems with this property do exist as the next examples show.

The unique $S(2, 4, 16)$ admits such a partition. To show this, we write its blocks as follows, the points being $A1, A2, A3, A4$, $B1, \ldots, B4$, $C1, \ldots, C4$, $D1, \ldots, D4$.

$A1\ A2\ B1\ B2$	$A1\ A3\ C1\ C3$	$A1\ A4\ D1\ D4$	$A1\ B3\ C4\ D2$	$A1\ B4\ C2\ D3$
$A3\ A4\ B3\ B4$	$A2\ A4\ C2\ C4$	$A2\ A3\ D2\ D3$	$A2\ B4\ C3\ D1$	$A2\ B3\ C1\ D4$
$C1\ C2\ D1\ D2$	$B1\ B3\ D1\ D3$	$B1\ B4\ C1\ C4$	$A3\ B1\ C2\ D4$	$A3\ B2\ C4\ D1$
$C3\ C4\ D3\ D4$	$B2\ B4\ D2\ D4$	$B2\ B3\ C2\ C3$	$A4\ B2\ C1\ D3$	$A4\ B1\ C3\ D2$.

Then it is easy to verify that $A1, \ldots, A4$; $B1, \ldots, B4$; $C1, \ldots, C4$; $D1, \ldots, D4$ are complete 4-arcs and it is clear that such 4-arcs partition the point set. In this case a block is either secant to two arcs of the partition or tangent to all four of them. Of course, such a situation cannot occur when v is odd.

The next possible value for v is 25. The $S(2, 4, 25)$ no. 1 in [21] contains a complete 5-arc. The points of the arc are 1 3 14 17 25. For the reader's convenience, we list the blocks of this Steiner system.

1 2 3 19	2 9 10 24	4 7 13 14	6 11 18 21	11 14 17 24
1 4 10 11	2 13 21 22	4 9 17 22	6 17 19 23	12 15 18 22
1 6 14 22	2 14 16 20	4 12 16 21	7 8 9 21	1 5 9 25
1 7 16 17	3 5 13 24	4 18 19 24	7 10 15 19	2 6 7 25
1 8 12 23	3 6 10 12	5 7 18 23	7 12 20 24	3 4 8 25
1 13 18 20	3 7 11 22	5 8 14 15	8 10 20 22	10 14 18 25
1 15 21 24	3 9 16 18	5 10 17 21	8 11 13 19	11 15 16 25
2 4 15 23	3 14 21 23	5 16 19 22	9 11 20 23	12 13 17 25
2 5 11 12	3 15 17 20	6 8 16 24	9 12 14 19	19 20 21 25
2 8 17 18	4 5 6 20	6 9 13 15	10 13 16 23	22 23 24 25.

We observe that this $S(2, 4, 25)$ has a special point, namely 25, in the sense of B. Rokowska [33]. She defines an $S(2, 4, v)$ with a special points 0 as follows. For any two blocks $0\, x_1\, x_2\, x_3$ and $0\, y_1\, y_2\, y_3$ there exist two blocks $0\, z_1\, z_2\, z_3$ and $0\, w_1\, w_2\, w_3$ such that $x_j\, y_j\, z_j\, w_j$, $j = 1, 2, 3$, is a block. The triples of points other than 0 on the blocks through 0 are to be considered as ordered triples. For instance, take the blocks 25 1 5 9 and 25 2 6 7. They uniquely determine the blocks 25 3 4 8 and 25 19 20 21 so that 1 2 3 19, 5 6 4 20 and 9 7 8 21 are blocks. Next, take 25 1 5 9 and 25 6 7 2. These blocks pick out the pair 25 14 18 10, 25 22 23 24 and the resulting blocks are 1 6 14 22, 5 7 18 23 and 9 2 10 24. In a similar manner one obtains all the blocks of the $S(2, 4, 25)$. The $S(2, 4, 25)$ no. 1 in [21] and the system in [33] might be isomorphic but this was not checked.

Also the $S(2, 4, 25)$ no. 6 in [21] contains complete 5-arcs. Furthermore, it admits a partition into five such arcs. The blocks of the system are the following ones.

1 2 6 25	4 5 9 23	11 17 18 22	2 5 15 18	6 8 16 24
1 5 10 24	4 6 10 15	12 18 19 23	2 10 17 19	6 9 19 22
1 7 8 12	4 18 24 25	13 19 20 24	2 11 14 24	6 14 21 23
1 20 21 22	5 6 7 11	14 16 20 25	3 5 13 16	7 9 17 25
2 3 7 21	5 19 21 25	15 16 17 21	3 6 18 20	7 10 20 23
2 8 9 13	6 12 13 17	1 3 11 19	3 12 15 25	7 15 22 24
2 16 22 23	7 13 14 18	1 4 14 17	4 7 16 19	8 10 18 21
3 4 8 22	8 14 15 19	1 9 16 18	4 11 13 21	8 11 23 25
3 9 10 14	9 11 15 20	1 13 15 23	5 8 17 20	9 12 21 24
3 17 23 24	10 11 12 16	2 4 12 20	5 12 14 22	10 13 22 25.

The partition is provided by the five 5-arcs $5+j$, $10+j$, $15+j$, $20+j$, $25+j$, $j = 0, 1, \ldots, 4$, addition mod 25.

We remark that the $S(2, 4, 25)$'s no.s 2 and 3 in [21] seem to contain no complete 5-arc. However, they contain complete 6-arcs. Furthermore, no. 2 has a special point, namely 25, in the sense of [33] and might be isomorphic to the Steiner system there. Again, this was not checked.

Some of the cyclic [4] and elementary abelian [14] $S(2, 4, 49)$'s were examined for complete 7-arcs. No exhaustive search was carried out but the performed random search was unsuccessful. However, in each of the investigated cases the orbit under Z_7 of a point yielded an incomplete 7-arc.

This raises two questions. First, the existence, for any square $v \geqslant 49$, $v \equiv 1$ or 4 (mod 12), of an $S(2, 4, v)$ containing a complete $(\sqrt{v})$-arc. Secondly, the existence, for any v as above, of an $S(2, 4, v)$ whose point set admits a partition into $\sqrt{v}$ complete $(\sqrt{v})$-arcs. We conjecture that such systems exist and, most likely, are neither cyclic nor elementary abelian.

Of course, arcs in Steiner systems are independent sets, since no three points are on a block. Some results on the largest cardinality of an independent set in an STS can be found in [5, 31] but arcs are not considered there.

Finally, we observe that in an $S(2, k, v)$ maximal $\{s; n\}$-arcs can be considered, i.e. s-sets of points met by any block in either 0 or n points. Necessary conditions for such maximal arcs to exist were given in [9] and other results on them can be found in [7, 30].

References

[1] Th. Beth, D. Jungnickel and H. Lenz, Design Theory (Bibliographisches Institut, Mannheim/Wien/Zürich, 1985).

[2] A.E. Brouwer, Some unitals on 28 points and their embeddings in projective planes of order 9, in Geometries and Groups, Lecture Notes in Math., 893 (Springer, 1981) 183–188.

[3] A.E. Brouwer and H. Lenz, Subspaces of linear spaces of line size 4, Europ. J. Combin. 2 (1981) 323–330.

[4] M.J. Colbourn and R.A. Mathon, On cyclic Steiner 2-designs, Ann. Discr. Math. 7 (1980) 215–253.

[5] M. de Brandes and V. Rödl, Steiner triple systems with small maximal independent sets, Ars Combin. 17 (1984) 15–19.

[6] R.H.F. Denniston, On arcs in projective planes of order 9, Manuscr. Math. 4 (1971) 61–90.

[7] R.H.F. Denniston, A Steiner system with a maximal arc, Ars Combin. 9 (1980) 247–248.

[8] R.H.F. Denniston, Some maximal arcs in finite projective planes, J. Combin. Theory 6 (1969) 317–319.

[9] M.J. de Resmini, On sets of type (m, n) in a Steiner system $S(2, l, v)$, in Finite Geometries and Designs, London Math. Soc. Lecture Note Series 49 (1981) 104–113.

[10] J. Doyen, Sur la croissance du nombre de systèmes triples de Steiner non isomorphes, J. Combin. Theory 8 (1970) 424–441.

[11] J. Doyen, Sur la structure de certain systèmes triples de Steiner, Math. Z. 111 (1969) 289–300.

[12] J. Doyen and A. Rosa, An updated biblography and survey of Steiner systems, Ann. Discr. Math. 7 (1980) 317–349.

[13] J. Doyen and A. Rosa, A bibliography and survey of Steiner systems, preprint, April 1985.

[14] H. Gropp, The elementary abelian Steiner systems $S(2, 4, 49)$, Discr. Math. 64 (1987) 87–90.

[15] H. Hanani, The existence and construction of balanced incomplete block designs, Ann. Math. Statistics 32 (1961) 361–368.

[16] J.W.P. Hirschfeld, Projective Geomety over Finite Fields (Clarendon Press, Oxford, 1979).

[17] D.G. Hoffman and C.C. Lindner, The flower intersection problem for Steiner triple systems, Ann. Discr. Math. 34 (1987) 243–248.

[18] P. Horák and A. Rosa, Decomposing Steiner triple systems into small configurations, Ars Combin. 26 (1988) 91–105.

[19] D.R. Hughes and F.C. Piper, Design Theory (Cambridge Univ. Press, 1985).

[20] T.P. Kirkman, On a problem in combinations, Cambridge and Dublin Math. J. 2 (1847) 191–204.

[21] E.S. Kramer, S.S. Magliveras and V.D. Tonchev, On the Steiner systems $S(2, 4, 25)$ invariant under a group of order 9, Preprint, March 1987.

[22] H. Lenz and H. Zeitler, Hyperovale in Steiner-Tripel-Systemen, Math. Semesterberichte 32 (1985) 19–49.

[23] H. Lenz and H. Zeitler, Regular ovals in Steiner triple systems, J. Combin., Inform. & System Sci. 9 (1984) 155–162.

[24] C.C. Lindner and A. Rosa, Steiner quadruple systems all of whose derived Steiner triple systems are non-isomorphic, J. Combin. Theory A 21 (1976), 35–43.

[25] C.C. Lindner and A. Rosa, Steiner quadruple systems – A survey, Discr. Math. 21 (1978) 147–181.

[26] R. Mathon, K.T. Phelps and A. Rosa, Small Steiner triple systems and their properties, Ars Combin. 15 (1983) 3–110.

[27] R.A. Mathon, K.T. Phelps and A. Rosa, A class of Steiner triple systems of order 21 and associated Kirkman systems, Math. Comp. 37 (1981) 209–222.
[28] R.A. Mathon and A. Rosa, The 4-rotational Steiner and Kirkman triple systems of order 21, Ars Combin. 17A (1984) 241–250.
[29] E.H. Moore, Tactical Memoranda I–III, Amer. J. Math. 18 (1896) 264–303.
[30] E.J. Morgan, Arcs in block designs, Ars Combin. 4 (1977) 3–16.
[31] K.T. Phelps and V. Rődl, Steiner triple systems with minimum independence number, Ars Combin. 21 (1986) 167–172.
[32] M. Reiss, Über eine Steinersche combinatorische Aufgabe, welche in 45sten Bande dieses Journal, Seite 181, gestellt worden ist, J. reine u. angew. Math. (J. Crelle) 56 (1859) 326–344.
[33] B. Rokowska, A new construction of the block systems $B(4, 1, 25)$ and $B(4, 1, 28)$, Colloq. Math. 38 (1977) 165–167.
[34] L. Teirlinck, On Steiner spaces, J. Combin. Theory A 26 (1979) 103–114.
[35] V.D. Tonchev, Steiner triple systems of order 21 with automorphisms of order 7, preprint, May 1986.
[36] V.D. Tonchev, Two new Steiner systems $S(2, 4, 25)$, Compt. rend. Acad. Bulg. Sci. 39 (1986) 47–48.
[37] V.D. Tonchev, Transitive Steiner triple systems of order 25, preprint, May 1985.
[38] H. Zeitler, Ovals in Steiner triple systems, Ann. Discr. Math. 30 (1986) 373–382.
[39] H. Zeitler, Ovale in STS(13), Math. Semesterberichte 31 (1984) 195–214.

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 75–87
North-Holland

A SURVEY OF RECENT WORKS WITH RESPECT TO A CHARACTERIZATION OF AN $(n, k, d; q)$-CODE MEETING THE GRIESMER BOUND USING A MIN·HYPER IN A FINITE PROJECTIVE GEOMETRY

Noboru HAMADA
Department of Mathematics, Osaka Women's University, Sakai-city, Osaka, Japan

Michel DEZA
Université de Paris VII, C.N.R.S., Paris, France

Received November 1987
Revised 24 April 1988

1. Introduction

Let F be a set of f points in a finite projective geometry $\mathrm{PG}(t, q)$ of t dimensions where $t \geqslant 2$, $f \geqslant 1$ and q is a prime power. If (a) $|F \cap H| \geqslant m$ for any hyperplane H in $\mathrm{PG}(t, q)$ and (b) $|F \cap H| = m$ for some hyperplane H in $\mathrm{PG}(t, q)$, then F is said to be an $\{f, m; t, q\}$-min·hyper (or an $\{f, m; t, q\}$-minihyper) where $m \geqslant 0$ and $|A|$ denotes the number of points in the set A. The concept of a min·hyper (called a minihyper) has been introduced by Hamada and Tamari [22]. In the special case $t = 2$, an $\{f, m; 2, q\}$-min·hyper F is called an m-blocking set if F contains no 1-flat in $\mathrm{PG}(2, q)$.

Let $E(t, q)$ be the set of all ordered sets $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{t-1})$ of integers ε_α such that $0 \leqslant \varepsilon_\alpha \leqslant q-1$ $(\alpha = 0, 1, \ldots, t-1)$ and $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{t-1}) \neq (0, 0, \ldots, 0)$. Let $U(t, q)$ be the set of all ordered sets $(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h)$ of integers ε, h and μ_i such that $0 \leqslant \varepsilon \leqslant q-1$, $1 \leqslant h \leqslant (t-1)(q-1)$, $1 \leqslant \mu_1 \leqslant \mu_2 \leqslant \cdots \leqslant \mu_h \leqslant t-1$ and $0 \leqslant n_l(\underline{\mu}) \leqslant q-1$ for $l = 1, 2, \ldots, t-1$ where $n_l(\underline{\mu})$ denotes the number of integers μ_i in $\underline{\mu} \equiv (\mu_1, \mu_2, \ldots, \mu_h)$ such that $\mu_i = l$ for the given integer l. Note that there is a one-to-one correspondence between the set $E(t, q)$ and the set $U(t, q)$ as follows:

$$\varepsilon = \varepsilon_0, \quad n_1(\underline{\mu}) = \varepsilon_1, \quad n_2(\underline{\mu}) = \varepsilon_2, \ldots, n_{t-1}(\underline{\mu}) = \varepsilon_{t-1} \tag{1.1}$$

where $\underline{\mu} = (\mu_1, \mu_2, \ldots, \mu_h)$ and $\sum_{\alpha=1}^{t-1} \varepsilon_\alpha = h$. For example, $(2, 4, 0, 2)$ in $E(4, 5)$ corresponds to $(2, 1, 1, 1, 1, 3, 3)$ in $U(4, 5)$. In what follows, we shall use an orderd set in either $E(t, q)$ or $U(t, q)$ as occasion demands.

Let $V(n; q)$ be an n-dimensional vector space consisting of row vectors over a Galois field $\mathrm{GF}(q)$ of order q where n is a positive integer. A k-dimensional subspace C of $V(n; q)$ is said to be an $(n, k, d; q)$-code (or a q-ary linear code

0012-365X/89/$3.50

with length n, dimension k, and minimum distance d) if the minimum (Hamming) distance of the code C is equal to d where $n > k \geqslant 3$ and $d \geqslant 1$ (cf. Blake and Mullin [3] and MacWilliams and Sloane [29]).

It is well known (cf. Griesmer [11] and Solomon and Stiffler [30]) that if there exists an $(n, k, d; q)$-code for given integers k, d and q, then

$$n \geqslant \sum_{l=0}^{k-1} \left\lceil \frac{d}{q^l} \right\rceil \tag{1.2}$$

where $\lceil x \rceil$ denotes the smallest integer $\geqslant x$. In what follows, we shall confine ourself to the case $k \geqslant 3$ and $1 \leqslant d \leqslant q^{k-1} - q$. In this case, d can be expressed as follows:

$$d = q^{k-1} - \sum_{\alpha=0}^{k-2} \varepsilon_\alpha q^\alpha \quad \left(\text{or } d = q^{k-1} - \left(\varepsilon + \sum_{i=1}^{h} q^{\mu_i}\right)\right), \tag{1.3}$$

using some ordered set $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{k-2})$ in $E(k-1, q)$ (or some ordered set $(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h)$ in $U(k-1, q)$, resp.) and the Griesmer bound (1.2) can be expressed as follows:

$$n \geqslant v_k - \sum_{\alpha=0}^{k-2} \varepsilon_\alpha v_{\alpha+1} \quad \left(\text{or } n \geqslant v_k - \left(\varepsilon + \sum_{i=1}^{h} v_{\mu_i+1}\right)\right), \tag{1.4}$$

where $v_l = (q^l - 1)/(q-1)$ for any integer $l \geqslant 0$.

Recently, Hamada [12, 16] showed that in the case $k \geqslant 3$ and $d = q^{k-1} - \sum_{\alpha=0}^{k-2} \varepsilon_\alpha q^\alpha$ (or $d = q^{k-1} - (\varepsilon + \sum_{i=1}^{h} q^{\mu_i})$), there is a one-to-one correspondence between the set of all $(n, k, d; q)$-codes meeting the Griesmer bound (1.4) and the set of all $\{\sum_{\alpha=0}^{k-2} \varepsilon_\alpha v_{\alpha+1}, \sum_{\alpha=1}^{k-2} \varepsilon_\alpha v_\alpha; k-1, q\}$-min · hypers (or the set of all $\{\sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i}; t, q\}$-min · hypers, resp.) if we introduce an equivalence relation between two $(n, k, d; q)$-codes as Definition 2.1 in Hamada [16] (cf. Theorem 3.11, Remark 3.3 and Example 3.1 in Section 3). Hence in order to obtain a necessary and sufficient condition for integers k, d and q that there exists an $(n, k, d; q)$-code meeting the Griesmer bound (1.2) in the case $1 \leqslant d \leqslant q^{k-1} - q$ and to characterize all $(n, k, d; q)$-codes meeting the Griesmer bound (1.2) in the case $1 \leqslant d \leqslant q^{k-1} - q$, it is sufficient to solve the following problem with respect to a min · hyper. The purpose of this paper is to survey recent works with respect to the following problem.

Problem A. (1) Find a necessary and sufficient condition for an ordered set $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{t-1})$ in $E(t, q)$ (or an ordered set $(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h)$ in $U(t, q)$) that there exists a

$$\left\{\sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_{\alpha+1}, \sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_\alpha; t, q\right\}\text{-min} \cdot \text{hyper}$$

$$\times \left(\text{or a } \left\{\sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i}; t, q\right\}\text{-min} \cdot \text{hyper}\right).$$

(2) Characterize all

$$\left\{\sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_{\alpha+1}, \sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_\alpha; t, q\right\}\text{-min} \cdot \text{hypers}$$

$$\times\left(\text{or all } \left\{\sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i}; t, q\right\}\text{-min} \cdot \text{hypers}\right)$$

in the case where there exist such min · hypers.

Example 1.1. Let F be a μ-flat in PG(t, q) where $1 \leq \mu < t$. Then $|F| = (q^{\mu+1} - 1)/(q-1) \equiv v_{\mu+1}$ and $|F \cap H| = v_\mu$ or $v_{\mu+1}$ for any hyperplane H in PG(t, q) according as $F \not\subset H$ or $F \subset H$. Hence F is a $\{v_{\mu+1}, v_\mu; t, q\}$-min · hyper if F is a μ-flat in PG(t, q). Tamari [31, 33] showed that the converse holds, i.e. if F is a $\{v_{\mu+1}, v_\mu; t, q\}$-min · hyper, then F is a μ-flat in PG(t, q). Hence in the special case $\varepsilon_0 = \varepsilon_1 = \cdots = \varepsilon_{\mu-1} = 0$, $\varepsilon_\mu = 1$, $\varepsilon_{\mu+1} = \cdots = \varepsilon_{t-1} = 0$ (or $\varepsilon = 0$, $h = 1$ and $\mu_1 = \mu$), F is a $\{v_{\mu+1}, v_\mu; t, q\}$-min · hyper if and only if F is a μ-flat in PG(t, q).

Example 1.2. In the case $t \geq 2$, $q \geq 3$, $\varepsilon = 0$ and $h = 2$, it is shown by Hamada [12, 13] that (1) in the case $\mu_1 + \mu_2 \geq t$, there is no $\{v_{\mu_1+1} + v_{\mu_2+1}, v_{\mu_1} + v_{\mu_2}; t, q\}$-min · hyper and (2) in the case $\mu_1 + \mu_2 \leq t - 1$, F is a $\{v_{\mu_1+1} + v_{\mu_2+1}, v_{\mu_1} + v_{\mu_2}; t, q\}$-min · hyper if and only if F is a union of a μ_1-flat and a μ_2-flat in PG(t, q) which are mutually disjoint where $1 \leq \mu_1 \leq \mu_2 < t$.

2. Construction of several min · hypers

Let F be a set of ε_0 0-flats, ε_1 1-flats, . . . , ε_{t-1} $(t-1)$-flats in PG(t, q) which are mutually disjoint where $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{t-1}) \in E(t, q)$. Then $|F| = \sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_{\alpha+1}$, $|F \cap H| \geq \sum_{\alpha=1}^{t-1} \varepsilon_\alpha v_\alpha$ for any hyperplane H in PG(t, q) and the equality holds for some hyperplane H in PG(t, q). Hence F is a $\{\sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_{\alpha+1}, \sum_{\alpha=1}^{t-1} \varepsilon_\alpha v_\alpha; t, q\}$-min · hyper (cf. Hamada [16]).

Let F be a set of ε points, a μ_1-flats, a μ_2-flat, . . . , a μ_h-flat in PG(t, q) which are mutually disjoint where $(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h) \in U(t, q)$. Then F is a $\{\sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i}; t, q\}$-min · hyper. Hence we have the following

Theorem 2.1. *Let* $\mathfrak{F}_E(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{t-1}; t, q) \neq \emptyset$ *and* $\mathfrak{F}_U(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h; t, q) \neq \emptyset$ *for given ordered sets* $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{t-1})$ *in* $E(t, q)$ *and* $(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h)$ *in* $U(t, q)$, *respectively, where* $\mathfrak{F}_E(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{t-1}; t, q)$ *denotes a family of all unions of* ε_0 *0-flats,* ε_1 *1-flats, . . . ,* ε_{t-1} $(t-1)$*-flats in* PG(t, q) *which are mutually disjoint and* $\mathfrak{F}_U(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h; t, q)$ *denotes a family of all unions of* ε *points, a* μ_1*-flat, a* μ_2*-flat, . . . , a* μ_h*-flat in* PG(t, q) *which are mutually disjoint.*

(1) *If* $F \in \mathfrak{F}_E(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{t-1}; t, q)$, *then* F *is a* $\{\sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_{\alpha+1}, \sum_{\alpha=1}^{t-1} \varepsilon_\alpha v_\alpha; t, q\}$*-min · hyper.*

(2) *If* $F \in \mathfrak{F}_U(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h; t, q)$, *then* f *is a* $\{\sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i}; t, q\}$*-min · hyper.*

Remark 2.1. If there exists a relation between a set $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{t-1})$ in $E(t, q)$ and a set $(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h)$ in $U(t, q)$ as (1.1), then $\mathfrak{J}_E(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{t-1}; t, q) = \mathfrak{J}_U(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h; t, q)$.

Remark 2.2. It is known (cf. Hamada and Tamari [24] for example) that (1) in the case $h=1$, $\mathfrak{J}_U(\varepsilon, \mu_1; t, q) \neq \emptyset$ for any (ε, μ_1) in $U(t, q)$ and (2) in the case $h \geq 2$, $\mathfrak{J}_U(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h; t, q) \neq \emptyset$ if and only if $\mu_{h-1} + \mu_h \leq t-1$.

Problem B. Find a necessary and sufficient condition for an ordered set $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{t-1})$ in $E(t, q)$ (or an ordered set $(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h)$ in $U(t, q)$ that the converse of (1) (or (2)) in Theorem 2.1 holds, i.e. $F \in \mathfrak{J}_E(\varepsilon, \varepsilon_1, \ldots, \varepsilon_{t-1}; t, q)$ for any $\{\sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_{\alpha+1}, \sum_{\alpha=1}^{t-1} \varepsilon_\alpha v_\alpha; t, q)$-min · hyper F (or $F \in \mathfrak{J}_U(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h; t, q)$ for any $\{\sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i}; t, q\}$-min · hyper F, resp.).

Let V be a θ-flat in PG(t, q) where $2 \leq \theta \leq t$. A set S of m points in V is said to be an m-arc in V if no $\theta+1$ points in S are linearly dependent where $m \geq \theta+1$. In the special case $\theta = t$, S is said to be an m-arc in PG(t, q). For convenience sake, a set S of θ points in the θ-flat V is said to be a θ-arc in V if θ points in S are linearly independent. Let $\mathfrak{U}(\theta, \varepsilon; t, q)$ denote a family of all sets $V \setminus S$ of a θ-flat V in PG(t, q) and a $(q+\theta-\varepsilon)$-arc S in V where $2 \leq \theta \leq t$ and $0 \leq \varepsilon < q$.

Let $\mathfrak{M}(\theta, \zeta; \xi, \pi_1, \pi_2, \ldots, \pi_l; t, q)$ denote a family of all sets $(V \setminus S) \cup A \cup B$ of a set $V \setminus S$ in $\mathfrak{U}(\theta, \zeta; t, q)$, a set A of ξ points in PG(t, q) and a set B in $\mathfrak{J}_U(0, \pi_1, \pi_2, \ldots, \pi_l; t, q)$ such that $V \cap A = \emptyset$, $(V \setminus S) \cap B = \emptyset$ and $A \cap B = \emptyset$ where either (a) $l = 0$, $2 \leq \theta \leq t-1$, $\zeta \geq 0$, $\xi \geq 0$ and $\zeta + \xi < q$ or (b) $1 \leq l \leq (t-2)(q-1)$, $2 \leq \theta \leq \pi_1$, $\zeta \geq 0$, $\xi \geq 0$, $\zeta + \xi < q$ and $(0, \pi_1, \pi_2, \ldots, \pi_l) \in U(t, q)$. Note that $\mathfrak{J}_U(0, \pi_1, \pi_2, \ldots, \pi_l; t, q) = \emptyset$ in the case $l = 0$ and $A = \emptyset$ in the case $\xi = 0$. The following theorem due to Hamada [16] gives another method of construction of a min · hyper.

Theorem 2.2. *Let* $\mathfrak{U}(\theta, \varepsilon; t, q) \neq \emptyset$ *and* $\mathfrak{M}(\theta, \zeta; \xi, \pi_1, \pi_2, \ldots, \pi_l; t, q) \neq \emptyset$ *for given integers.*

(1) *If* $F \in \mathfrak{U}(\theta, \varepsilon; t, q)$, *then* F *is a* $\{\sum_{\alpha=1}^{\theta-1} (q-1) v_{\alpha+1} + \varepsilon, \sum_{\alpha=1}^{\theta-1} (q-1) v_\alpha; t, q\}$*-min · hyper.*

(2) *If* $F \in \mathfrak{M}(\theta, \zeta; \xi, \pi_1, \pi_2, \ldots, \pi_l; t, q)$, *then* F *is a* $\{\sum_{\alpha=1}^{\theta-1} (q-1) v_{\alpha+1} + \sum_{i=1}^{l} v_{\pi_i+1} + \zeta + \xi, \sum_{\alpha=1}^{\theta-1} (q-1) v_\alpha + \sum_{i=1}^{l} v_{\pi_i}; t, q\}$*-min · hyper.*

Helleseth [25] characterized all $(n, k, d; q)$-codes meeting the Griesmer bound for the case $k \geq 3$, $q = 2$ and $1 \leq d < 2^{k-1}$. In terms of a min · hyper, the result of Helleseth can be expressed as follows.

Theorem 2.3. *Let* $(\varepsilon, \mu_1, \mu_2, \ldots, \mu_n)$ *be an ordered set in* $U(t, 2)$ *and let* $f = \sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon$ *and* $m = \sum_{i=1}^{h} v_{\mu_i}$ *where* $v_l = 2^l - 1$ *for any integer* $l \geq 0$.

(1) *In the case $h = 1$, F is a $\{v_{\mu_1+1} + \varepsilon, v_{\mu_1}; t, 2\}$-min · hyper if and only if $F \in \mathfrak{J}_U(\varepsilon, \mu_1; t, 2)$.*

(2) *In the case $h \geq 2$, $\mu_{h-1} + \mu_h \leq t - 1$ and $(\mu_1, \mu_2) \neq (1, 2)$, F is an $\{f, m; t, 2\}$-min · hyper if and only if $F \in \mathfrak{J}_U(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h; t, 2)$.*

(3) *In the case $h \geq 2$, $\mu_{h-1} + \mu_h > t - 1$ and $(\mu_1, \mu_2) \neq (1, 2)$, there is no $\{f, m; t, 2\}$-min · hyper.*

(4) *In the case $t \geq 3$, $(\mu_1, \mu_2, \ldots, \mu_h) = (1, 2, \ldots, h)$ and $t/2 < h \leq t - 1$ (i.e. $\mu_{h-1} + \mu_h > t - 1$), F is an $\{f, m; t, 2\}$-min · hyper if and only if $F \in \mathfrak{B}(h + 1, \varepsilon; t, 2)$ where $\mathfrak{B}(h + 1, 0; t, 2) = \mathfrak{U}(h + 1, 0; t, 2)$ and $\mathfrak{B}(h + 1, 1; t, 2) = \mathfrak{U}(h + 1, 1; t, 2) \cup \mathfrak{M}(h + 1, 0; 1; t, 2)$.*

(5) *In the case $t \geq 4$, $(\mu_1, \mu_2, \ldots, \mu_h) = (1, 2, \ldots, h)$ and $2 \leq h \leq t/2$ (i.e. $\mu_{h-1} + \mu_h \leq t - 1$), F is an $\{f, m; t, 2\}$-min · hyper if and only if either $F \in \mathfrak{J}_U(\varepsilon, 1, 2, \ldots, h; t, 2)$ or $F \in \mathfrak{B}(h + 1, \varepsilon; t, 2)$ or $F \in \mathfrak{M}(l, \zeta; \xi, l, l + 1, \ldots, h; t, 2)$ for some integer l in $\{2, 3, \ldots, h\}$ and some nonnegative integers ζ and ξ such that $\zeta + \xi = \varepsilon$.*

(6) *In the case $h \geq \theta$, $(\mu_1, \mu_2, \ldots, \mu_{\theta-1}) = (1, 2, \ldots, \theta - 1)$, $\mu_\theta > \theta$ and $\mu_{h-1} + \mu_h \leq t - 1$ for some integer $\theta \geq 3$, F is an $\{f, m; t, 2\}$-min · hyper if and only if either $F \in \mathfrak{J}_U(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h; t, 2)$ or $F \in \mathfrak{M}(l, \zeta; \xi, \mu_l, \mu_{l+1}, \ldots, \mu_h; t, 2)$ for some integer l in $\{2, 3, \ldots, \theta\}$ and some nonnegative integers ζ and ξ such that $\zeta + \xi = \varepsilon$.*

(7) *In the case $h \geq \theta$, $(\mu_1, \mu_2, \ldots, \mu_{\theta-1}) = (1, 2, \ldots, \theta - 1)$, $\mu_\theta > \theta$ and $\mu_{h-1} + \mu_h > t - 1$ for some integer $\theta \geq 3$, there is no $\{f, m; t, 2\}$-min · hyper.*

Remark 2.3. Theorem 2.3 shows that in the case $q = 2$, there is no $\{f, m; t, 2\}$-min · hyper except for $\{f, m; t, 2\}$-min · hypers given by Theorems 2.1 and 2.2 where f and m are integers given in Theorem 2.3.

3. Characterization of certain min · hypers

In what follows, we shall survey recent works with respect to a characterisation of a $\{\sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{h} v_{\mu_i}; t, q\}$-min · hyper where $t \geq 2$, $q \geq 3$ and $(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h) \in U(t, q)$.

Theorem 3.1 (Tamari [33]). *Let ε and μ be any integers such that $\varepsilon \in \{0, 1\}$ and $1 \leq \mu < t$. Then F is a $\{v_{\mu+1} + \varepsilon, v_\mu; t, q\}$-min · hyper if and only if $F \in \mathfrak{J}_U(\varepsilon, \mu; t, q)$.*

Theorem 3.2 (Hamada and Deza [21]). *Let ε and μ be any integers such that $0 \leq \varepsilon \leq q - 1$ and $1 \leq \mu < t$.*

(1) *In the case $0 \leq \varepsilon < \sqrt{q}$, F is a $\{v_{\mu+1} + \varepsilon, v_\mu; t, q\}$-min · hyper if and only if $F \in \mathfrak{J}_U(\varepsilon, \mu; t, q)$.*

(2) *In the case $\varepsilon \geq \sqrt{q}$ and $q = p^{2r}$ for a prime p and a positive integer r, there exists at least one $\{v_2 + \varepsilon, v_1; t, q\}$-min · hyper F such that $F \notin \mathfrak{J}_U(\varepsilon, 1; t, q)$.*

Remark 3.1. Let F be a square-root subplane (called a Baer subplane) in PG(2, q) where $q=p^{2r}$ (cf. p. 81 in Hughes and Piper [28]). Then $|F|=q+\sqrt{q}+1$, $1\leq|F\cap H|\leq\sqrt{q}+1$ for any 1-flat H in PG(2, q) and $|F\cap H|=1$ for some 1-flat H in PG(2, q). Hence F is a $\{v_2+\sqrt{q}, 1; 2, q\}$-min · hyper which contains no 1-flat in PG(2, q).

Theorem 3.3 (Hamada [12]). *Let $(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h)$ be any ordered set in $U(t, q)$ such that $\varepsilon\in\{0, 1\}$, $2\leq h<t$ and $1\leq\mu_1<\mu_2<\cdots<\mu_h<t$.*

(1) *In the case $\mu_{h-1}+\mu_h\leq t-1$, F is a $\{\sum_{i=1}^h v_{\mu_i+1}+\varepsilon, \sum_{i=1}^h v_{\mu_i}; t, q\}$-min · hyper if and only if $F\in\mathfrak{F}_U(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h; t, q)$.*

(2) *In the case $\mu_{h-1}+\mu_h\geq t$, there is no $\{\sum_{i=1}^h v_{\mu_i+1}+\varepsilon, \sum_{i=1}^h v_{\mu_i}; t, q\}$-min · hyper F.*

In what follows, $\mathfrak{F}_U(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h; t, q)$ will be denoted by $\mathfrak{F}(\lambda_1, \lambda_2, \ldots, \lambda_\eta; t, q)$ where $\eta=h+\varepsilon$, $\lambda_i=0$ $(i=1, 2, \ldots, \varepsilon)$ and $\lambda_{\varepsilon+j}=\mu_j$ $(j=1, 2, \ldots, h)$.

Corollary 3.1. *Let α and β be any integers such that $0\leq\alpha<\beta<t$.*

(1) *In the case $t\geq\alpha+\beta+1$, F is a $\{v_{\alpha+1}+v_{\beta+1}, v_\alpha+v_\beta; t, q\}$-min · hyper if and only if $F\in\mathfrak{F}(\alpha, \beta; t, q)$.*

(2) *In the case $t\leq\alpha+\beta$, there is no $\{v_{\alpha+1}+v_{\beta+1}, v_\alpha+v_\beta; t, q\}$-min · hyper F.*

Corollary 3.2. *Let α, β and γ be any integers such that $0\leq\alpha<\beta<\gamma<t$.*

(1) *In the case $t\geq\beta+\gamma+1$, F is a $\{v_{\alpha+1}+v_{\beta+1}+v_{\gamma+1}, v_\alpha+v_\beta+v_\gamma; t, q\}$-min · hyper if and only if $F\in\mathfrak{F}(\alpha, \beta, \gamma; t, q)$.*

(2) *In the case $t\leq\beta+\gamma$, there is no $\{v_{\alpha+1}+v_{\beta+1}+v_{\gamma+1}, v_\alpha+v_\beta+v_\gamma; t, q\}$-min · hyper.*

The following proposition due to Hamada [16] plays an important role in solving Problems A and B.

Proposition 3.1 (Hamada [16]). *Let $(0, \lambda_1, \lambda_2, \ldots, \lambda_h)$ be an ordered set in $U(t, q)$ such that $h\geq 2$ and $\lambda_{h-1}+\lambda_h\leq t-1$ and let l be a positive integer such that $\lambda_n+l\leq t-1$. If $F^*\in\mathfrak{F}(\lambda_1, \lambda_2, \ldots, \lambda_h; t, q)$ for any $\{\sum_{i=1}^h v_{\lambda_i+1}, \sum_{i=1}^h v_{\lambda_i}; t, q\}$-min · hyper F^*, then* (1) *in the case $1\leq l<(t-\lambda_{h-1}-\lambda_h)/2$, $F\in\mathfrak{F}(\lambda_1+l, \lambda_2+l, \ldots, \lambda_h+l; t, q)$ for any $\{\sum_{i=1}^h v_{\lambda_i+l+1}, \sum_{i=1}^h v_{\lambda_i+l}; t, q\}$-min · hyper F and* (2) *in the case $l\geq(t-\lambda_{h-1}-\lambda_n)/2$, there is no $\{\sum_{i=1}^h v_{\lambda_i+l+1}, \sum_{i=1}^j v_{\lambda_i+l}; t, q\}$-min · hyper F.*

Corollary 3.3. *If $F^*\in\mathfrak{F}(1, 1; t, q)$ for any $\{2v_2, 2v_1; t, q\}$-min · hyper F^*, then* (1) *in the case $t\geq 2\mu+1\geq 5$, $F\in\mathfrak{F}(\mu, \mu; t, q)$ for any $\{2v_{\mu+1}, 2v_\mu; t, q\}$-min · hyper F and* (2) *in the case $3\leq\mu+1\leq t\leq 2\mu$, there is no $\{2v_{\mu+1}, 2v_\mu; t, q\}$-min · hyper F.*

Corollary 3.4. *If $F^* \in \mathfrak{J}(1, 1, 1; t, q)$ for any $\{3v_2, 3v_1; t, q\}$-min · hyper F^*, then (1) in the case $t \geq 2\mu + 1 \geq 5$, $F \in \mathfrak{J}(\mu, \mu, \mu; t, q)$ for any $\{3v_{\mu+1}, 3v_\mu; t, q\}$-min · hyper F and (2) in the case $3 \leq \mu + 1 \leq t \leq 2\mu$, there is no $\{3v_{\mu+1}, 3v_\mu; t, q\}$-min · hyper F where $q \geq 4$.*

Corollary 3.5. *Let γ be an integer such that $2 \leq \gamma < t$. If $F^* \in \mathfrak{J}(1, 1, \gamma; t, q)$ for any $\{v_{\gamma+1} + 2v_2, v_\gamma + 2v_1; t, q\}$-min · hyper F^*, then (1) in the case $1 \leq l < (t - 1 - \gamma)/2$, $F \in \mathfrak{J}(l+1, l+1, l+\gamma; t, q)$ for any $\{v_{\gamma+l+1} + 2v_{l+2}, v_{\gamma+l} + 2v_{l+1}; t, q\}$-min · hyper F and (2) in the case $l \geq (t-1-\gamma)/2$, there is no $\{v_{\gamma+l+1} + 2v_{l+2}, v_{\gamma+l} + 2v_{l+1}; t, q\}$-min · hyper F.*

Theroem 3.4 (Hamada [13]).

(1) *In the case $t \geq 3$, F is a $\{2v_2, 2v_1; t, q\}$-min · hyper if and only if $F \in \mathfrak{J}(1, 1; t, q)$.*

(2) *In the case $t = 2$, there is no $\{2v_2, 2v_1; t, q\}$-min · hyper F.*

Theorem 3.5 (Hamada [13]).

(1) *In the case $t \geq 2\mu + 1 \geq 3$, F is a $\{2v_{\mu+1}, 2v_\mu; t, q\}$-min · hyper if and only if $F \in \mathfrak{J}(\mu, \mu; t, q)$.*

(2) *In the case $t \leq 2\mu$, there is no $\{2v_{\mu+1}, 2v_\mu; t, q\}$-min · hyper F.*

Theorem 3.6 (Hamada [13]).

(1) *In the case $t = 2$ and $q = 3$, F is a $\{2v_2 + v_1, 2v_1 + v_0; 2, 3\}$-min · hyper if and only if $F \in \mathfrak{U}(2, 1; 2, 3)$.*

(2) *In the case $t \geq 3$ and $q = 3$, F is a $\{2v_2 + v_1, 2v_1 + v_0; t, 3\}$-min · hyper if and only if either $F \in \mathfrak{J}(0, 1, 1; t, 3)$ or $F \in \mathfrak{U}(2, 1; t, 3)$.*

(3) *In the case $t = 2$ and $q \geq 4$, there is no $\{2v_2 + v_1, 2v_1 + v_0; 2, q\}$-min · hyper F.*

(4) *In the case $t \geq 3$ and $q \geq 4$, F is a $\{2v_2 + v_1, 2v_1 + v_0; t, q\}$-min · hyper if and only if $F \in \mathfrak{J}(0, 1, 1; t, q)$.*

Theorem 3.7 (Hamada [14]).

(1) *In the case $t \geq 2$ and $q = 3$, F is a $\{v_2 + 2v_1, v_1 + 2v_0; t, 3\}$-min · hyper if and only if either $F \in \mathfrak{J}(0, 0, 1; t, 3)$ or $F = \{(\mathbf{v}_1), (\mathbf{v}_0 + \mathbf{v}_1), (2\mathbf{v}_0 + \mathbf{v}_1), (\mathbf{v}_2), (\mathbf{v}_1 + \mathbf{v}_2), (c\mathbf{v}_0 + 2\mathbf{v}_1 + \mathbf{v}_2)\}$ for some integer c in $\{1, 2\}$ and some noncollinear points $(\mathbf{v}_0)$, $(\mathbf{v}_1)$ and $(\mathbf{v}_2)$ in* PG$(t, 3)$.

(2) *In the case $t \geq 2$ and $q = 4$, F is a $\{v_2 + 2v_1, v_1 + 2v_0; t, 4\}$-min · hyper if and only if either $F \in \mathfrak{J}(0, 0, 1; t, 4)$ or $F = \{(\mathbf{v}_0 + \mathbf{v}_1), (\alpha\mathbf{v}_0 + \mathbf{v}_1), (\alpha^2\mathbf{v}_0 + \mathbf{v}_1), (\mathbf{v}_2), (c\mathbf{v}_0 + \mathbf{v}_1 + \mathbf{v}_2), (c\alpha^2\mathbf{v}_0 + \alpha\mathbf{v}_1 + \mathbf{v}_2), (c\alpha\mathbf{v}_0 + \alpha^2\mathbf{v}_1 + \mathbf{v}_2)\}$ for some element c in $\{1, \alpha, \alpha^2\}$ and some noncollinear points $(\mathbf{v}_0)$, $(\mathbf{v}_1)$ and $(\mathbf{v}_2)$ in* PG$(t, 4)$ *where α is a primitive element in* GF(2^2).

(3) *In the case $t \geq 2$ and $q \geq 5$, F is a $\{v_2 + 2v_1, v_1 + 2v_0; t, q\}$-min · hyper if and only if $F \in \mathfrak{J}(0, 0, 1; t, q)$.*

Theorem 3.8 (Hamada [14, 15] and Hamada and Deza [20]). *Let α, β and γ be any integers such that either $0 \leqslant \alpha = \beta < \gamma < t$ or $0 \leqslant \alpha < \beta = \gamma < t$ where $t \geqslant 2$ and $q \geqslant 5$.*

(1) *In the case $t \geqslant \beta + \gamma + 1$, F is a $\{v_{\alpha+1} + v_{\beta+1} + v_{\gamma+1}, v_\alpha + v_\beta + v_\gamma; t, q\}$-min · hyper if and only if $F \in \mathfrak{J}(\alpha, \beta, \gamma; t, q)$.*

(2) *In the case $t \leqslant \beta + \gamma$, there is no $\{v_{\alpha+1} + v_{\beta+1} + v_{\gamma+1}, v_\alpha + v_\beta + v_\gamma; t, q\}$-min · hyper F.*

Theorem 3.9 (Hamada [14, 17]).

(1) *In the case $q \geqslant 5$, there is no $\{2v_2 + 2v_1, 2v_1 + 2v_0; 2, q\}$-min · hyper.*

(2) *In the case $q = 3$, F is a $\{2v_2 + 2v_1, 2v_1 + 2v_0; 2, 3\}$-min · hyper if and only if $F \in \mathfrak{U}(2, 2; 2, 3)$ where $v_0 = 0$, $v_1 = 1$ and $v_2 = 4$.*

(3) *In the case $q = 4$, F is a $\{2v_2 + 2v_1, 2v_1 + 2v_0; 2, 4\}$-min-hyper if and only if there exist some noncollinear points (v_0), (v_1) and (v_2) in PG(2, 4) such that either (a), (b) or (c) as follows:*

(a) $F = L_0 \cup L_1 \cup \{(c_0\mathrm{v}_0 + \mathrm{v}_1 + \mathrm{v}_2), (c_1\mathrm{v}_0 + \alpha\mathrm{v}_1 + \mathrm{v}_2), (c_2\mathrm{v}_0 + \alpha^2\mathrm{v}_1 + \mathrm{v}_2)\}$ *for some elements c_0, c_1 and c_2 in $\{0, 1, \alpha, \alpha^2\}$.*

(b) $F = L_0 \cup \{(\mathrm{v}_2), (\mathrm{v}_1 + \mathrm{v}_2), (c\mathrm{v}_0 + \mathrm{v}_1 + \mathrm{v}_2), (c\mathrm{v}_0 + \alpha\mathrm{v}_1 + \mathrm{v}_2), (c\alpha\mathrm{v}_0 + \alpha\mathrm{v}_1 + \mathrm{v}_2), (c\mathrm{v}_0 + \alpha^2\mathrm{v}_1 + \mathrm{v}_2), (c\alpha^2\mathrm{v}_0 + \alpha^2\mathrm{v}_1 + \mathrm{v}_2)\}$ *for some element c in $\{1, \alpha, \alpha^2\}$.*

(c) $F = (L_0 \setminus \{(\mathrm{v}_1)\}) \cup (L_1 \setminus \{(\mathrm{v}_2)\} \cup (M_2 \setminus \{(c\mathrm{v}_1 + \mathrm{v}_2)\}) \cup \{(c\alpha\mathrm{v}_1 + \mathrm{v}_2), (c\alpha^2\mathrm{v}_1 + \mathrm{v}_2)\}$ *for some element c in $\{1, \alpha, \alpha^2\}$.*

Where $v_0 = 0$, $v_1 = 1$, $v_2 = 5$, $L_0 = (\mathrm{v}_0) \oplus (\mathrm{v}_1)$, $L_1 = (\mathrm{v}_0) \oplus (\mathrm{v}_2)$, $M_2 = (\mathrm{v}_0) \oplus (c\mathrm{v}_1 + \mathrm{v}_2)$ and $(\omega_1) \oplus (\omega_2)$ denotes a 1-flat in PG(2, 4) passing through two points (ω_1) and (ω_2) in PG(2, 4) and α is a primitive element in GF(2^2) such that $\alpha^2 = \alpha + 1$ and $\alpha^3 = 1$.

Theorem 3.10 (Hamada and Deza [18, 19]). *Let α and β be any integers such that $0 \leqslant \alpha < \beta < t$ where $t \geqslant 2$ and $q \geqslant 5$.*

(1) *In the case $t \geqslant 2\beta + 1$, F is a $\{2v_{\alpha+1} + 2v_{\beta+1}, 2v_\alpha + 2v_\beta; t, q\}$-min · hyper if and only if $F \in \mathfrak{J}(\alpha, \alpha, \beta, \beta; t, q)$.*

(2) *In the case $t \leqslant 2\beta$, there is no $\{2v_{\alpha+1} + 2v_{\beta+1}, 2v_\alpha + 2v_\beta; t, q\}$-min · hyper F.*

Remark 3.2. It is conjectured by Hamada (cf. Remark 4.1 in [16]) that in the case $t \geqslant 3$, $q \geqslant 3$, $\varepsilon = 0$, $h \geqslant 2$ and $\mu_1 \geqslant 2$, "there is no $\{\sum_{i=1}^h v_{\mu_i+1}, \sum_{i=1}^h v_{\mu_i}; t, q\}$-min · hyper" or "$F$ is a $\{\sum_{i=1}^h v_{\mu_i+1}, \sum_{i=1}^h v_{\mu_i}; t, q\}$-min · hyper if and only if $F \in \mathfrak{J}(\mu_1, \mu_2, \ldots, \mu_h; t, q)$" according as $\mu_{h-1} + \mu_h \geqslant t$ or $\mu_{h-1} + \mu_h \leqslant t - 1$.

Let $W(k; q)$ be a k-dimensional vector space over GF(q) consisting of column vectors. Then every point in a finite projective geometry PG($k-1$, q) may be represented by $(\underset{\sim}{c})$ using some nonzero vector $\underset{\sim}{c}$ in $W(k; q)$ where $(\underset{\sim}{c}_1) = (\underset{\sim}{c}_2)$ when and only when there exists some nonzero element σ of GF(q) such that

$\underset{\sim}{c}_2 = \sigma \underset{\sim}{c}_1$. Hamada [16] showed that there is the following connection between a min · hyper and an anticode.

Theorem 3.11. *Let k and q be any integer $\geqslant 3$ and any prime power, respectively, and let f and m be some integers such that $0 \leqslant m < f \leqslant v_k$. Let $\underset{\sim}{e}_l$ $(l = 1, 2, \ldots, f)$ be f nonzero vectors in $W(k; q)$ such that any two vectors in $(\underset{\sim}{e}_1, \underset{\sim}{e}_2, \ldots, \underset{\sim}{e}_f)$ are linearly independent. Then $\{(\underset{\sim}{e}_1), (\underset{\sim}{e}_2), \ldots, (\underset{\sim}{e}_f)\}$ is an $\{f, m; k-1, q\}$-min · hyper in $\mathrm{PG}(k-1, q)$ if and only if $[\underset{\sim}{e}_1, \underset{\sim}{e}_2 \ldots \underset{\sim}{e}_f]$ is a $k \times f$ generator matrix of a q-ary anticode with length f and maximum distance $f - m$.*

Remark 3.3. It is well known (cf. Ch. 17 Section 6 in MacWilliams and Sloane [29]) that in the case $k \geqslant 3$ and $d = q^{k-1} - \sum_{\alpha=0}^{k-2} \varepsilon_\alpha v_{\alpha+1}$ (or $d = q^{k-1} - (\varepsilon + \sum_{i=1}^{h} q^{\mu_i})$), there is a one-to-one correspence between the set of all $(n, k, d; q)$-codes meeting the Griesmer bound (1.4) and the set of all q-ary anticodes, generated by a $k \times f$ matrix whose any two column vectors are linearly independent over $\mathrm{GF}(q)$, with length f and maximum distance $f - m$ if we introduce some equivalence relation between two codes where $f = \sum_{\alpha=0}^{k-2} \varepsilon_\alpha v_{\alpha+1}$ and $m = \sum_{\alpha=0}^{k-2} \varepsilon_\alpha v_\alpha$ (or $f = \varepsilon + \sum_{i=1}^{h} v_{\mu_i+1}$ and $m = \sum_{i=1}^{h} v_{\mu_i}$). Hence Theorem 3.11 shows that in the case $k \geqslant 3$ and $d = q^{k-1} - \sum_{\alpha=0}^{k-2} \varepsilon_\alpha q^\alpha$ (or $d = q^{k-1} - (\varepsilon + \sum_{i=1}^{h} q^{\mu_i})$), there is a one-to-one corresondence between the set of all $(n, k, d; q)$-codes meeting the Griesmer bound (1.4) and the set of all $\{\sum_{\alpha=0}^{k-2} \varepsilon_\alpha v_{\alpha+1}, \sum_{\alpha=0}^{k-2} \varepsilon_\alpha v_\alpha; k-1, q\}$-min · hypers (or the set of all $\{\varepsilon + \sum_{i=1}^{h} v_{\mu_i+1}, \sum_{i=1}^{h} v_{\mu_i}; k-1, q\}$-min · hypers, resp.) if we introduce some equivalence relation between two $(n, k, d; q)$-codes.

Finally, we shall give the following example in order to show a connection between a $\{\sum_{i=1}^{h} v_{\mu_i+1} + \varepsilon, \sum_{i=1}^{h} u_{\mu_i}; k-1, q\}$-min · hyper and an $(n, k, d; q)$-code meeting the Griesmer bound in the case $d = q^{k-1} - (\varepsilon + \sum_{i=1}^{h} q^{\mu_i})$ where $(\varepsilon, \mu_1, \mu_2, \ldots, \mu_h) \in U(k-1, q)$ and $n = v_k - (\varepsilon + \sum_{i=1}^{h} v_{\mu_i+1})$ (cf. Theorem 5.2 and Example 5.1 in Hamada [16] in detail).

Example 3.1. Consider the case $k = 3$, $d = 4$ and $q = 3$. In this case, $h = 1$, $\varepsilon = 2$, $\mu_1 = 1$ and $v_3 = (3^3 - 1)/(3 - 1) = 13$. Let $\underset{\sim}{c}_i$ $(i = 1, 2, \ldots, 13)$ be 13 vectors given by

$\underset{\sim}{c}_1$	$\underset{\sim}{c}_2$	$\underset{\sim}{c}_3$	$\underset{\sim}{c}_4$	$\underset{\sim}{c}_5$	$\underset{\sim}{c}_6$	$\underset{\sim}{c}_7$	$\underset{\sim}{c}_8$	$\underset{\sim}{c}_9$	$\underset{\sim}{c}_{10}$	$\underset{\sim}{c}_{11}$	$\underset{\sim}{c}_{12}$	$\underset{\sim}{c}_{13}$
0	0	0	0	1	1	1	1	1	1	1	1	1
0	1	1	1	0	0	0	1	1	1	2	2	2
1	0	1	2	0	1	2	0	1	2	0	1	2.

Then any two vectors in $(\underset{\sim}{c}_1, \underset{\sim}{c}_2, \ldots, \underset{\sim}{c}_{13})$ are linearly independent over $\mathrm{GF}(3)$. Hence 13 points in $\mathrm{PG}(2, 3)$ can be expressed by $(\underset{\sim}{c}_1), (\underset{\sim}{c}_2), \ldots, (\underset{\sim}{c}_{13})$. Let $F = \{(\underset{\sim}{c}_1), (\underset{\sim}{c}_2), (\underset{\sim}{c}_3), (\underset{\sim}{c}_4), (\underset{\sim}{c}_5), (\underset{\sim}{c}_6)\}$, $G^* = [\underset{\sim}{c}_1\, \underset{\sim}{c}_2 \ldots \underset{\sim}{c}_6]$ and $G = [\underset{\sim}{c}_7\, \underset{\sim}{c}_8 \ldots \underset{\sim}{c}_{13}]$.

Let C^* be a subspace in $V(6;3)$ generated by 3 row vectors of G^* and let C be a subspace in $V(7;3)$ generated by 3 row vectors of G where $V(n;3)$ denotes an n-dimensional vector space consisting of row vectors over GF(3). Then it is easy to see that F is a $\{6,1;2,3\}$-min · hyper such that $F \in \mathfrak{F}(0,0,1;2,3)$ (i.e. F is a set of a 1-flat $\{(\underset{\sim}{c}_1),(\underset{\sim}{c}_2),(\underset{\sim}{c}_3),(\underset{\sim}{c}_4)\}$ and two 0-flats $(\underset{\sim}{c}_5)$ and $(\underset{\sim}{c}_6)$ in PG(2, 3) which are mutually disjoint) and C^* is a 3-ary anticode with length 6 and maximum distance 5 and C is a $(7,3,4;3)$-code meeting the Griesmer bound. In this case, C is said to be a $(7,3,4;3)$-code constructed by using 1-flat $\{(\underset{\sim}{c}_1),(\underset{\sim}{c}_2),(\underset{\sim}{c}_3),(\underset{\sim}{c}_4)\}$ and two 0-flats $(\underset{\sim}{c}_5)$ and $(\underset{\sim}{c}_6)$ in PG(2, 3).

4. A connection between a min · hyper and a linear programming derived from a BIB design

It is well known that there are v_{t+1} points and v_{t+1} hyperplanes in PG(t,q) where $v_{t+1}=(q^{t+1}-1)/(q-1)$. After numbering v_{t+1} hyperplanes and v_{t+1} points in PG(t,q) respectively in some way, let us denote v_{t+1} hyperplanes and v_{t+1} points in PG(t,q) by Π_i $(i=1,2,\ldots,v_{t+1})$ and Q_j $(j=1,2,\ldots,v_{t+1})$, respectively, and let $N=(n_{ij})$ where $n_{ij}=1$ or 0 according to whether or not the jth point Q_j in PG(t,q) is contained in the ith hyperplane Π_i in PG(t,q). Then N is the incidence matrix of a BIB design (denoted by PG$(t,q):t-1$) with parameters $(v_{t+1},v_{t+1},v_t,v_t,v_{t-1})$. Consider the following integral linear programming derived from the BIB design PG$(t,q):t-1$.

Problem C. Find a vector $(y_1,y_2,\ldots,y_{v_{t+1}})$ of integers y_j $(j=1,2,\ldots,v_{t+1})$ that minimize the summation $\sum_{j=1}^{v_{t+1}} y_j$ subject to the following inequalities:

$$0\leqslant y_j\leqslant\omega \quad (j=1,2,\ldots,v_{t+1}) \tag{4.1}$$

$$\sum_{j=1}^{v_{t+1}} n_{ij}y_j\geqslant m \quad (i=1,2,\ldots,v_{t+1}) \tag{4.2}$$

for given integers t, ω, m and q where $t\geqslant 2$, $\omega\geqslant 1$, $m\geqslant 0$ and $v_{t+1}=(q^{t+1}-1)/(q-1)$.

It is known that if there exist nonnegative integes y_j $(j=1,2,\ldots,v_{t+1})$ which satisfy conditions (4.1) and (4.2) for given integers t, ω, q and $m=\sum_{\alpha=1}^{t-1}\varepsilon_\alpha v_\alpha$, then

$$\sum_{j=1}^{v_{t+1}} y_j\geqslant\sum_{\alpha=1}^{t-1}\varepsilon_\alpha v_{\alpha+1}, \tag{4.3}$$

where $0\leqslant\varepsilon_\alpha\leqslant q-1$ for $\alpha=1,2,\ldots,t-1$. Hence we shall consider the following

Problem D. (1) Find a necessary and sufficient condition for an integer ω and an ordered set $(\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{t-1})$ in $E(t, q)$ that there exists a vector $(y_1, y_2, \ldots, y_{v_{t+1}})$ of integers y_j which satisfy the following conditions:

$$0 \leq y_j \leq \omega \quad (j = 1, 2, \ldots, v_{t+1}), \tag{4.4}$$

$$\sum_{j=1}^{v_{t+1}} y_j = \sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_{\alpha+1}, \tag{4.5}$$

$$\sum_{j=1}^{v_{t+1}} n_{ij} y_j \geq \sum_{\alpha=1}^{t-1} \varepsilon_\alpha v_\alpha \quad (i = 1, 2, \ldots, v_{t+1}). \tag{4.6}$$

(2) Find all vectors $(y_1, y_2, \ldots, y_{v_{t+1}})$ which satisfy conditions (4.4), (4.5) and (4.6) in the case where there exists such a vector for given integers.

Definition 4.1. Let F be a set of points in PG(t, q) and let w be a mapping of F into z^+ where $t \geq 2$ and z^+ denotes the set of all positive integers. Let $\mathfrak{H}$ be the set of all hyperplanes in PG(t, q). If F and w satisfy the following condition:

$$\sum_{P \in F} w(P) = f \text{ and } \min\left\{ \sum_{P \in F \cap H} w(P) \mid H \in \mathfrak{H} \right\} = m \tag{4.7}$$

for given integers $f \geq 1$ and $m \geq 0$, then (F, w) is said to be an $\{f, m; t, q\}$-min · hyper. In the special case $w(P) = 1$ for any point P in F, a min · hyper (F, w) is denoted simply by F.

Remark 4.1. In the special case $w(P) = 1$ for any point P in F, condition (4.7) can be expressed as follows:

$$|F| = f \text{ and } \min\{|F \cap H| \mid H \in \mathfrak{H}\} = m. \tag{4.8}$$

Hence a min · hyper F in Sections 1–3 is a min · hyper (F, w) such that $w(P) = 1$ for any point P in F.

Theorem 4.1 (Hamada [12]). *Let $\mathfrak{B}_y(t, \omega, \underline{\varepsilon}, q)$ be the set of all vectors $(y_1, y_2, \ldots, y_{v_{t+1}})$ of integers y_j which satisfy conditions* (4.4), (4.5) *and* (4.6) *and let $\mathfrak{B}_F(t, \omega, \underline{\varepsilon}, q)$ be the set of all $\{\sum_{\alpha=0}^{t-1} \varepsilon_\alpha v_{\alpha+1}, \sum_{\alpha=1}^{t-1} \varepsilon_\alpha v_\alpha; t, q\}$-min · hypers (F, w) such that $1 \leq w(P) \leq \omega$ for any point P in F where $t \geq 2$, $\omega \geq 1$, $0 \leq \varepsilon_\alpha \leq q - 1$ $(\alpha = 0, 1, \ldots, t-1)$ and $\underline{\varepsilon} = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{t-1})$. Then there is a one-to-one correspondence between the set $\mathfrak{B}_y(t, \omega, \underline{\varepsilon}, q)$ and the set $\mathfrak{B}_F(t, \omega, \underline{\varepsilon}, q)$ in the case $\underline{\varepsilon} \neq \underline{0}$.*

References

[1] L.D. Baumert and R.J. McEliece, A note on the Griesmer bound, Trans. Information Theory 19 (1973) 134–135.

[2] B.I. Belov, A conjecture on the Griesmer bound, in Optimization Methods and Their Applications, (Russian) (Sibirsk. Energet. Inst. Sibirsk. Otdel. Akad. Nauk SSSR, Irkutsk, 1974) 100–106.

[3] I.F. Blake and R.C. Mullin, The Mathematical Theory of Coding (Academic Press, New York 1975).
[4] R.C. Bose, Mathematical theory of the symmetrical factorial design, Sankhya 8 (1947) 107–166.
[5] R.C. Bose, On some connections between the design of experiments and information theory, Bull. Inst. Int. Statist. 38 (1961) 257–271.
[6] R.C. Bose and J.N. Srivastava, On a bound useful in the theory of factorial designs and error correcting codes, Ann. Math. Statist. 35 (1964) 408–414.
[7] R.D. Carmichael, Introduction to the Theory of Groups of Finite Groups (Dover Publications, New York, 1956).
[8] P. Dembowski, Finite Geometries (Springer-Verlag, Berlin, Heidelberg, New York, 1968).
[9] S.M. Dodunekov and N.L. Manev, Characterization theorems for two classes of codes meeting the Griesmer bound, Comptes rendus de l'Académie bulgare des Sciences 35 (1982) 751–752.
[10] P. G. Farrell, Linear binary anticode, Electron. Lett. 6 (1970) 419–421.
[11] J.H. Griesmer, A bound for error-correcting codes, IBM J. Res. Develop. 4 (1960) 532–542.
[12] N. Hamada, Characterization resp. nonexistence of certain q-ary linear codes attaining the Griesmer bound, Bull. Osaka Women's Univ. 22 (1985) 1–47.
[13] N. Hamada, A characterization of some $(n, k, d; q)$-codes meeting the Griesmer bound using a min · hyper in a finite projective geometry, to appear in Annals of Discrete Mathematics (Combinatorial Aspects of Design Experiments).
[14] N. Hamada, Characterization of $\{(q+1)+2, 1; t, q\}$-min · hypers and $\{2(q+1)+2, 2; 2, q\}$-min · hypers in a finite projective geometry, Graphs and Combinatorics 5 (1989) 63–81.
[15] N. Hamada, Characterization of $\{v_{\mu+1}+2v_{\mu}, v_{\mu}+2v_{\mu-1}; t, q\}$-min · hypers and its applications to error-correcting codes, Graphs and Combinatorics 5 (1989) 137–147.
[16] N. Hamada, Characterization of min · hypers in a finite projective geometry and its applications to error-correcting codes, Bull. Osaka Women's Univ. 24 (1987) 1–24.
[17] N. Hamada, Characterization of $\{12, 2; 2, 4\}$-min · hypers in a finite projective geometry PG(2, 4), Bull. Osaka Women's Univ. 24 (1987) 25–31.
[18] N. Hamada and M. Deza, Characterization of $\{2(q+1)+2, 2; t, q\}$-min · hypers in PG(t, q) $(t \geqslant 3, q \geqslant 5)$ and its applications to error-correcting codes, Discrete Mathematics 71 (1988) 219–231.
[19] N. Hamada and M. Deza, Characterization of $\{2v_{\alpha+1}+2v_{\beta+1}, 2v_{\alpha}+2v_{\beta}; t, q\}$-min · hypers in PG$(t, q)$ $(t \geqslant 2,\ q \geqslant 5$ and $0 \leqslant \alpha < \beta < t)$ and its applications to error-correcting codes, submitted.
[20] N. Hamada and M. Deza, Characterization of $(n, k, d; q)$-codes meeting the Griesmer bound for given integers $k \geqslant 3$, $q \geqslant 5$ and $d = q^{k-1} - q^{\alpha} - q^{\beta} - q^{\gamma}$ $(0 \leqslant \alpha \leqslant \beta < \gamma < k-1$ or $0 \leqslant \alpha < \beta \leqslant \gamma < k-1)$, in the First Sino-Franco Conference on Combinatorics, Algorithms, and Coding Theory, Bull. Inst. Math. Acad. Sinica 16 (1988) 321–338.
[21] N. Hamada and M. Deza, A characterization of $\{v_{\mu+1}+\varepsilon, v_{\mu}; y, q\}$-min · hypers and its applications to error-correcting codes and factorial designs, to appear in J. Statistical Planning and Inference 22 (1989).
[22] N. Hamada and F. Tamari, On a geometrical method of construction of maximal t-linearly independent sets, J. Combin. Theory (A) 25 (1978) 14–28.
[23] N. Hamada and F. Tamari, Construction of optimal codes and optimal fractional factorial designs using linear programming, Annals of Discrete Mathemat. 6 (1980) 175–188.
[24] N. Hamada and F. Tamari, Construction of optimal linear codes using flats and spreads in a finite projective geometry, Europ. J. Combinator. 3 (1982) 129–141.
[25] T. Helleseth, A characterization of codes meeting the Griesmer bound, Information and Control 50 (1981) 128–159.
[26] T. Helleseth, New construction of codes meeting the Griesmer bound, IEEE Trans. Information Theory IT-29 (1983) 434–439.
[27] T. Helleseth and H.C.A. van Tilborg, A new class of codes meeting the Griesmer bound, IEEE Trans. Information Theory IT-27 (1981) 548–555.
[28] D.R. Hughes and F.C. Piper, Projective Planes (Springer, New York, 1973).
[29] F.J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes (North-Holland Mathematical Library, Vol. 16, Amsterdam, 1977).

[30] G. Solomon and J.J. Stiffler, Algebraically punctured cyclic codes, Information and Control 8 (1965) 170–179.

[31] F. Tamari, A note on the construction of optimal linear codes, J. Statistical Planning and Inference 5 (1981) 405–411.

[32] F. Tamari, On an $\{f, m; t, s\}$-max · hyper and a $\{k, m; t, s\}$-min · hyper in a finite projective geometry PG(t, s), Bull. Fukuoka University of Education 31 (III) (1981) 35–43.

[33] F. Tamari, On linear codes which attain the Solomon–Stiffler bound, Discrete Mathematics 49 (1984) 179–191.

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 89–96
North-Holland

BIBD'S WITH BLOCK-SIZE SEVEN

H. HANANI
Technion, Israel Institute of Technology, Haifa, Israel

It is proved that the obvious necessary conditions for the existence of a BIBD with $k = 7$ and $\lambda = 3$ and 21 are sufficient except, perhaps, for the values $\lambda = 3$ and $v = 323, 351, 407, 519, 525, 575, 665$.

This paper is an addition to Section 5.5 of the paper [0]. All the theorems and lemmas referred to as well as all the relevant definitions may be found in [0]. The lemmas and tables in the sequel of this paper will be numbered from 101 up. We start with a list of group divisible designs $v \in GD(7, 1, 7)$.

Table 101

v GD[7, 1, 7; v]

49 $X = I(7) \times I(7)$.
Form $T[7, 1; 7]$ on X.

91 $X = Z(7, 3) \times Z(13, 2)$.
$P = \langle(\emptyset; \emptyset), (2\alpha; 4\alpha + 6\beta + 3\gamma) : \alpha = 0, 1, 2; \beta = 0, 1\rangle \mathrm{mod}(7; 13)$, $\gamma = 0, 1$.

217 $X = Z(7, 3) \times Z(31, 3)$.
$P = \langle(\emptyset; \emptyset), (2\alpha; 10\alpha + 15\beta + 3\gamma) : \alpha = 0, 1, 2; \beta = 0, 1\rangle \mathrm{mod}(7, 31)$,
$\gamma = 0, 1, 2, 3, 4$.

301 $X = Z(7, 3) \times Z(43, 3)$.
$P = \langle(\emptyset; \emptyset), (2\alpha; 7\alpha + 21\beta + 3\gamma) : \alpha = 0, 1, 2; \beta = 0, 1\rangle \mathrm{mod}(7; 43)$,
$\gamma = 0, 1, \ldots, 6$.

343 $X = I(7) \times I(49)$.
Form $B[7, 1; 49]$ on $I(49)$ by Theorem 2.2 and for every block B of this design form $T[7, 1; 7]$ on $I(7) \times B$.

427 $X = Z(7, 3) \times Z(61, 2)$.
$P = \langle(\emptyset; \emptyset), (2\alpha; 28\alpha + 30\beta + 3\gamma) : \alpha = 0, 1, 2; \beta = 0, 1\rangle \mathrm{mod}(7; 61)$,
$\gamma = 0, 1, \ldots, 9$.

469 $X = Z(7, 3) \times Z(67, 2)$.
$P = \langle(\emptyset; \emptyset), (2\alpha; 26\alpha + 33\beta + 3\gamma) : \alpha = 0, 1, 2; \beta = 0, 1\rangle \mathrm{mod}(7; 67)$,
$\gamma = 0, 1, \ldots, 10$.

511 $X = Z(7, 3) \times Z(73, 5)$.
$P = \langle(\emptyset; \emptyset),\ (2\alpha; 25\alpha + 36\beta + 3\gamma): \alpha = 0, 1, 2;\ \beta = 0, 1\rangle \mathrm{mod}(7; 73)$,
$\gamma = 0, 1, \ldots, 11$.

553 $X = Z(7, 3) \times Z(79, 3)$.
$P = \langle(\emptyset; \emptyset),\ (2\alpha; 13\alpha + 3\gamma): \alpha = 0, 1, 2, 3, 4, 5\rangle \mathrm{mod}(7, 79)$,
$\gamma = 0, 1, \ldots, 12$.

637 $X = I(7) \times I(91)$.
As above $91 \in \mathrm{GD}(7, 1, 7)$. By Lemma 2.10 form $B[7, 1; 91]$ on $I(91)$ and for every block B of this design form $T[7, 1; 7]$ on $I(7) \times B$.

679 $X = Z(7, 3) \times Z(97, 5)$.
$P = \langle(\emptyset; \emptyset),\ (2\alpha; 16\alpha + 3\gamma): \alpha = 0, 1, 2, 3, 4, 5\rangle \mathrm{mod}(7, 97)$,
$\gamma = 0, 1, \ldots, 15$.

By Lemma 2.10 for every v in Table 101 $v \in B(7, 1) \subset B(7, 3)$ holds. Further we have

Table 102

v $B[7, 1; v]$

169 $X = Z(13, 2) \times Z(13, 2)$.
$B = \langle \emptyset, \emptyset),\ (\emptyset, 4\alpha + 3),\ (4\alpha, \emptyset): \alpha = 0, 1, 2\rangle \mathrm{mod}(13, 13)$,
$\langle \emptyset, \emptyset),\ (4\alpha + 1, 4\alpha + 4\beta),\ (4\alpha + 7, 4\alpha + 4\beta + 1): \alpha = 0, 1, 2\rangle \mathrm{mod}(13, 13)$,
$\beta = 0, 1, 2$.

385 $X = I(6) \times I(64) \cup \{\infty\}$.
Form, by Theorem 2.2, $B[8, 1; 64]$ on $I(64)$ and for every block B of this design form $B[7, 1; 49]$ on $I(6) \times B \cup \{\infty\}$ in such way that it includes as blocks the sets $I(6) \times \{i\} \cup \{\infty\}$, $i \in B$;
delete these blocks, but leave each of them once.

We shall now prove an auxiliary lemma which will be used later.

Lemma 101. $32 \in \mathrm{GD}(7, 3, 4)$.

$X = \mathrm{GF}(4, x^2 = x + 1) \times (Z(7, 3) \cup \{\infty\})$.

$P = \langle(\emptyset; \emptyset),\ (\emptyset; \alpha): \alpha = 0, 1, \ldots, 5\rangle$,
$\langle(\emptyset; \emptyset)(\alpha; 2\alpha - \beta): \alpha = 0, 1, 2;\ \beta = 0, 1\rangle \mathrm{mod}(-, 7)$,
$\langle(\emptyset; \infty),\ (\emptyset; 2\alpha)(\alpha; 2\alpha - 1): \alpha = 0, 1, 2;\rangle \mathrm{mod}(-, 7)$,
$\langle(\emptyset; \infty),\ (\alpha; 2\alpha + 3\beta): \alpha = 0, 1, 2;\ \beta = 0, 1,\rangle \mathrm{mod}(-, 7)$,
$\langle(\gamma, \infty),\ (\emptyset; 2\beta + 2\gamma + 1),\ (\gamma; 2\gamma - 1),\ (\gamma + 2; 2\alpha): \alpha = 0, 1, 2;\ \beta = 0, 1\rangle \mathrm{mod}(-, 7)$,
$\gamma = 0, 1, 2$,
$\langle(\gamma; \infty),\ (\emptyset; \emptyset),\ (\gamma; 2\beta + 2\gamma + 3),\ (\gamma + 1; 2\alpha): \alpha = 0, 1, 2: \beta = 0, 1\rangle \mathrm{mod}(-, 7)$,
$\gamma = 0, 1, 2$.

Lemma 102. *If* $u = 0$ *or* $3 \pmod 7$, *and* $u \notin \{161, 175, 203, 259, 262, 287, 332\} = E$ *then* $u \in \mathrm{GD}(\{7, 8\}, 1, M_7)$ *holds, where*

$$M_7 = \{3, 7, 10, 14, 17, 21, 24, 28, 31, 35, 38, 42, 45, 59, 63, 66, 70, 73, 77, 80, 84, 87, 91, 94, 98, 101, 105, 108, 112, 115, 140, 143, 147, 150, 154, 157, 164, 168, 171, 178, 182, 185, 189, 192, 196, 199, 206, 210, 213, 252, 255, 266, 269, 273, 276, 280, 283, 290, 294, 297, 301, 304, 308, 311, 315, 318, 322, 325, 329, 336, 339, 507\}.$$

Proof. According to Lemma 2.13 with $t = 1$, $s = 7$, $r \equiv 0$ or $3 \pmod 7$ it may be checked that if $u \geqslant 539$, then there exists (use Theorem 3.7 and Remark) a transversal design $T[7+1, 1; r]$ such that by truncating one of its groups $7r + r_1 = u$ is obtained. Clearly $r_1 \equiv 0$ or $3 \pmod 7$ and there is no difficulty in avoiding the situations where either $r \in E$ or $r_1 \in E$. For $u < 539$ use the truncated transversal design $T[7+1, 1; r]$ with values of r as in Table 103. □

Table 103

u	*r*	*u*	*r*
49–56	7	395–448	56
119–136	17	451–504	63
217–248	31	511–539	73
343–392	49		

Theorem 103. *If* $v \equiv 1$ *or* $7 \pmod{14}$, *and* $v \notin \{323, 351, 407, 519, 525, 575, 665\} = 2E + 1$, *then* $v \in B(7, 3)$ *holds.*

Proof. Let $v = 2u + 1$, where $u \equiv 0$ or $3 \pmod 7$. By Lemma 101, $u \in \mathrm{GD}(\{7, 8\}1, M_7)$. By Lemmas 2.26 and 4.29 it suffices to show that $v = 2\mu + 1 \in B(7, 3)$ for every $\mu \in M_7$. The case $v = 7$ is trivial.

$\{49, 91, 169, 217, 301, 343, 385, 427, 511, 553, 631, 637, 679\} \subset B(7, 1)$ as shown in Tables 101 and 102, $\{29, 43, 71, 127, 197, 211, 281, 337, 379, 421, 547, 617, 659, 673\} \subset B(7, 3)$ by Lemma 4.3. $\{63, 77, 119, 133, 161, 175, 189, 203, 287, 329, 371, 413, 567, 581, 623\} \subset B(7, 3)$ by Lemmas 4.26 and 2.10. $\{15, 21, 57, 141, 147, 183\} \subset B(7, 3)$ is shown in Table 5.21. It remains to prove that $\{35, 85, 155, 225, 231, 295, 309, 315, 323, 351, 357, 365, 393, 399, 407, 505, 519, 525, 533, 539, 561, 575, 589, 595, 603, 609, 645, 651, 665, 1015\} \subset B(7, 3)$ which is shown in Table 104 with the possible exception of $\{323, 351, 407, 519, 525, 575, 665\}$ for which we do not know whether $B[7, 3; v]$ exists.

We go over now to the case $\lambda = 21$.

Table 104

v	$B[7, 3; v]$
35	$X = Z(5, 2) \times Z(7, 3)$. Form $T[7, 2; 5]$ on $Z(5) \times Z(7)$ and the blocks $\langle(\emptyset, 2\alpha), (\beta, \emptyset) : \alpha = 0, 1, 2;\ \beta = 0, 1, 2, 3\rangle \bmod(5, 7)$.
85	$X = Z(5, 2) \times Z(17, 3)$. $B = \langle(\emptyset, \emptyset),\ (\gamma, 8\alpha + 4\gamma + 1),\ (\gamma + 1, 8\alpha + 4\gamma + 3),\ (\gamma + 3, 8\alpha + 4\gamma + 7):$ $\alpha = 0, 1\rangle \bmod(5, 17),\ \gamma = 0, 1,$ $\langle(\emptyset; \emptyset),\ (\gamma, 8\alpha + 4\gamma + 7),\ (\gamma + 1, 8\alpha + 4\gamma + 2),\ (\gamma + 3, 8\alpha + 4\gamma + 4):$ $\alpha = 0, 1\rangle \bmod(5, 17),\ \gamma = 0, 1,$ $\langle(\emptyset, \emptyset),\ (2\alpha + \gamma, 4\gamma + 1),\ (2\alpha + \gamma,\ 4\gamma + 2),\ (2\alpha + \gamma, 4\gamma + 5):$ $\alpha = 0, 1\rangle \bmod(5, 17),\ \gamma = 0, 1.$
155	$X = Z(5, 2) \times Z(31, 3)$ $B = \langle(\emptyset, \emptyset),\ (2\delta, 10\alpha + 3\gamma),\ (2\delta + 2, 10\alpha + 3\gamma + 4) : \alpha = 0, 1, 2\rangle \bmod(5, 31),$ $\gamma = 0, 1;\ \delta = 0, 1,$ $\langle(\emptyset, 10\alpha + 1),\ (\beta, \emptyset) : \alpha = 0, 1, 2;\ \beta = 0, 1, 2, 3\rangle \bmod(5, 31),$ $\langle(\emptyset, \emptyset), (0, 15\alpha + 5\gamma),\ (1, 15\alpha + 5\gamma + 1),\ (3, 15\alpha + 5\gamma - 1) : \alpha = 0, 1\rangle$ $\bmod(5, 31),\ \gamma = 0, 1, 2,$ $\langle(\emptyset, \emptyset),\ (0, 15\alpha + 5\gamma + 2),\ (1, 15\alpha + 5\gamma - 2),\ (3, 15\alpha + 5\gamma) : \alpha = 0, 1\rangle$ $\bmod(5, 31),\ \gamma = 0, 1, 2.$
255	$X = I(4) \times I(56) \cup \{\infty\}$ Form GD[8, 1, 7; 56] on $I(56)$ by Lemma 2.12 and Theorem 2.1. For every group G of this design form $B[7, 3; 29]$ on $I(4) \times G \cup \{\infty\}$, and for every block B form GD[7, 3, 4; 32] on $I(4) \times B$ by Lemma 101.
231	We prove $231 \in \mathrm{GD}(7, 3, 21)$. $X = (Z(3) \times Z(7, 3)) \times Z(11, 2)$. $P = \langle(\emptyset, \emptyset; 2\beta),\ (\emptyset, \emptyset; 2\beta + 3),\ (\emptyset, 2\alpha + 4; 2\beta + 4),\ (\emptyset, 2\alpha + 5; 2\beta + 6),$ $(1, \emptyset; 2\beta + 2),\ (0, 2\alpha; 2\beta + 1),\ (1, 2\alpha + 2;\ 2\beta + 5) > \bmod(3, 7; 11),$ $\alpha = 0, 1, 2;\ \beta = 0, 1, 2, 3, 4.$ Further form $B[7, 3; 21]$ on $(Z(3) \times Z(7)) \times \{i\},\ i \in Z(11)$.
295	$X = I(42) \times I(7) \cup \{\infty\}$ Form $T[7, 3; 42]$ on $I(42) \times I(7)$ and $B[7, 3; 43]$ on $I(42) \times \{i\} \cup \{\infty\}$, $i \in I(7)$.
309	$X = I(7) \times (I(6) \times Z(7, 3) \cup \{(i, \infty) : i = 0, 1\}) \cup \{(\infty, \infty)\}$ Form GD[7, 3, $\{6, 2^*\}$; 44] on $I(6) \times Z(7) \cup \{(i, \infty) : i = 0, 1\}$ as follows: form $T[7, 2; 6]$ on $I(6) \times Z(7)$ and the blocks $\{(\beta, \alpha) : \alpha \in Z(7)\},\ \beta \in I(6)$ and $\{(\gamma, \infty), (\alpha, \alpha(\beta + 3\gamma + 1) : \alpha \in I(6)\} \bmod(-, 7),\ \beta = 0, 1, 2;\ \gamma = 0, 1.$ Now for every group G of this design form $B[7, 3; 43]$ and $B[7, 3; 15]$ respectively on $I(7) \times G \cup \{(\infty, \infty)\}$ and for every block B form $T[7, 1; 7]$ on $I(7) \times B$.

* The asterisk means that there is exactly one group of size 2, all other groups being of size 6.

315 $X = I(7) \times Z(3) \times Z(3) \times Z(5))$
Form GD[7, 3, 3; 45] on $(Z(3) \times Z(3) \times Z(5))$ with blocks $\langle(\emptyset; \emptyset, \emptyset),\ (0; \alpha, \emptyset),\ (1; \alpha, \alpha + 2\beta) : \alpha = 0, 1;\ \beta = 0, 1\rangle \bmod(3; 3, 5)$ $\langle(0; \emptyset, \emptyset),\ (\emptyset; \gamma, \emptyset),\ (0; 1 - \gamma, \emptyset),\ (1; \alpha, \alpha + 2\beta) : \alpha = 0, 1;\ \beta = 0, 1\rangle$ $\bmod(3; 3, 5)$, $\gamma = 0, 1$; For every group G of this design form $B[7, 3; 21]$ on $I(7) \times G$, and for every block B form GD[7, 1, 7; 49] on $I(7) \times B$.

357 $X = Z(2) \times \mathrm{GF}(25, x^2 = 2x + 2) \times Z(7, 3) \cup \{(\infty, i) : i \in Z(7)\}$.
B = Blocks of $T[7, 3; 50]$ on $(Z(2) \times \mathrm{GF}(25)) \times Z(7)$, $\langle(\infty, \emptyset),\ (\emptyset, 8\alpha + 2, \emptyset),\ (0, 8\alpha + 2, \emptyset) : \alpha = 0, 1, 2\rangle \bmod(-, 25, 7)$, $\langle(\infty, \beta), (\emptyset, 8\alpha + \beta, \emptyset), (0, 8\alpha - \beta + 1, \emptyset) : \alpha = 0, 1, 2\rangle \bmod(-, 25, 7), \beta = 0, 1$, $\langle(\infty, \beta + 2), (\emptyset, 8\alpha + \beta + 2, \emptyset), (0, 8\alpha - \beta + 3, \emptyset) : \alpha = 0, 1, 2\rangle \bmod(-, 25, 7)$, $\beta = 0, 1$,
$\langle(\emptyset, \emptyset, \emptyset), (0, 8\alpha, \emptyset), (0, 8\alpha + 1, \emptyset) : \alpha = 0, 1, 2\rangle \bmod(2, 25, 7)$,
$\langle(\infty, \emptyset), (\infty, \alpha) : \alpha = 0, 1, \ldots, 5\rangle$ 3 times.

365 $X = I(4) \times I(91) \cup \{\infty\}$.
Form GD[7, 1, 7; 91] on $I(91)$ as in Table 101. For every group G of this design form $B[7, 3; 29]$ on $I(4) \times G \cup \{\infty\}$, and for every block B form $T[7, 3; 4]$ on $I(4) \times B$.

393 $X = I(56) \times I(7) \cup \{\infty\}$.
Form $T[7, 3; 56]$ on $I(56) \times I(7)$ and $B[7, 3; 57]$ on $I(56) \times \{i\} \cup \{\infty\}$, $i \in I(7)$.

399 $X = I(57) \times I(7)$.
Form $T[7, 3; 57]$ on $I(57) \times I(7)$ and $B[7, 3; 57]$ on $I(57) \times \{i\}$, $i \in I(7)$.

505 $X = I(7) \times (I(8) \times I(9)) \cup \{\infty\}$.
Form $T[9, 1; 8]$ on $I(8) \times I(9)$. for every group G of this design.
Form $B[7, 3; 57]$ on $I(7) \times G \cup \{\infty\}$, and for every block B form GD[7, 3, 7; 63] on $I(7) \times B$ by Lemma 4.26.

533 $X = I(76) \times I(7) \cup \{\infty\}$.
Form $T[7, 3, 76]$ on $I(76) \times I(7)$ and $B[7, 3; 77]$ on $I(76) \times \{i\} \cup \{\infty\}$, $i \in I(7)$.

539 $X = I(77) \times I(7)$,
Form $T[7, 3, 77]$ on $I(77) \times I(7)$ and $B[7, 3; 77]$ on $I(77) \times \{i\}$, $i \in I(7)$.

561 $X = I(7) \times I(80) \cup \{\infty\}$.
Form GD[9, 1, 8; 80] on $I(80)$ by Lemma 2.12 and Theorem 2.2.
For every group G of this design form $B[7, 3; 57]$ on $I(7) \times G \cup \{\infty\}$, and for every block B form GD[7, 3, 7; 63] on $I(7) \times B$ by Lemma 4.26.

589 $X = I(84) \times I(7) \cup \{\infty\}$.
Form $T[7, 3, 84]$ on $I(84) \times I(7)$ and $B[7, 3; 85]$ on $I(84) \times \{i\} \cup \{\infty\}$, $i \in I(7)$.

595 $X = I(85) \times I(7)$.
Form $T[7, 3, 85]$ on $I(85) \times I(7)$ and $B[7, 3; 85]$ on $I(85) \times \{i\}$, $i \in I(7)$.

603 $X = I(84) \times I(7) \cup I(15)$.
The construction of $B[7, 3; 99]$ shows that it contains $B[7, 3; 15]$.
Form $B[7, 3; 99]$ on $I(84) \times \{i\} \cup I(15)$, $i \in I(7)$ in such way that it contains $B[7, 3, 15]$ on $I(15)$ and take this $B[7, 3; 15]$ once only. Further form $T[7, 3, 84]$ on $I(84) \times I(7)$.

609 $X = I(29) \times I(21)$.
Form $T[21, 1; 29]$. On every group G of this design form $B[7, 3; 29]$, and on every block B form $B[7, 3; 21]$.

645 $X = I(90) \times I(7) \cup I(15)$.
The construction of $B[7, 3; 105]$ shows that it contains $B[7, 3; 15]$.
Form $B[7, 3; 105]$ on $I(90) \times \{i\} \cup I(15)$, $i \in I(7)$ in such way that it contains $B[7, 3, 15]$ on $I(15)$ and take this $B[7, 3; 15]$ once only. Further form $T[7, 3; 90]$ on $I(90) \times I(7)$.

651 We prove $651 \in \mathrm{GD}(7, 3, 21)$. $X = (Z(3) \times Z(7, 3)) \times Z(31, 3)$. $P = \langle(\emptyset, \emptyset; 2\beta), \quad (\emptyset, \emptyset; 2\beta + 3), \quad (\emptyset, 2\alpha + 4; 2\beta + 4), \quad (\emptyset, 2\alpha + 5; 2\beta + 6), \quad (1, \emptyset; 2\beta + 2), \quad (0, 2\alpha; 2\beta + 1), \quad (1, 2\alpha + 2; 2\beta + 5)\rangle \bmod (3, 7; 31)$, $\alpha = 0, 1, 2$; $\beta = 0, 1, \ldots, 14$; Further form $B[7, 3; 21]$ on $(Z(3) \times Z(7)) \times \{i\}$, $i \in Z(31)$.

1015 $X = I(29) \times I(35)$.
Form $B[7, 3, 35]$ on $I(35)$ and for every block B of this design form $T[7, 1; 29]$ on $I(29) \times B$. Further form $B[7, 3; 29]$ on $I(29) \times \{i\}$, $i \in I(35)$.

Lemma 104. *If* $u \geq 3$, *then* $u \in \mathrm{GD}(\{7, 8\}, 1, M_7')$ *holds, where* $M_7' = \{3, 4, \ldots, 48, 50, 51, 57, 58, 65, 73, 74, 75, 76, 78, 79, 89, 90, 92, 93, 105, 106, 107, 108, 109, 110, 111, 113, 114, 153, 154, 155, 156, 157, 158, 159, 160, 162, 163, 257, 258, 260, 261\}$.

Proof. According to Lemma 3.13 with $t = 1$, $s = 7$, $r \geq 7$, $r_1 \geq 3$, it may be checked that if $u \geq 542$, then there exists (use Theorem 3.7 and Remark) a transversal design $T[7 + 1, 1; r]$ such that by truncating one of its groups $7r + r_1 = u$ is obtained. for $u < 542$ use $T[7 + 1, 1; r]$ with values of r as in Table 105. □

Table 105

u	r	u	r	u	r
49	7	115–128	16	259	37
52–56	7	129–136	17	262–296	37
59–64	8	137–152	19	297–328	41
66–72	9	161	23	329–344	43
77	11	164–184	23	345–376	46
80–88	11	185–200	25	377–424	53
91	13	201–216	27	425–472	59
94–104	13	217–232	29	473–536	67
112	16	233–256	32	537–542	73

Lemma 105. *If $v = 3q$, where $q \equiv 1 \pmod 6$ is a prime-power, then $v \in B(7, 21)$.*

Proof. Consider Lemma 4.2. By this lemma $q \in B(7, 7)$. Form $B[7, 21; v]$ as follows. Let $X = I(3) \times I(q)$. On $I(q)$ form $B[7, 7; q]$ as in Lemma 4.2. For blocks B obtained for $\alpha = 0$ form $B[7, 3; 21]$ on $I(3) \times B$. For other blocks B' form $T[7, 3; 3]$ on $I(3) \times \dot{B}'$. □

Lemma 106. *If $v = 5q$, where $q \equiv 1 \pmod 6$ is a prime-power, then $v \in B(7, 21)$.*

Proof. As in Lemma 105, $q \in B(7, 7)$. Form $B[7, 21; v]$ as follows. Let $X = I(5) \times I(q)$. On $I(q)$ form $B[7, 7; q]$. For blocks B obtained for $\alpha = 0$ form $B[7, 3; 35]$ on $I(5) \times B$. For other blocks B' form $T[7, 3; 5]$ on $I(5) \times B'$. □

Theorem 107. *If $v \equiv 1 \pmod 2$, $v \geqslant 7$, then $v \in B(7, 21)$ holds.*

Proof. Let $v = 2u + 1$, where $u \geqslant 3$. By Lemma 104, $u \in \mathrm{GD}(\{7, 8\}, 1, M_7')$. By Lemmas 2.26 and 4.29 it suffices to show that $v = 2\mu + 1 \in B(7, 21)$ for every $\mu \in M_7'$. $\{7, 13, 19, 25, 31, 37, 43, 49, 55, 61, 67, 73, 79, 85, 91, 97, 103, 115, 151, 157, 181, 187, 211, 217, 223, 229, 307, 313, 319, 325, 517, 523\} \subset B(7, 7)$ by Lemma 5.38; $\{15, 21, 29, 35, 57, 63, 71, 77, 147, 309, 315\} \subset B(7, 3)$ by Lemma 103; $\{9, 11, 17, 23, 27, 41, 47, 53, 59, 81, 83, 89, 101, 131, 149, 179, 227, 311, 317, 521, 523\} \subset B(7, 21)$ by Lemma 4.2; for $\{33, 39, 45\} \subset B(7, 21)$ see Table 5.22, $\{65, 75, 93, 95, 185, 215, 219, 327, 515\} \subset B(7, 21)$ by Lemmas 105 and 106. It remains to prove that $\{51, 69, 87, 117, 153, 159, 213, 221, 321\} \subset B(7, 21)$, which is shown in Table 106. □

Table 106

v	B[7, 21, v]
51	$X = Z(3) \times Z(17, 3)$. $B = \langle(\emptyset, \emptyset), (\emptyset, 8\alpha + \gamma + 4), (\beta, 8\alpha + \beta + \gamma) : \alpha = 0, 1;\ \beta = 0, 1\rangle \bmod(3, 17)$, $\gamma = 0, 1, \ldots, 15$, $\langle(\emptyset, \emptyset), (\emptyset, \alpha + 4\gamma), (\emptyset, \alpha + 4\gamma + 10), (\alpha, \emptyset) : \alpha = 0, 1\rangle \bmod(3, 17)$, $\gamma = 0, 1$, $\langle(\emptyset, \emptyset), (\emptyset, 3\alpha + 4\gamma - 1), (\emptyset, \alpha + 4\gamma + 8), (\alpha, \emptyset) : \alpha = 0, 1\rangle \bmod(3, 17)$, $\gamma = 0, 1$, $\langle(\emptyset, \emptyset), (\alpha, 4\alpha + \gamma), (\beta, \emptyset) : \alpha = 0, 1, 2, 3;\ \beta = 0, 1\rangle \bmod(3, 17)$, $\gamma = 0, 1, 2$ $\langle(\emptyset, \emptyset), (0, 4\alpha + 3), (0, 8\beta + 4\gamma) : \alpha = 0, 1, 2, 3; \beta = 0, 1\rangle \bmod(3, 17)$, $\gamma = 0, 1$.
69	$X = \mathrm{GF}(9, x^2 = 2x + 1) \times Z(7, 3) \cup I(4) \cup I(2)$. Form $B[7, 3; 63]$ on $\mathrm{GF}(9) \times Z(7)$ and $T[7, 1; 9]$ on $\mathrm{GF}(9) \times Z(7)$ 8 times. Further form $B[7, 3; 15]$ on $\mathrm{GF}(9) \times \{i\} \cup I(4) \cup I(2)$, $i \in Z(7)$ and blocks $\langle(j), (\alpha + 4\beta + j, \emptyset) : \alpha = 0, 1, 2; \beta = 0, 1\rangle \bmod(9, 7)$, $j \in I(4)$. Now form $\mathrm{RT}[7, 1; 9]$ on $\mathrm{GF}(9) \times Z(7)$, twice and obtain 18, parallel classes of blocks. For every $j \in I(4)$ chose two such parallel classes and for every $j \in I(2)$—three classes. For every $j \in I(4) \cup I(2)$ and for every block $B = \{0, 1, 2, 3, 4, 5, 6\}$ of the chosen classes form blocks $\{j\} \cup \{0, 1, 2, 3, 4, 5\}$ mod 7, and the blocks of the remaining 4 classes take 5 times each.

87 $X = I(3) \times I(29)$.
Form $B[7, 3; 29]$ on $I(29)$ as in Lemma 4.3. For blocks B obtained with $\alpha = 0$ form $B[7, 3; 21]$ and $T[7, 4; 3]$ on $I(3) \times B$. For other blocks B' form $T[7, 7; 3]$ on $I(3) \times B'$.

117 $X = I(13) \times I(9)$.
Form $T[9, 1; 13]$ on $I(13) \times I(9)$. On every block B of this design form $B[7, 21; 9]$ and on every group G form $B[7, 21; 13]$.

153 $X = I(17) \times I(9)$.
Form $T[9, 1; 17]$ on $I(17) \times I(9)$. On every block B of this design form $B[7, 21; 9]$ and on every group G form $B[7, 21; 17]$.

159 $X = I(25) \times I(6) \cup I(8) \cup \{\infty\}$.
Form RT[6, 1; 25] on $I(25) \times I(6)$, 7 times and obtain 175 parallel classes of blocks of size 6. For every $i \in I(8)$ chose 21 such parallel classes and for $\{\infty\}$, chose the remaining 7 classes. Now for every block B of the respective chosen classes form $B \cup \{i\}$, $i \in I(8)$ and $B \cup \{\infty\}$ respectively. Further form $B[7, 7; 151]$ on $I(25) \times I(6) \cup \{\infty\}$ twice by Lemma 5.38 and $B[7, 7; 25]$ on $I(25) \times \{j\}$, $j \in I(6)$, by Lemma 5.38. Also form $B[7, 21; 9]$ on $I(8) \cup \{\infty\}$.

213 $X = I(3) \times I(71)$.
Form $B[7, 3; 71]$ on $I(71)$ as in Lemma 4.3. For blocks B obtained with $\alpha = 0$. Form $B[7, 3; 21]$ and $T[7, 4; 3]$ on $I(3) \times B$. For other blocks B' form $T[7, 7; 3]$ on $I(3) \times B'$.

221 $X = I(17) \times I(13)$.
Form $T[13, 1; 17]$ on $I(17) \times I(13)$. On every block B of this design form $B[7, 21; 13]$ and on every group G form $B[7, 21; 17]$.

321 $X = Z(43, 3) \times Z(7, 3) \cup I(19) \cup \{\infty\}$.
Form $B[7, 3; 301]$ on $Z(43) \times Z(7)$ and $T[7, 1; 43]$, 13 times on $Z(43) \times Z(7)$. Further form $B[7, 3; 63]$ on $Z(43) \times \{i\} \cup I(19) \cup \{\infty\}$, $i \in Z(7)$ and blocks $\langle (j),\ (\alpha + 21\beta + j, \emptyset) : \alpha = 0, 1, 2;\ \beta = 0, 1\rangle \bmod (43, 7)$, $j \in I(19)$ and $\langle (\infty),\ (\alpha + 21\beta + j, \emptyset) : \alpha = 0, 1, 2;\ \beta = 0, 1\rangle \bmod (43, 7)$, $j \in \{19, 20\}$. Now form RT[7, 1; 43] on $Z(43) \times Z(7)$ and obtain 43 parallel classes of blocks. For every $j \in I(19)$ chose two such parallel classes and for ∞ one class. For every $j \in I(19) \cup \{\infty\}$ and every block $B = \{0, 1, 2, 3, 4, 5, 6\}$ of the chosen classes form blocks $\{j\} \cup \{0, 1, 2, 3, 4, 5\} \bmod 7$, and the blocks of the remaining 4 classes take 5 times each.

Reference

[0] H. Hanani, Balanced incomplete block designs and related designs, Discr. Math. 11 (1975) 255–269.

Discrete Mathematics 77 (1989) 97–121
North-Holland

ON ALSPACH'S CONJECTURE

Katherine HEINRICH
Department of Mathematics and Statistics, Simon Fraser University, Burnaby, B.C., Canada V5A 1S6

Peter HORÁK
Katedra matematiky SvF SVŠT, Radlinského 11, 81368 Bratislava, Czechoslovakia

Alexander ROSA
Department of Mathematics and Statistics, McMaster University, Hamilton, Ontario, Canada L8S 4K1

Dedicated to Haim Hanani on his 75th birthday.

1. Introduction

Several years ago B. Alspach asked the following question. If n is odd and $a_1 + a_2 + \cdots + a_m = n(n-1)/2$ (if n is even and $a_1 a_2 + \cdots + a_m = n(n-2)/2$), $3 \leq a_i \leq n$, can the edges of the complete graph K_n (the edges of $K_n - F$, the complete graph from which a 1-factor has been removed) be partitioned into m cycles $C_{a_1}, C_{a_2}, \ldots, C_{a_m}$ where C_{a_i} has length a_i [1]?

When all cycles are required to have the same length, we have the well known uniform cycle decomposition problem on which considerable work has been done, although the problem is still far from solved. For details on this problem, the reader is referred to the forthcoming survey paper by Alspach, Bermond, Heinrich, Rosa and Sotteau [2].

The third author has shown that when $n \leq 10$, all possible edge-partitions into cycles exist [8]. Sun [11] has shown that if m and n are odd, then there exist positive integers a, b and c so that $K_{mn} = aC_m + bC_{2m} + cC_n$. In this paper we consider the following three situations:

(i) $a_i \in \{n-2, n-1, n\}$, $1 \leq i \leq m$,

(ii) $a_i \in \{3, 4, 6\}$, $1 \leq i \leq m$ and

(iii) $a_i \in \{2^k, 2^{k+1}\}$, $k \geq 2$.

We will show in each case that if $a_1 + a_2 + \cdots + a_m = n(n-1)/2$ or $n(n-2)/2$, then an edge partition of the relevant graph (K_n or $K_n - F$) exists.

We first need some notation. Let G be a graph of even degree with $|V(G)| = n$. Let $S = \{b_1, b_2, \ldots, b_t\}$, $3 \leq b_i \leq n$, and suppose that $m_1 b_1 + m_2 b_2 + \cdots + m_t b_t = |E(G)|$. If the edge-set of G can be partitioned into m_1 cycles of length b_1, m_2 cycles of length $b_2, \ldots,$ and m_t cycles of length b_t, we will write $G = m_1 C_{b_1} + m_2 C_{b_2} + \cdots + m_t C_{b_t}$. If $m_i = 1$, $m_i C_{b_i}$ will be written as C_{b_i}. (We

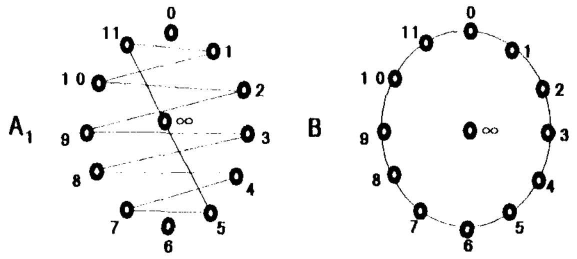


Fig. 1

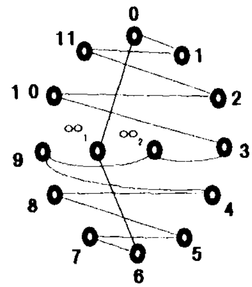


Fig. 2

may also refer to this edge partition of G as a decomposition of G into m_1 cycles of length b_1, m_2 of length $b_2, \ldots,$ and m_r cycles of length b_r.) More generally we will write $G = m_1H_1 + m_2H_2 + \cdots + m_rH_r$ if G has an edge decomposition into m_1 subgraphs H_1, m_2 subgraphs $H_2, \ldots, m_r$ subgraphs H_r. Our first theorem resolves the case when all cycles are long.

Theorem 1.1. *Let* $S = \{n-2, n-1, n\}$. *If* n *is odd and* $a(n-2) + b(n-1) + cn = n(n-1)/2$, *then* $K_n = aC_{n-2} + bC_{n-1} + cC_n$. *If* n *is even and* $a(n-2) + b(n-1) + cn = n(n-2)/2$, *then* $K_n - F = aC_{n-2} + bC_{n-1} + cC_n$.

Proof. Let n be odd. It is not difficult to verify that the only solutions to $a(n-2) + b(n-1) + cn = n(n-1)/2$ are $a = b = 0$, $c = (n-1)/2$, and $a = (n-1)/2$, $b = 1$, $c = 0$. Since K_n has a hamilton cycle decomposition we know that $K_n = ((n-1)/2)C_n$. Using the cycles in Fig. 1 we can see that $K_{13} = 6C_{11} + C_{12}$. The cycles of length 11 are A_1 and A_{i+1}, $1 \leq i \leq 5$, where if $(x, y) \in E(A_1)$, $(x+i, y+i) \in E(A_1 + i)$ with addition modulo 12 and $\infty + i = \infty$, and B is the cycle of length 12. This construction is easily generalized to obtain $K_n = ((n-1)/2)C_{n-2} + C_{n-1}$.

For even n the only solutions to $a(n-2) + b(n-1) + cn = n(n-2)/2$ are $a = b = 0$, $c = (n-2)/2$, and $a = n/2$, $b = c = 0$. B. Alspach has provided us with simple decompositions in these two cases. Let D_1 be the cycle shown in Fig. 2 and D_{i+1}, $1 \leq i \leq 5$ be cycles of length 12 defined by $(x+i, y+i) \in E(D_{i+1})$ if

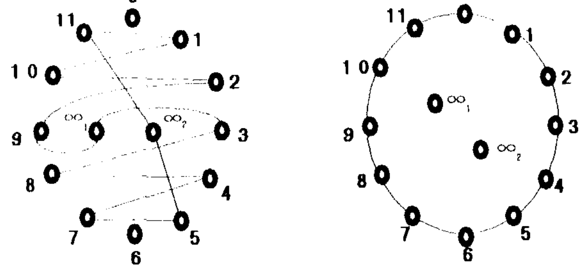


Fig. 3

$(x, y) \in E(D_1)$ where addition is modulo 12 and $\infty_1 + i = \infty_2 + i = i$. These cycles yield $K_{14} - F = 6C_{14}$. Clearly this generalizes to produce $K_n - F = ((n-2)/2)C_n$.

To obtain $K_n - F = (n/2)C_{n-2}$ we again generalize the situation for $n = 14$. Here six cycles of length 12 are obtained from E_1 as shown in Fig. 3. These are E_{i+1}, $1 \leq i \leq 5$, defined as were D_{i+1}. The seventh cycle is the cycle F of Fig. 3. □

2. Small cycle lengths

In this section we will show that if all cycles are of length 3, 4 or 6, and if n is odd and $3a + 4b + 6c = n(n-1)/2$, or if n is even and $3a + 4b + 6c = n(n-2)/2$, then $G = aC_3 + bC_4 + cC_6$ where $G = K_n$ if n is odd and $G = K_n - F$ if n is even.

To begin we need some decompositions for small graphs. Let H_1 and H_2 be as shown in Fig. 4.

Lemma 2.1. *If G is $K_{4,4}$, $K_{4,6}$, $K_{6,6}$ or H_1, and $4b + 6c = |E(G)|$, then $G = bC_4 + cC_6$.*

Proof. (a) $G = K_{4,4}$. We have $4b + 6c = 16$ so we need to show that $K_{4,4} = 4C_4 = C_4 + 2C_6$. Since $K_{2,2} = C_4$ the first of these is immediate and the second is given by the cycles $(x_1, y_1, x_3, y_3, x_2, y_2)$, $(x_1, y_3, x_4, y_2, x_3, y_4)$ and (x_2, y_1, x_4, y_4), where $V(K_{4,4}) = \{x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4\}$.

(b) $G = K_{4,6}$. Here $4b + 6c = 24$ and we want to show that $K_{4,6} = 6C_4 = 3C_4 + 2C_6 = 4C_6$. Again (as in (a)) the first is easy, and the second follows on adding two vertices and two 4-cycles to $K_{4,4} = C_4 + 2C_6$. For the third let $V(K_{4,6}) = \{x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4, y_5, y_6\}$ and take the 6-cycles $(x_1, y_1, x_2, y_2, x_3, y_3)$, $(x_2, y_4, x_3, y_5, x_4, y_6)$, $(x_1, y_4, x_4, y_1, x_3, y_6)$ and $(x_1, y_5, x_2, y_3, x_4, y_2)$.

(c) $G = K_{6,6}$. Counting edges $4b + 6c = 36$. Except for $K_{6,6} = 6C_6$ all follow by adding two vertices and three 4-cycles to each of the decompositions of $K_{4,6}$. For this remaining case let $V(K_{6,6}) = \{x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3, y_4, y_5, y_6\}$. The 6-cycles are given by $(x_1, y_1, x_2, y_4, x_4, y_2)$, $(x_2, y_2, x_3, y_5, x_5, y_3)$, $(x_3, y_3, x_4, y_6, x_6, y_4)$, $(x_1, y_4, x_5, y_1, x_4, y_5)$, $(x_2, y_5, x_6, y_2, x_5, y_6)$ and $(x_3, y_6, x_1, y_3, x_6, y_1)$.

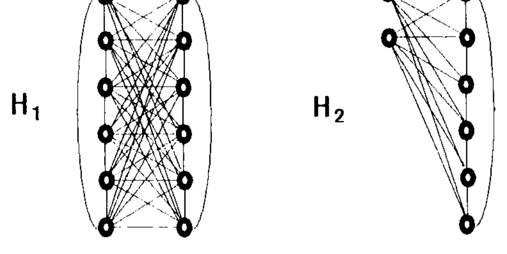


Fig. 4

(d) $G = H_1$. We see that H_1 is $K_{6,6}$ to which two 6-cycles have been added. From the decompositions of $K_{6,6}$ and $4b + 6c = 48$, all cases except $H_1 = 12C_4$ are resolved. With vertices as for $K_{6,6}$ (above) the twelve 4-cycles are (x_1, y_3, x_2, y_4), (x_1, y_5, x_2, y_6), (x_3, y_1, x_4, y_2), (x_3, y_5, x_4, y_6), (x_5, y_1, x_6, y_2), (x_5, y_3, x_6, y_4), (x_1, y_1, y_6, x_6), (x_2, y_2, y_3, x_3), (x_4, y_4, y_5, x_5), (x_1, y_2, y_1, x_2), (x_3, y_4, y_3, x_4) and (x_5, y_6, y_5, x_6). □

Lemma 2.2. *If* $3a + 4b + 6c = 18$, *then* $H_2 = aC_3 + 6C_4 + cC_6$.

Proof. Let $V(H_2) = \{x_1, x_2, y_1, y_2, y_3, y_4, y_5, y_6\}$. For each of the six possible decompositions we will give a set of appropriate cycles.

(a) $H_2 = 6C_3$: (x_1, y_1, y_2), (x_1, y_3, y_4), (x_1, y_5, y_6), (x_2, y_2, y_3), (x_2, y_4, y_5), (x_2, y_6, y_1).

(b) $H_2 = 4C_3 + C_6$: (x_1, y_1, y_6), (x_1, y_4, y_5), (x_2, y_2, y_3), (x_2, y_5, y_6), $(x_1, y_2, y_1, x_2, y_4, y_3)$.

(c) $H_2 = 2C_3 + 2C_6$: (x_1, y_5, y_6), (x_2, y_2, y_3), $(x_1, y_1, y_6, x_2, y_5, y_4)$, $(x_1, y_2, y_1, x_2, y_4, y_3)$.

(d) $H_2 = 3C_6$: $(x_1, y_1, y_2, x_2, y_5, y_4)$, $(x_1, y_2, y_3, x_2, y_6, y_5)$, $(x_1, y_3, y_4, x_2, y_1, y_6)$.

(e) $H_2 = 2C_3 + 3C_4$: (x_1, y_1, y_2), (x_2, y_6, y_1), (x_1, y_4, y_5, y_6), (x_2, y_2, y_3, y_4), (x_1, y_3, x_2, y_5)

(f) $H_2 = 3C_4 + C_6$: (x_1, y_2, x_2, y_3), (x_1, y_4, x_2, y_6), (x_2, y_5, y_6, y_1), $(x_1, y_1, y_2, y_3, y_4, y_5)$. □

We will first show that if n is even and $3a + 4b + 6c = n(n-2)/2$, then $K_n - F = aC_3 + bC_4 + cC_6$. Because of the nature of the proof it is necessary to begin by constructing all such decompositions of $K_n - F$ for small even values of n.

Lemma 2.3. *If* $n \in \{4, 6, 8, 10, 12, 14\}$ *and* $3a + 4b + 6c = n(n-2)/2$, *then* $K_n - F = aC_3 + bC_4 + cC_6$.

Proof. We will, in turn, do each value of n. When $n = 4$, there is the one obvious decomposition $K_4 - F = C_4$. Now let $V(K_n - F) = \{1, 2, \ldots, n\}$.

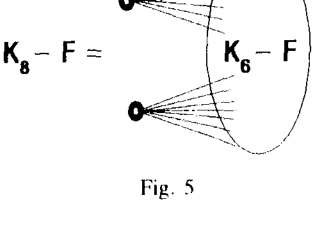


Fig. 5

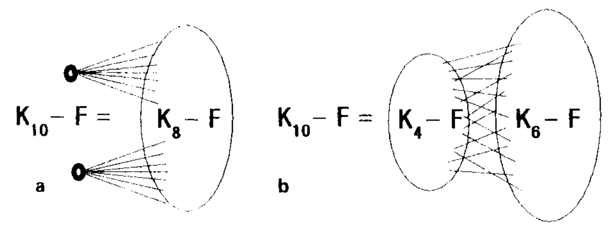


Fig. 6

(a) $n = 6$. We find $3a + 4b + 6c = 12$ and there are four decompositions. We have done $K_6 - F = 2C_6 = 3C_4$ in Theorem 1.1. This leaves $K_6 - F = 4C_3$ for which we take the 3-cycles $(1, 2, 6)$, $(2, 3, 4)$, $(4, 5, 6)$ and $(1, 3, 5)$, and $K_6 - F = 2C_3 + C_6$ for which we use the cycles $(1, 3, 5)$, $(2, 4, 6)$ and $(1, 2, 3, 4, 5, 6)$.

(b) $n = 8$. We view $K_8 - F$ as shown in Fig. 5. Since $K_6 - F = 2C_3 + C_6 = 3C_4 = 2C_6$, $H_2 = 6C_3 = 4C_3 + C_6 = 2C_3 + 2C_6 = 3C_6 = 2C_3 + 3C_4 = 3C_4 + C_6$ (Lemma 2.1) and $K_{2,6} = 3C_4$, we easily obtain all the decompositions.

(c) $n = 10$. Viewing $K_{10} - F$ as in Fig. 6(a), knowing the decompositions for $K_8 - F$ and the fact that $K_{2,8} = 4C_4$, it is not difficult to see that if $3a + 4b + 6c = 40$ and $b \geqslant 4$, then all such decompositions can be constructed. (To do this note that $3a + 4(b - 4) + 6c = 24$.) From $3a + 4b + 6c = 40$ it follows that $b \equiv 1 \pmod 3$ so only the cases with $b = 1$ remain; that is $3a + 4 + 6c = 40$.

Using $K_6 - F = 2C_6$, and $K_4 - F = C_4$, we can think of $K_{10} - F$ as the union of two copies of H_2 and one 4-cycle (as in Fig. 6(b)). Now using the decompositions of H_2 (with $b = 0$) as given in Lemma 2.2, we obtain all remaining decompositions of $K_{10} - F$.

(d) $n = 12$. Let $3a + 4b + 6c = 60$. We find the decompositions of $K_{12} - F$ in much the same way as we did for $K_{10} - F$. Consider the view of $K_{12} - F$ as given in Figs 7(a) and 7(b).

Using Fig. 7(a), $K_{2,10} = 5C_4$, the decompositions of $K_{10} - F$ and the fact that $3a + 4(b - 5) + 6c = 40$ we obtain all decompositions of $K_{12} - F$ with $b \geqslant 5$. Since $b \equiv 0 \pmod 3$, this leaves the cases $b = 3$ and $b = 0$. The view of $K_{12} - F$ shown in Fig. 7(b) allows us to think of $K_{12} - F$ as one copy of $K_6 - F$, two copies

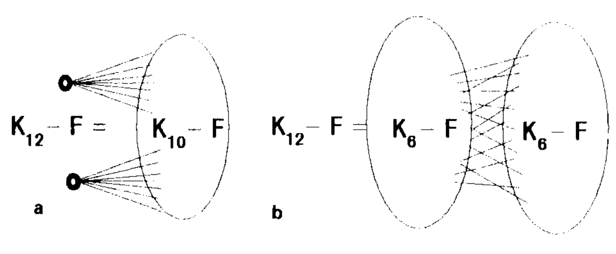


Fig. 7

of H_2 and three 4-cycles. Thus we get all decompositions with $b=3$. For $b=0$ the constructions are a little more complicated. Let $V(K_{12}-F)=\{x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4, z_1, z_2, z_3, z_4\}$ and let the one-factor deleted from K_{12} be $F=\{(x_1, x_3), (x_2, x_4), (y_1, y_3), (y_2, y_4), (z_1, z_3), (z_2, z_4)\}$. Now $K_{12}-F$ consists of three copies of K_6-F, on vertex sets $\{x_1, x_2, x_3, x_4, y_1, y_3\}$, $\{y_1, y_2, y_3, y_4, z_1, z_3\}$, $\{z_1, z_2, z_3, z_4, x_1, x_3\}$, and the four 6-cycles $(y_1, z_4, y_4, z_1, y_2, z_2)$, $(x_3, y_4, x_4, z_3, x_2, y_2)$, $(z_1, x_2, z_2, y_3, z_4, x_4)$ and $(x_2, z_4, y_2, x_4, z_2, y_4)$. Using our decompositions of K_6-F we obtain all decompositions of $K_{12}-F$ with $b=0$ and $c \geqslant 4$. This leaves $K_{12}-F=20C_3=18C_3+C_6=16C_3+2C_6=14C_3+3C_6$ to be constructed. For the first of these, see e.g. [6] and the rest are as follows.

Let $V(K_{12}-F)=\{x_1, x_2, x_3, x_4, x_5, x_6, y_1, y_2, y_3, y_4, y_5, y_6\}$ and we view $K_{12}-F$ as in Fig. 7(b). In $K_{12}-F$ we have the 3-cycles (x_1, x_2, y_4), (x_2, x_3, y_5), (x_3, x_4, y_6), (x_4, x_5, y_1), (x_5, x_6, y_2), (x_6, x_1, y_3), (x_3, x_5, y_3), (x_4, x_6, y_4), (x_5, x_1, y_5), (x_6, x_2, y_6), (x_1, x_3, y_1) and (x_2, x_4, y_2), the 6-cycles $(x_1, y_2, x_3, y_4, x_5, y_6)$ and $(x_2, y_3, x_4, y_5, x_6, y_1)$ and a K_6-F on the vertex-set $\{y_1, y_2, y_3, y_4, y_5, y_6\}$. Thus we have $K_{12}-F=16C_3+2C_6=14C_3+3C_6$. From the $16C_3+2C_6$, delete the 6-cycles and two of the C_3 in $K_6-F=4C_3$ and replace them by the 3-cycles (y_2, x_1, y_6), (y_2, x_3, y_4), (y_4, x_5, y_6), (y_1, x_2, y_3), (y_3, x_4, y_5) and (y_5, x_6, y_1). This yields $K_{12}-F=18C_3+C_6$.

(e) $n=14$. As in the other cases, first view $K_{14}-F$ as in Fig. 8(a).

We immediately have all decompositions in which $b \geqslant 6$. Since $3a+4b+6c=84$, $b \equiv 0 \pmod 3$ and again the decompositions with $b=3$ and $b=0$ remain to be constructed. For $b=3$, take any decomposition of $K_{12}-F$ which has no 4-cycle and at least one 6-cycle. Then $K_{14}-F$ as in Fig. 8(a) can be viewed as the cycles

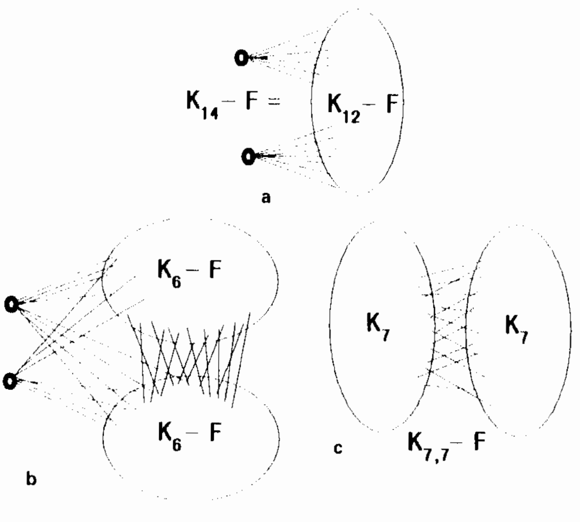


Fig. 8

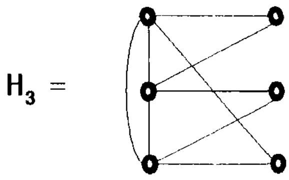


Fig. 9

of $(K_{12} - F) - C_6$, one copy of H_2 and three 4-cycles (from the remaining $K_{2,6}$). We now easily construct all decompositions with $b = 3$. This leaves the decompositions with $b = 0$ and, as in the case of $K_{12} - F$, these take some work to construct. Viewing $K_{14} - F$ as in Fig. 8(b) and using the decompositions of $K_8 - F$ and $K_{6,6}$ we obtain all the desired decompositions with $c \geq 6$. This leaves six cases: $K_{14} - F = 18C_3 + 5C_6 = 20C_3 + 4C_6 = 22C_3 + 3C_6 = 24C_3 + 2C_6 = 26C_3 + C_6 = 28C_3$. The last four of these can be constructed by viewing $K_{14} - F$ as in Fig. 8(c). Take a near 1-factorization of the K_7 with vertex set $\{x_1, x_2, \ldots, x_7\}$. Let the vertices of the other K_7 be $\{y_1, y_2, \ldots, y_7\}$. Pairing the near 1-factors and the vertices $\{y_1, y_2, \ldots, y_7\}$ yields 21 3-cycles. What remains is a copy of K_7. Adding a vertex and the edges of F to $K_6 - F$ yields all decompositions of K_7 with $a \geq 3$. Hence we have constructions showing $K_{14} - F = 28C_3 = 26C_3 + C_6 = 24C_3 + 2C_6$. Since $K_7 = C_3 + 3C_6$ (the cycles are (x_1, x_2, x_3), $(x_1, x_4, x_6, x_7, x_3, x_5)$, $(x_1, x_6, x_2, x_5, x_4, x_7)$ and $(x_2, x_4, x_3, x_6, x_5, x_7)$) we also obtain $K_{14} - F = 22C_3 + 3C_6$. Two cases remain. Return now to Fig. 8(b). On each $K_8 - F$ use $K_8 - F = 8C_3$, and on the $K_{6,6}$ use $K_{6,6} = 6C_6$. Choose two of the 6-cycles in $K_{6,6}$ and in positioning the $K_8 - F = 8C_3$ place them so that in each a triangle can be placed with one of the chosen 6-cycles so that we obtain two copies of the graph H_3 in Fig. 9. Since $H_3 = C_3 + C_6 = 3C_3$ we can, in turn, eliminate the two 6-cycles and obtain the last two decompositions. □

We are now ready to give all decompositions for even n.

Theorem 2.4. *When n is even and $3a + 4b + 6c = n(n-2)/2$, then $K_n - F = aC_3 + bC_4 + cC_6$.*

Proof. Let $n = 2t$ and consider the residue classes of n modulo 12.

(a) $n \equiv 2$ or $6 \pmod{12}$. In this case $t \equiv 1$ or $3 \pmod 6$ and there is an STS(t) [3]. Let $V(K_{2t} - F) = \{a_1, a_2, \ldots, a_t, b_1, b_2, \ldots, b_t\}$ where $F = \{(a_i, b_i) : 1 \leq i \leq t\}$. Take an STS($t$) on the point-set $\{a_1, a_2, \ldots, a_t\}$. Then each 3-cycle (a_i, a_j, a_k) in the STS(t) corresponds to a copy of $K_6 - F$ on the vertex set $\{a_i, a_j, a_k, b_i, b_j, b_k\}$. (The copies of $K_6 - F$ are all edge-disjoint and partition the edges of $K_n - F$.)

If $n = 12m + 2$, $m \geq 1$, then $3a + 4b + 6c = 12m(6m+1)$ and so $a \equiv 0 \pmod 2$ and $b \equiv 0 \pmod 3$. There are two cases: (i) $a = 4a'$, $b = 3b'$, $c = 2c'$, and (ii)

$a = 4a' + 2$, $b = 3b'$, $c = 2c' + 1$. In the first $a' + b' + c' = m(6m + 1)$, the number of 3-cycles in the STS(t). To see that $K_n - F = aC_3 + bC_4 + cC_6$, in a' of the $K_6 - F$ use the decomposition $K_6 - F = 4C_3$, in b' of them use $K_6 - F = 3C_4$ and in the remaining c' use $K_6 - F = 2C_6$. In the second case we find that $a' + b' + c' + 1 = m(6m + 1)$ so here in a' of the $K_6 - F$ use $K_6 - F = 4C_3$, in b' of them use $K_6 - F = 3C_4$, in c' use $K_6 - F = 2C_6$ and in the one remaining put $K_6 - F = 2C_3 + C_6$ to yield $K_n - F = aC_3 + bC_4 + cC_6$.

If $n = 12m + 6$, $m \geq 1$, then $3a + 4b + 6c = 12(3m + 1)(2m + 1)$ and again $a \equiv 0 \pmod 2$ and $b \equiv 0 \pmod 3$. We now repeat the argument given in the case $n = 12m + 2$. Finally, when $n = 6$ the result follows from Lemma 2.3.

(b) $n \equiv 10 \pmod{12}$. Then $t \equiv 5 \pmod 6$ and there is ([6]) a near-STS(t) in which one block has size five and all other size 3. Let $V(K_{2t} - F) = \{a_1, a_2, \ldots, a_t, b_1, b_2, \ldots, b_t\}$ and, as before, to the 3-cycles (blocks of size 3) in the near-STS(t) correspond copies of $K_6 - F$ and to the block of size 5 corresponds a $K_{10} - F$. Letting $n = 12m + 10$, $m \geq 1$, we get $3a + 4b + 6c = 36(2m + 1)(m + 1) + 4$ and hence $b \equiv 1 \pmod 3$ and $a \equiv 0 \pmod 2$. Two cases need be considered: (i) $a = 4a'$, $b = 3b' + 1$, $c = 2c'$ and (ii) $a = 4a' + 2$, $b = 3b' + 1$, $c = 2c' + 1$. In case (i) $a' + b' + c' = 3(2m + 1)(m + 1)$. Now as $m \geq 1$, one of a', b', and c' is at least three. Depending on which write either $(a' - 3) + b' + c' = 3m(2m + 3)$, $a' + (b' - 3) + c' = 3m(2m + 3)$ or $a' + b' + (c' - 3) = 3m(2m + 3)$. Note that $3m(2m + 3)$ is the number of edge-disjoint $K_6 - F$ we have in $K_n - F$. We are now ready to describe the decomposition. Given $a^* + b^* + c^* = 3m(2m + 3)$, in a^* of the $K_6 - F$ use $K_6 - F = 4C_3$, in b^* use $K_6 - F = 3C_4$ and in c^* of them use $K_6 - F = 2C_6$. All that remains is to choose the appropriate decomposition of $K_{10} - F$. Choose respectively, $K_{10} - F = 12C_3 + C_4$, $K_{10} - F = 10C_4$ or $K_{10} - F = C_4 + 6C_6$.

Case (ii) follows in a similar fashion and the case $n = 10$ was resolved in Lemma 2.3.

(c) $n \equiv 0, 8 \pmod{12}$. Unfortunately we must work modulo 24, and consider the two cases: (c') $n \equiv 0, 8 \pmod{24}$, and (c'') $n \equiv 12, 20 \pmod{24}$.

(c') $n \equiv 0, 8 \pmod{24}$.

Thus $t \equiv 0, 4 \pmod{12}$ and it is known ([5]) that there is a group divisible design on t symbols in which the groups have size 4 and the blocks size 3. As in (a) this yields a partition of the edges of $K_n - F$ into copies of $K_6 - F$ and $K_8 - F$.

If $n = 24m$, $m \geq 1$, $3a + 4b + 6c = 24m(12m - 1)$ and so $b \equiv 0 \pmod 3$ and $a \equiv 0 \pmod 2$. Thus $b = 3b'$ and either (i) $a = 4a'$, $c = 2c'$ or (ii) $a = 4a' + 2$, $c = 2c' + 1$. We will discuss (i) as (ii) is done similarly. First list all $K_6 - F$ and then all $K_8 - F$ in $K_n - F$ and from them choose a copies of C_3 as follows. In the first $K_6 - F$ put $K_6 - F = 4C_3$. Continuing until we have a 3-cycles our last decomposition will be either $K_6 - F = 4C_3$, $K_8 - F = 4C_3 + xC_4 + yC_6$ or $K_8 - F = 8C_3$. Now we find the c 6-cycles. The first decomposition containing C_6 will be either $K_6 - F = 2C_6$, $K_8 - F = 4C_3 + 2C_6$, $K_8 - F = 4C_6$ or $K_8 - F = 3C_4 + 2C_6$. When we have reached cC_6, the remainder of the $K_6 - F$ and $K_8 - F$ are to be decomposed into C_4.

An almost identical construction works when $n = 24m + 8$.

(c″) $n \equiv 12, 20 \pmod{24}$. In this case $t \equiv 6,\ 10 \pmod{12}$ and it is known ([9]) that if $t - 2 \equiv 4,\ 8 \pmod{12}$, there is a group divisible design on t points with one group of size 6, the rest of size 4 and all blocks of size 3. As in (c′) this gives us a partition of the edges of $K_n - F$ into copies of $K_6 - F$, $K_8 - F$ and one $K_{12} - F$. To construct the required decomposition of $K_n - F$ we list the $K_6 - F$, then the $K_8 - F$ and last the one $K_{12} - F$ and decompose them in turn (using Lemma 2.3) as was done in (c′).

(d) $n \equiv 4 \pmod{12}$. Let $n = 12m + 4$ so $t = 6m + 2$. We know ([7]) that $K_{6m} - F$, $m \geqslant 3$, has a resolvable decomposition into cycles of length 3.

Adding to $K_{6m} - F$ one new vertex and the edges of F yields a decomposition of K_{6m+1} into 3-cycles (an STS$(6m + 1)$) which has a set of $2m$ vertex-disjoint 3-cycles (from one of the resolutions). Now, duplicate as in (a) to get a partition of the edges of $K_{12m+2} - F$ into copies of $K_6 - F$. In particular this partition has $2m$ vertex-disjoint copies of $K_6 - F$ and a copy of $K_2 - F$ (as shown in Fig. 10). Now add two more vertices (non-adjacent) to get $K_{12m+4} - F$ which is edge-partitioned into $2m$ copies of $K_8 - F$, one C_4 and $m(6m - 1)$ copies of $K_6 - F$.

Since $3a + 4b + 6c = 12m(6m + 3) + 4$, $b \equiv 1 \pmod 3$. Thus $b \geqslant 1$ and we have an obvious C_4 as shown in Fig. 10. The remainder of $K_{12m+4} - F$ is decomposed into $K_6 - F$ and $K_8 - F$. We now fill these as we did in (c).

Two cases remain: $K_{16} - F$ and $K_{28} - F$. First we do $K_{16} - F$ viewing the graph in the four different ways as shown in Fig. 11.

Here $3a + 4b + 6c = 112$. From Fig. 11(a) we can construct all decompositions $K_{16} - F = aC_3 + bC_4 + cC_6$ with $b \geqslant 7$. This leaves $b = 1$ and $b = 4$. From Fig. 11(b) we get all decompositions with $c \geqslant 6$. From Fig. 11(c) we get all

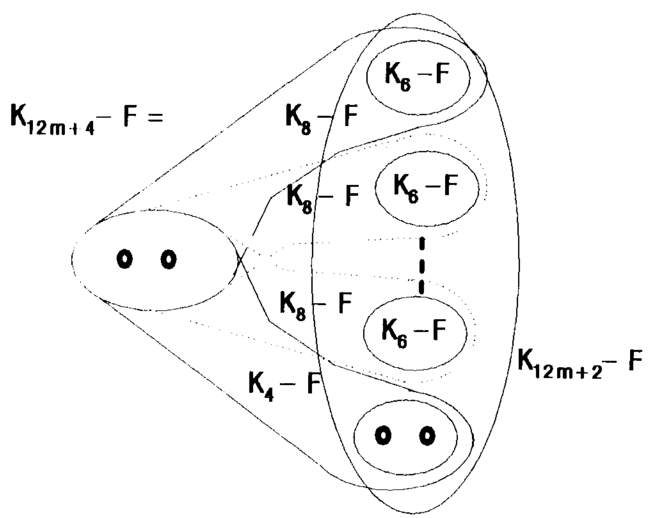


Fig. 10

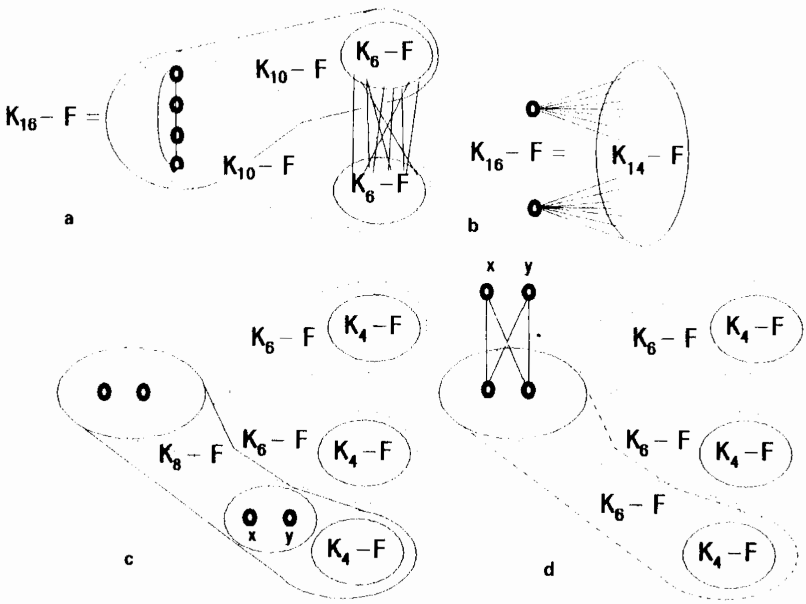


Fig. 11

decompositions with $b=4$ and $a \geqslant 16$ (observe that $K_{2,4,4}-K_{4,4}=K_{2,8}=4C_4$, and recall the well-known fact that $K_{4,4,4}=16C_3$). This leaves the case $b=1$ and $a \geqslant 26$ (as $c \leqslant 5$). Here we use Fig 11(d), noting that the unmarked edges are those of $K_{2,4,4,4}$. All that remains to be shown is that $K_{2,4,4,4}$ can be partitioned into 24 triangles, or, equivalently, that $K_{4,4,4}$, with two suitably chosen 1-factors deleted, can be partitioned into 12 triangles. The latter is an easy exercise.

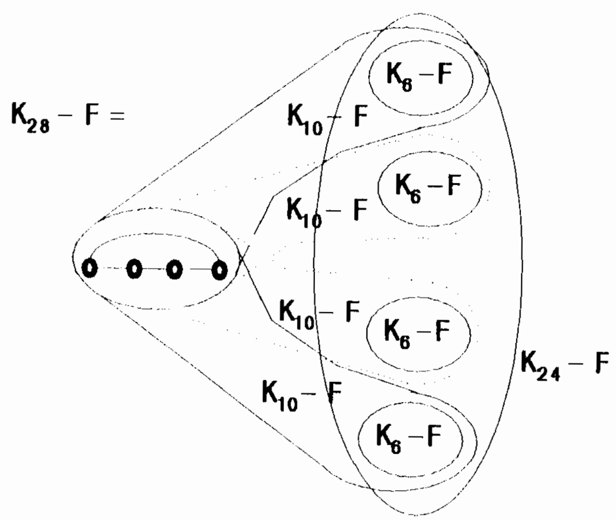


Fig. 12

Note that in Fig. 11(b) we require that in each decomposition of $K_{10} - F$ one of the C_4 (there is always at least one) has on its diagonals two of the edges of F. From Figs 6(a) and 6(b) it is easy to see that this can always be arranged.

The last case is $K_{28} - F$. Since there is a group divisible design on 12 points with groups of size 3 and blocks of size 4, we can view $K_{28} - F$ as in Fig. 12.

Noting the earlier comment regarding $K_{10} - F$ we can now decompose the $K_8 - F$ and $(K_{10} - F) - C_4$ as in (c) to obtain all decompositions. □

The previous theorem immediately gives us many of the decompositions $K_n = aC_3 + bC_4 + cC_6$ when n is odd.

Corollary 2.5. *When n is odd, $a \geq (n-1)/2$, and $3a + 4b + 6c = n(n-1)/2$, then $K_n = aC_3 + bC_4 + cC_6$.*

Proof. From $3a + 4b + 6c = n(n-1)/2$ we obtain $3a' + 4b + 6c = (n-1)(n-3)/2$ where $a' = a - (n-1)/2$ and by Theorem 2.5 $K_{n-1} - F = a'C_3 + bC_4 + cC_6$. Now, adding a new vertex and the edges of F to $K_{n-1} - F$, we obtain $K_n = aC_3 + bC_4 + cC_6$. □

Hence, when n is odd we need only consider the cases $a \leq (n-3)/2$. As when n was even we begin with a lemma which takes care of the small odd values of n.

Lemma 2.6. *If $n \in \{3, 5, 7, 9, 11, 13, 17\}$ and $3a + 4b + 6c = n(n-1)/2$, then $K_n = aC_3 + bC_4 + cC_6$.*

Proof. Thanks to Corollary 2.5 we consider only the cases $a \leq (n-3)/2$. When $n = 3$ and $n = 5$ there is only one decomposition and it is easily constructed.

(a) $n = 7$, $a \leq 2$. Since $3a + 4b + 6c = 21$, a is odd and the only decompositions are $K_7 = C_3 + 3C_4 + C_6$ and $K_7 = C_3 + 3C_6$. These are given by the cycles $(1,2,3)$, $(1,6,3,7)$, $(2,4,3,5)$, $(4,6,7,5)$, $(1,4,7,2,6,5)$, and $(1,2,3)$, $(1,4,6,7,3,5)$, $(1,6,2,5,4,7)$ and $(2,4,3,6,5,7)$, respectively, where $V(K_7) = \{1, 2, 3, 4, 5, 6, 7\}$.

(b) $n = 9$, $a \leq 3$. Since $3a + 4b + 6c = 36$, a is even and we must consider $a = 0$ and $a = 2$. To $K_7 = C_3 + 3C_6 = C_3 + 3C_4 + C_6$ add two new vertices, replace the C_3 by a K_5 and add two more C_4. This yields $K_9 = 2C_3 + 3C_4 + 3C_6 = 2C_3 + 6C_4 + C_6$. For $K_9 = 2C_3 + 5C_6$ let $V(K_9) = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ and take the cycles $(1,2,3)$, $(2,6,7)$, $(1,4,2,5,3,6)$, $(4,7,5,8,6,9)$, $(7,1,8,2,9,3)$, $(1,5,4,8,7,9)$ and $(3,4,6,5,9,8)$. We now have the four cases with $a = 0$: $K_9 = 9C_4 = 6C_4 + 2C_6 = 3C_4 + 4C_6 = 6C_6$. These are given respectively by the following sets of cycles: $\{(1,2,9,6)$, $(2,3,1,7)$, $(3,4,2,8)$, $(4,5,3,9)$, $(5,6,4,1)$, $(6,7,5,2)$, $(7,8,6,3)$, $(8,9,7,4)$, $(9,1,8,5)\}$, $\{(1,8,3,9)$, $(2,7,9,5)$, $(4,7,6,8)$, $(1,5,4,2)$, $(2,6,5,3)$, $(1,6,4,3)$, $(1,4,9,8,5,7)$, $(2,8,7,3,6,9)\}$, $\{(1,8,3,9)$, $(2,7,9,5)$, $(4,7,6,8)$, $(1,4,9,8,5,7)$, $(2,8,7,3,6,9)$, $(1,5,4,6,2,3)$,

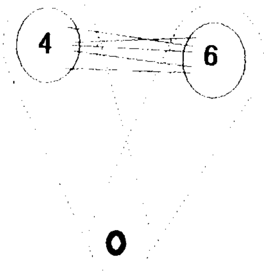


Fig. 13

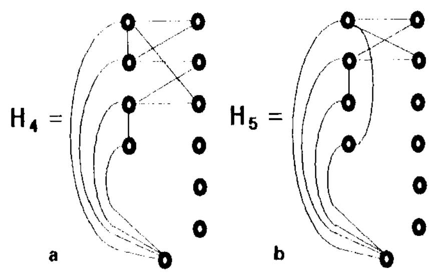


Fig. 14

$(1,6,5,3,4,2)\}$ and $\{(1,5,4,6,2,3),(1,6,5,3,4,2),(1,4,9,8,2,7),(3,7,4,8,6,9),$ $(1,8,7,5,2,9),\ (3,8,5,9,7,6)\}$.

(c) $n=11$, $a \leqslant 4$. It is easy to see that a is odd, so $a=1$ or $a=3$, and $b \equiv 1 \pmod 3$.

Using Fig. 13 and known decompositions of $K_{4,6}$, K_5, and K_7 we get all decompositions of K_{11} with $a=3$. Note that using Fig. 13 we must always have two 3-cycles as K_5 does. However, since $H_4 = 2C_6$ (H_4 is shown in Fig. 14(a)), $K_{4,6} = 3C_4 + 2C_6 = 4C_6$ and we have decompositions of K_7, we easily obtain $K_{11} = C_3 + C_4 + 8C_6 = C_3 + 4C_4 + 6C_6 = C_3 + 7C_4 + 4C_6$. Next, H_5 (shown in Fig. 14(b)) easily decomposes as $H_5 = C_4 + C_6$ and since $K_{4,6} = 6C_4$ and $K_7 = C_3 + 3C_4 + C_6$, we obtain $K_{11} = C_3 + 10C_4 + 2C_6$. This leaves $K_{11} = C_3 + 13C_4$ which is given by the cycles $(1,6,9)$, $(6,8,1,10)$, $(9,11,1,7)$, $(11,8,10,7)$, $(2,4,3,5)$, $(2,8,3,11)$, $(4,8,5,11)$, $(1,2,10,3)$, $(2,6,7,3)$, $(2,7,8,9)$, $(1,4,7,5)$, $(3,6,5,9)$, $(4,9,10,5)$ and $(4,6,11,10)$, where $V(K_{11}) = \{1, 2, 3, \ldots, 11\}$.

(d) $n=13$, $a \leqslant 5$. Counting we find that a is even, so we must consider $a=0$, 2 and 4. Consider K_{13} as in Fig. 15. When $a=4$ decompose one K_7 as either $K_7 = C_3 + 3C_4 + C_6$ or $K_7 = C_3 + 3C_6$, and the other as $K_7 = 3C_3 + 2C_6$. Removing a 6-cycle from each of these and attaching them to $K_{6,6}$ yields a copy of H_1. On now decomposing H_1 all possible decompositions of K_{13} with $a=4$ are achieved. When $a=2$ decompose each K_7 as either $K_7 = C_3 + 3C_4 + C_6$ or as

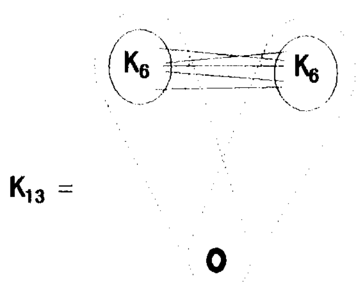


Fig. 15

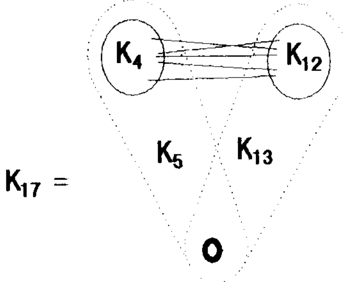


Fig. 16

$K_7 = C_3 + 3C_6$. Using the above argument yields all decompositions of K_{13} with $a = 2$. When $a = 0$ we first construct $K_{13} = 13C_6$. Let $V(K_{13}) = \{0, 1, 2, \ldots, 12\}$ and $G_1 = (1, 4, 10, 2, 3, 5)$. The remaining 6-cycles are $G_{i+1} = G + i$ where $(x + i, y + i) \in E(G_{i+1})$ if $(x, y) \in E(G_1)$, $1 \leq i \leq 12$, and addition is modulo 13. Since $G_i \cup G_{i+1} = 3C_4$, $1 \leq i \leq 12$, all decompositions of K_{13} with $a = 0$ are constructed.

(e) $n = 17$, $a \leq 7$. Clearly a is even so $a \in \{0, 2, 4, 6\}$. View K_{17} as in Fig. 16. We see that the edges of K_{17} can be partitioned into one K_5, one K_{13} and two copies of $K_{4,6}$. By appropriately decomposing each of these we obtain all decompositions of K_{17} with $2 \leq a \leq 6$. This leaves $a = 0$. Again we use Fig. 16. First, in the decomposition of one of the $K_{4,6}$ make sure a 4-cycle (respectively a 6-cycle) from it and the two 3-cycles from $K_5 = 2C_3 + C_4$ are as in $H_5 = C_4 + C_6$ (respectively, $H_4 = 2C_6$). Choosing appropriate decompositions of $K_{4,6}$ and K_{13} yields all decompositions of K_{17} with $a = 0$ except for $K_{17} = 34C_4$. If $V(K_{17}) = \{0, 1, 2, \ldots, 16\}$ the 4-cycles for this decomposition are $J_1 = (1, 3, 2, 9)$, $K_1 = (4, 10, 13, 9)$ and $J_{i+1} = J_1 + i$, $K_{i+1} = K_1 + i$, $1 \leq i \leq 16$, where all addition is modulo 17. □

We are now ready to prove the main result for odd n.

Theorem 2.7. *If n is odd and $3a + 4b + 6c = n(n-1)/2$, then $K_n = aC_3 + bC_4 + cC_6$.*

Proof. We know by Corollary 2.5 that we may assume $a \leq (n-3)/2$. The proof will look at the residue classes of n modulo 12 and all cases will be based on Fig. 17 where $s + t + 1 = n$.

(a) $n = 12m + 1$, $m \geq 2$. Since $3a + 4b + 6c = 6m(12m + 1)$, then a is even and $a \leq 6m - 2$. The construction of the decompositions is by induction on m; all decompositions of K_{13} (the case $m = 1$) are given in Lemma 2.6. In Fig. 17 let $s = 12$ and $t = 12(m-1)$. We assume that all decompositions of $K_{12(m-1)+1}$ are possible. Since $3(6m-2) \leq 6(m-1)(12(m-1)+1)$ for $m \geq 2$, we know that for $a \leq 6m - 2$, and b' and c' satisfying $3a + 4b' + 6c' = 6(m-1)(12(m-1)+1)$,

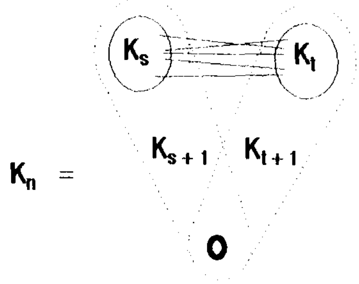


Fig. 17

then $K_{12(m-1)+1} = aC_3 + b'C_4 + c'C_6$. As well as the K_{13} and $K_{12(m-1)+1}$, K_{12m+1} also contains $4(m-1)$ disjoint copies of $K_{6,6}$. Since $K_{6,6} = 9C_4 = 6C_4 + 2C_6 = 3C_4 + 4C_6 = 6C_6$ (by Lemma 2.1) and $K_{13} = 18C_4 + C_6 = \cdots = 13C_6$, it appears that we can, by appropriate choice of the decompositions of "the pieces", obtain the required decompositions of K_{12m+1}. However, this is not quite correct as if $a \equiv 0 \pmod 4$ and m is even, or if $a \equiv 2 \pmod 4$ and m is odd, then we require decompositions of the form $K_{12m+1} = aC_3 + bC_4$. But decompositions of K_{13} always contain a 6-cycle. Fortunately in these cases the decompositions of $K_{12(m-1)+1}$ also all contain a 6-cycle and we simply locate these 6-cycles so that one of the $K_{6,6}$ becomes the graph H_1, and $H_1 = 12C_4$.

(b) $n = 12m + 7$, $m \geq 1$. In this case $3a + 4b + 6c = 6((12m+1)(m+1)+2) + 3$ so a is odd and $a \leq 6m + 1$. Choose $s = 6$ and $t = 12m$ in Fig. 17. From (a) we have all decompositions of K_{12m+1} and from Lemma 2.6 all decompositions of $K_7 = C_3 + b'C_4 + c'C_6$. Note that each decomposition of K_7 has both a 3-cycle and a 6-cycle. Our decompositions of K_{12m+7} must have an odd number of 3-cycles. Since $18m \leq 6m(12m+1)$ when $m \geq 1$, we can choose decompositions of K_{12m+1} with $(a-1)$ 3-cycles which, with the one in K_7, gives us a 3-cycles. We now proceed as in (a) and again must pay particular attention to the case $c = 0$. In this case the difficulties occur when $a \equiv 1 \pmod 4$ and m is odd, or when $a \equiv 3 \pmod 4$ and m is even, but we use the same technique as before to obtain the decompositions.

(c) $n = 12m + 5$, $m \geq 2$. Counting edges we have $3a + 4b + 6c = 6(12m^2 + 9m + 1) + 4$ so a is even and $a \leq 6m$. In this case we put $s = 16$ and $t = 12(m-1)$, and note that K_{17} has a 4-cycle in each decomposition, all decompositions of $K_{12(m-1)+1}$ have an even number of 3-cycles and as $3a \leq 18m \leq 6(m-1)(12(m-1)+1)$ for $m \geq 2$, there are decompositions with exactly a 3-cycles. When viewed as in Fig. 17, K_{12m+5} has also $8(m-1)$ disjoint copies of $K_{4,6}$ and by Lemma 2.1 $K_{4,6} = 6C_4 = 3C_4 + 2C_6 = 4C_6$. By suitably choosing decompositions of the K_{17}, $K_{4,6}$ and $K_{12(m-1)+1}$ all required decompositions of K_{12m+5} can be constructed.

(d) $n = 12m + 9$, $m \geq 1$. This case is also easily dealt with. In Fig. 17 choose $s = 8$ and $t = 12n$. From $3a + 4b + 6c = 6(4m+3)(3m+2)$ a is even and $a \leq$

6m + 2. Since $3(6m+2) \leqslant 6m(12m+1)$, for $m \geqslant 1$, all 3-cycles will be found in the decomposition of K_{12m+1}. Now we just choose appropriate decompositions of K_9, K_{12m+1} and the $4m$ disjoint copies of $K_{4,6}$.

(e) $n = 12m + 3$, $m \geqslant 1$. In Fig. 17 choose $s = 6$ and $t = 12(m-1)+8$. Counting edges $3a + 4b + 6c = 6m(12m+5)+3$, and so a is odd and $a \leqslant 6m - 1$, Now $3(a-1) \leqslant 3(6m-2) \leqslant 6(4m-1)(3m-1)$, for $m \geqslant 1$, and so we take a decomposition of K_7 with exactly one 3-cycle, and of $K_{12(m-1)+9}$ with $(a-1)$ 3-cycles. The rest of K_{12m+3} consists of two copies of $K_{4,6}$ and $2(m-1)$ copies of $K_{6,6}$. As in (a) we have to pay special attention to the case $c = 0$ as each decomposition of K_7 has a 6-cycle. When $a \equiv 1 \pmod 4$ and m is even, or $a \equiv 3 \pmod 4$ and m odd both K_7 and $K_{12(m-1)+9}$ have a 6-cycle. These can be chosen so that one of the $K_{6,6}$ becomes a copy of H_1 and now we proceed as before.

(f) $n = 12m + 11$, $m \geqslant 1$. This last case follows as the others. In Fig. 17 choose $s = 10$ and $t = 12m$. From $3a + 4b + 6c = 6(12m^2 + 21m + 8) + 4 + 3$ we know that a is odd and so $a \leqslant 6m + 3$. Each decomposition of K_{11} has a 3-cycle and a 4-cycle. Since $3(6m+2) \leqslant 6m(12m+1)$, $m \geqslant 1$, we choose decompositions of K_{12m+1} with $(a-1)$ 3-cycles. The remainder of K_{12m+11} consists of $2m$ disjoint $K_{4,6}$ and $2m$ disjoint $K_{6,6}$. Decomposing all these graphs appropriately yields the desired decompositions of K_{12m+11}. □

3. Cycles of length 2^k and 2^{k+1}

We need to introduce the notion of switching on cycles. Suppose G contains the three edge disjoint cycles of lengths s, t and r as shown in Fig. 18(a). We can, by *switching on the cycle* (v_0, v_1, v_2, v_3), obtain the two cycles of lengths $s + t$ and r as shown in Fig. 18(b).

This switching procedure can be applied many times as illustrated in Fig. 19.

The next result, due to D. Sotteau [10], will be used often in the proofs.

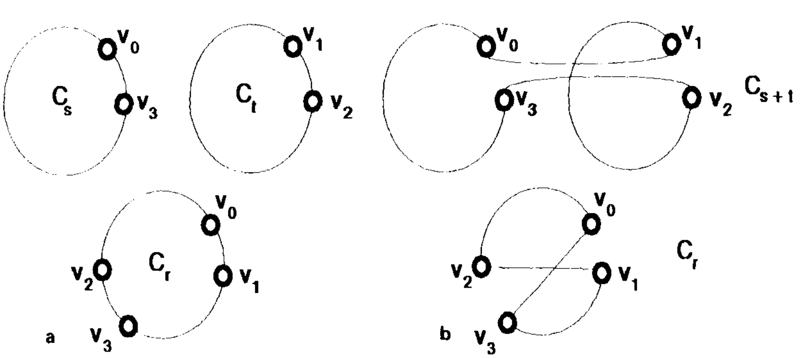


Fig. 18

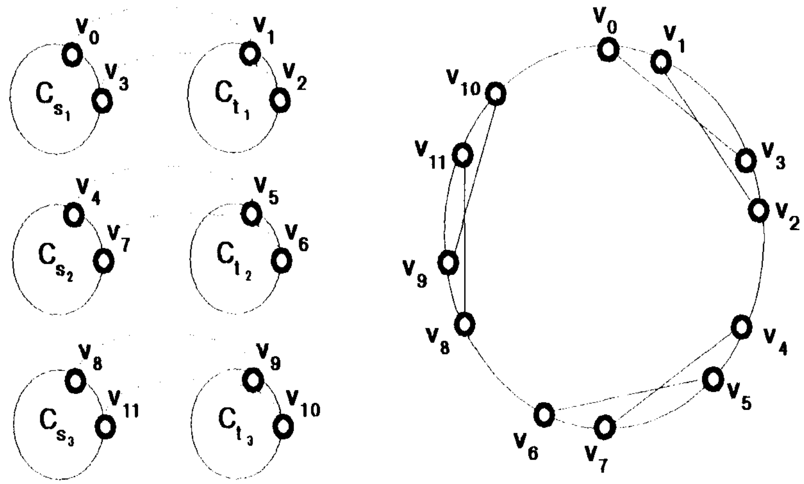


Fig. 19

Theorem 3.1. *Suppose $k \leq n$, $k \leq m$, m and n are even and $mn = 2kt$. Then $K_{m,n} = tC_{2k}$.*

We now state and prove several lemmas.

Lemma 3.2. *Let $K_{p,q} = C_{i_1} + C_{i_2} + \cdots + C_{i_t}$ where p and q are even. Then $K_{2p,2q} = D_{i_1} + D_{i_2} + \cdots + D_{i_t}$ where either $D_{i_k} = 4C_{i_k}$ or $D_{i_k} = 2C_{2i_k}$.*

Proof. Let $K_{p,q} = C_{i_1} + C_{i_2} + \cdots + C_{i_t}$ and let $V(K_{p,q}) = \{x_1, x_2, \ldots, x_p, y_1, y_2, \ldots, y_q\}$. Let $V(K_{2p,2q}) = \{a_1, a_2, \ldots, a_{2p}, b_1, b_2, \ldots, b_{2q}\}$. If C is a cycle of $K_{p,q}$, then C is necessarily even and we will assume (without loss of generality) that $C = (x_1, y_1, x_2, y_2, \ldots, x_r, y_r)$. In $K_{2p,2q}$ this describes either the four $2r$-cycles $(a_1, b_1, a_2, b_2, \ldots, a_r, b_r)$, $(a_{p+1}, b_{q+1}, a_{p+2}, b_{q+2}, \ldots, a_{p+r}, b_{q+r})$, $(a_1, b_{q+1}, a_2, b_{q+2}, \ldots, a_r, b_{q+r})$ and $(a_{p+1}, b_1, a_{p+2}, b_2, \ldots, a_{p+r}, b_r)$, or the two $4r$-cycles $(a_1, b_{q+1}, a_2, b_{q+2}, \ldots, a_r, b_r, a_{p+r}, b_{r-1}, a_{p+r-1}, \ldots, b_1, a_{p+1}, b_{q+r})$ and $(a_1, b_1, a_2, b_2, \ldots, a_r, b_{q+r}, a_{p+r}, b_{q+r-1}, a_{p+r-1}, \ldots, b_{q+1}, a_{p+1}, b_r)$. □

Lemma 3.3. *If y and n are even and $0 \leq y \leq n$, then $K_{2n,2n} = (2n - 2y)C_{2n} + yC_{4n}$.*

Proof. From Theorem 3.1 we know that $K_{n,n} = (n/2)C_{2n}$. Applying Lemma 3.2 to this decomposition yields the result. □

Although Theorem 3.1 yields $K_{2n,2n} = nC_{4n}$ we need a very particular decomposition in order to prove the main result. This decomposition is given in Lemma 3.4.

Lemma 3.4. *Let $A = (a_{ij})$ be a latin square of order n based on the set $\{1, 2, \ldots, n\}$. Let $X = \{x_1, x_2, \ldots, x_{2n}\}$ and $Y = \{y_1, y_2, \ldots, y_{2n}\}$. Then the n cycles of length $4n$ given by $D_i = (x_1, y_{2a_{i1}-1}, x_2, y_{2a_{i1}}, \ldots, x_{2j-1}, y_{2a_{ij}-1}, x_{2j}, y_{2a_{ij}}, \ldots, x_{2n-1}, y_{2a_{i,n}-1}, x_{2n}, y_{2a_{i,n}})$ where subscript calculations are modulo $2n$ on the residues $1, 2, \ldots, 2n$, constitute a decomposition $K_{2n,2n} = nC_{4n}$ with $V(K_{2n,2n}) = X \cup Y$.*

Proof. Since the ith row of A contains each of the entries $1, 2, \ldots, n$, D_i is a $4n$-cycle. Since the jth column of A contains each of the entries $1, 2, \ldots, n$, then $K_{2n,2n} = D_1 + D_2 + \cdots + D_n = nC_{4n}$. □

Let G be either $K_{2^m,2^m}$ or $K_{2^m+2,2^m}$, $m \geqslant 2$. Let $V(G) = X \cup Y$ where $X = \{x_1, \ldots, x_t\}$, $t = 2^m$ or $t = 2^m + 2$, and $Y = \{y_1, y_2, \ldots, y_{2^m}\}$. The decomposition $G = aC_{2^m} + bC_{2^{m+1}}$ is *basic* if $a = 0$ and it contains the cycle $(x_1, y_1, x_2, y_2, \ldots, x_{2^m}y_{2^m})$, or if $b = 0$ and it contains both the cycle $(x_1, y_1, x_2, y_2, \ldots, x_{2^{m-1}}, y_{2^{m-1}})$ and the cycle $(x_{2^{m-1}+1}, y_{2^{m-1}+1}, \ldots, x_{2^m}, y_{2^m})$. These are the *basic cycles*. Since by Theorem 3.1 $G = bC_{2^{m+1}}$, then after suitably labelling the vertices of G we can always obtain a basic decomposition. For a basic decomposition $G = aC_{2^m}$ we use the fact that both $K_{2^m,2^{m-1}}$ and $K_{2^m+2,2^{m-1}}$ have decompositions into cycles of length 2^m (again use Theorem 3.1).

Lemma 3.5. *There is a decomposition $K_{2n} - F = (n-1)C_{2n}$, $n \geqslant 2$, with the property that there is a set of edges $E = \{e_1, \ldots, e_{n-1}\}$, one from each cycle, so that $F \cup E$ is a path with edges alternating between E and F.*

Proof. We use the decomposition given in Theorem 1.1. Let $E = \{(2i, 2i+1): 0 \leqslant i \leqslant n-3\} \cup \{(2n-4, \infty_1)\}$ when n is even, and let $E = \{(2i, 2i+1): 0 \leqslant i \leqslant (n-3)/2\} \cup \{(2i+1, 2i+2): (n-1)/2 \leqslant i \leqslant n-3\} \cup \{(2n-3, \infty)\}$ when n is odd. Since $F = \{(i, n-1+i): 0 \leqslant i \leqslant n-2\} \cup \{(\infty_1, \infty_2)\}$ it is not difficult to check that $E \cup F$ is as required. □

Note that the edges E form an independent set of edges.

Lemma 3.6. *There is a decomposition $K_{2n-2} - F = (n+1)C_{2n}$, $n \geqslant 2$, with the property that there is a set $E = \{e_1, \ldots, e_n\}$ of independent edges, each from a different cycle.*

Proof. We again use the decomposition given in Theorem 1.1. Let $E = \{((n/2) + i, (3n/2) - 1 + i): 0 \leqslant i \leqslant n-2\} \cup \{((n/2) - 2, (n/2) - 1)\}$ if n is even, and let $E = \{((n+1)/2 + i, (3n-1)/2 + i): 0 \leqslant i \leqslant n-2\} \cup \{((n-3)/2, (n-1)/2)\}$ if n is odd. □

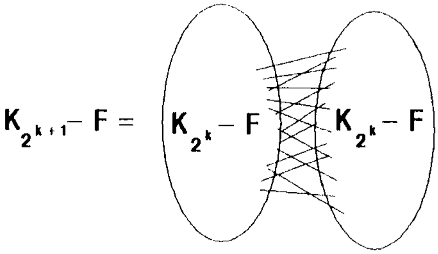


Fig. 20

We now have the tools necessary to prove the main theorem when n is even. First note that in this case if $K_n - F = aC_{2^k} + bC_{2^{k+1}}$, then $n \equiv 0, 2 \pmod{2^k}$ and if $b \neq 0$, $n \geq 2^{k+1}$. We begin with the cases $n = 2^{k+1}$ and $n = 2^{k+1} + 2$ as if $n = 2^k$ or $n = 2^k + 2$, then $b = 0$ and the situation has been dealt with in Theorem 1.1.

Theorem 3.7. *If* $a2^k + b2^{k+1} = 2^{k+1}(2^k - 1)$, *then* $K_{2^{k+1}} - F = aC_{2^k} + bC_{2^{k+1}}$.

Proof. We view $K_{2^{k+1}} - F$ as in Fig. 20.

Let G_1 and G_2 denote the two copies of $K_{2^k} - F$ with $V(G_1) = \{x_1, x_2, \ldots, x_{2^k}\}$ and $V(G_2) = \{y_1, y_2, \ldots, y_{2^k}\}$.

We use the decomposition $G_1 = G_2 = (2^{k-1} - 1)C_{2^k}$ of Lemma 3.5. Permute labels of the vertices in G_1 and G_2 so that the independent edges are given by $E_1 = \{(x_{2i-1}, x_{2i}): 1 \leq i \leq 2^{k-1} - 1\}$ and $E_2 = \{(y_{2i-1}, y_{2i}): 1 \leq i \leq 2^{k-1} - 1\}$.

Suppose $b < 2^{k-1}$. By Theorem 3.1 and the comments following Lemma 3.4 there is a basic decomposition of $K_{2^k,2^k}$ into cycles of length 2^k. Now switching on the cycles $(x_{2i-1}, y_{2i-1}, y_{2i}, x_{2i})$, $1 \leq i \leq b$, we obtain $K_{2^{k+1}} - F = aC_{2^k} + bC_{2^{k+1}}$, $1 \leq b \leq 2^{k-1} - 1$.

Consider the case $b \geq 2^{k-1}$. Here we use the fact that there is a basic decomposition of this type $K_{2^k,2^k} = 2^{k-1}C_{2^{k+1}}$. Since $b - 2^{k-1} \leq 2^{k-1} - 1$ we now switch on $b - 2^{k-1}$ of the cycles $(x_{2i-1}, y_{2i-1}, y_{2i}, x_{2i})$, $1 \leq i \leq 2^{k-1}$, and obtain $K_{2^{k+1}} - F = aC_{2^k} + bC_{2^{k+1}}$, $2^{k-1} \leq b \leq 2^k - 1$. $\square$

Theorem 3.8. *If* $a2^k + b2^{k+1} = 2^{k+1}(2^k + 1)$, $k \geq 2$, *then* $K_{2^{k+1}+2} - F = aC_{2^k} + bC_{2^{k+1}}$.

Proof. The proof is much like that of Theorem 3.7. We first view $K_{2^{k+1}+2} - F$ as in Fig. 21.

Let $V(K_{2^k+2} - F) = \{x_1, x_2, \ldots, x_{2^k+2}\}$ and $V(K_{2^k} - F) = \{y_1, y_2, \ldots, y_{2^k}\}$. By Lemmas 3.5 and 3.6 there are decompositions $K_{2^k+2} - F = (2^{k-1} + 1)C_{2^k}$ with edges $E_1 = \{(x_{2i-1}, x_{2i}): 1 \leq i \leq 2^{k-1}\}$ each from a different cycle, and $K_{2^k} - F = (2^{k-1} - 1)C_{2^k}$ with edges $E_2 = \{y_{2i-1}, y_{2i}\}: 1 \leq i \leq 2^{k-1} - 1\}$ each from a different cycle.

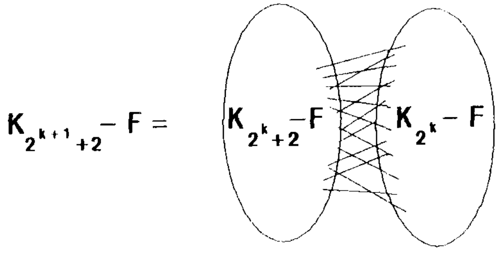


Fig. 21

If $b \le 2^{k-1} - 1$ we simply take a basic decomposition $K_{2^k+2,2^k} = (2^k + 2)C_{2^k}$ and switch on the cycles $(x_{2i-1}, y_{2i-1}, y_{2i}, x_{2i})$, $1 \le i \le b$.

If $2^{k-1} + 1 \le b \le 2^k$ we take a basic decomposition $K_{2^k+2,2^k} = (2^{k-1} + 1)C_{2^{k+1}}$ and switch on the cycles $(x_{2i-1}, y_{2i-1} y_{2i}, x_{2i})$, $1 \le i \le b - (2^{k-1} + 1)$.

This leaves the two cases $b = 2^{k-1}$ and $b = 2^k + 1$. The case $b = 2^k + 1$ is covered in Lemma 3.6. When $b = 2^{k-1}$ the construction is somewhat complicated. Consider $K_{2^{k+1}+2} - F$ as in Fig. 22.

In Theorem 3.11 we will prove that $K_{2^k+1} = C_{2^{k-1}} + 2^{k-1}C_{2^k}$ so that there is a set of edges $E = \{e_1, \dots, e_{2^{k-1}}, e\}$ so that $e_1, \dots, e_{2^{k-1}}$ are independent and each lies in a different cycle of length 2^k, e lies in the $C_{2^{k-1}}$ and e is incident with both e_1 and e_2. We now show that $K_{4m+1,4m+1} - F = (4m + 1)C_{4m}$. Let $V(K_{4m+1,4m+1} - F) = \{x_1, x_2, \dots, x_{4m+1}, y_1, y_2, \dots, y_{4m+1}\}$. Then C, the first cycle, is given by $C = (x_{m+1}, y_m, x_{m+2}, y_{m-1}, \dots, x_{2m-1}, y_2, x_{2m}, y_1, x_{2m+2}, y_{4m+1}, x_{2m+3}, y_{4m}, \dots, x_{3m}, y_{3m+3}, x_{3m+1}, y_{3m+2})$ and the remainder by $C + i$, $1 \le i \le 4m$, where $(x_{r+i}, y_{s+i}) \in E(C + i)$ if and only if $(x_r, y_s) \in E(C)$. (Subscript addition is modulo $4m + 1$).

In $G_1 = K_{2^k+1}$ with vertex set X, the decomposition can be arranged so that the set E_1 of independent edges is $E_1 = \{(x_{2i-1}, x_{2i}): 1 \le i \le 2^{k-1}\}$ and $e = (x_{2^{k-2}+1}, x_{2^{k-1}+2})$, whereas in $G_2 = K_{2^k+1}$ with vertex set Y, the decomposition is arranged so that $E_2 = \{(y_{2i-1}, y_{2i}): 1 \le i \le 2^{k-1}\}$ and $e = (y_1, y_{3\cdot 2^{k-2}+2})$. Now, for the cycles containing edges (x_{2i-1}, x_{2i}) and (y_{2i-1}, y_{2i}) switch these with the edges (x_{2i-1}, y_{2i-1}) and (x_{2i}, y_{2i}) of the 1-factor, $1 \le i \le 2^{k-1}$. For the cycles of length

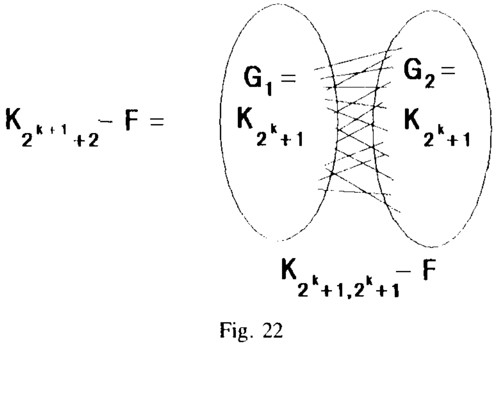


Fig. 22

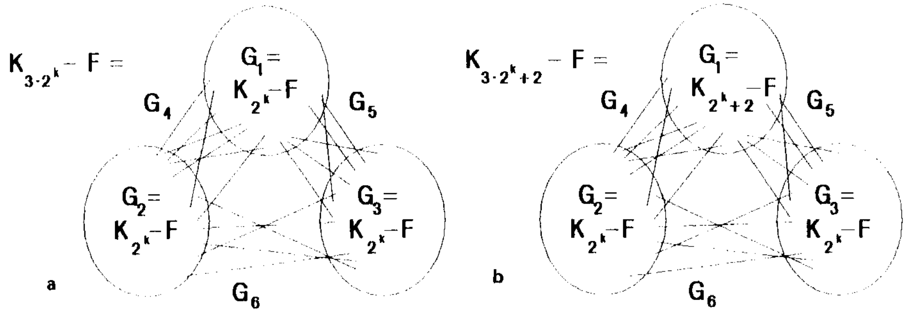


Fig. 23

2^{k-1} switch the edges $(x_{2^{k-2}+1}, x_{2^{k-1}+2})$ and $(y_1, y_{3.2^{k-2}+2})$ with the edges $(x_{2^{k-2}+1}, y_{3.2^{k-2}+2})$ and $(x_{2^{k-1}+2}, y_1)$. This yields the desired decomposition. $\square$

Theorem 3.9. *Let $n = 3.2^k$ or $3.2^k + 2$, $k \geqslant 2$, and suppose that $a2^k + b2^{k+1} = n(n-2)/2$. Then $K_n - F = aC_{2^k} + bC_{2^{k+1}}$.*

Proof. View $K_n - F$ as in Fig. 23, where $K_n - F = G_1 + G_2 + G_3 + G_4 + G_5 + G_6$.

By Lemmas 3.5 and 3.6 $K_{2^k} - F = (2^{k-1} - 1)C_{2^k}$ and $K_{2^k+2} - F = (2^{k-1} + 1)C_{2^k}$ so that with each such decomposition of G_i, $1 \leqslant i \leqslant 3$, we have a set E_i of independent edges, each from a different cycle. Let us consider the two cases separately.

(a) $n = 3.2^k$. Here $0 \leqslant b \leqslant 2^{k+1} + 2^{k-2} - 2$ and $|E_i| = 2^{k-1} - 1$.

If $0 \leqslant b \leqslant 2^k - 1$, let $G_5 = G_6 = 2^k C_{2^k}$, $G_3 = (2^{k-1} - 1)C_{2^k}$ and $G_1 + G_2 + G_4 = K_{2^{k+1}} - F = a'C_{2^k} + bC_{2^{k+1}}$.

If $2^{k-1} \leqslant b \leqslant 2^k + 2^{k-1} - 1$, $G_5 = 2^{k-1}C_{2^{k+1}}$, $G_6 = 2^k C_{2^k}$, $G_3 = (2^{k-1} - 1)C_{2^k}$ and $G_1 + G_2 + G_4 = K_{2^{k+1}} - F = a'C_{2^k} + (b - 2^{k-1})C_{2^{k+1}}$.

If $2^k + 2^{k-1} \leqslant b \leqslant 2^{k+1} - 1$, let $G_5 = G_6 = 2^{k-1}C_{2^{k+1}}$, $G_3 = (2^{k-1} - 1)C_{2^k}$ and $G_1 + G_2 + G_4 = K_{2^{k+1}} - F = a'C_{2^k} + (b - 2^k)C_{2^{k+1}}$.

Finally if $2^{k+1} \leqslant b \leqslant 2^{k+1} + 2^{k-2} - 2$, let $G_1 = G_2 = G_3 = (2^{k-1} - 1)C_{2^k}$ and let the independent edges be $E_i = E_i' \cup E_i''$ where $|E_i'| = 2^{k-2}$ and $|E_i''| = 2^{k-2} - 1$. Let $G_4 = G_5 = G_6$ have a basic decomposition $K_{2^k,2^k} = 2^{k-1}C_{2^{k+1}}$. Now switch on $b - 3.2^{k+1}$ of the cycles determined by E_2' and E_3', and G_6; E_1'', E_2'' and G_4; and $E_1' \setminus \{e_j\}$, E_3'' and G_5. Care must be taken in positioning the basic cycles so that the switching operation is possible. Notice that one cycle of length 2^k must remain.

(b) $n = 3.2^k + 2$. In this case $0 \leqslant b \leqslant 2^{k+1} + 2^{k-2} + 1$ and $|E_1| = 2^{k-1}$, $|E_2| = |E_3| = 2^{k-1} - 1$.

If $0 \leqslant b \leqslant 2^k + 1$, let $G_5 = (2^k + 2)C_{2^k}$, $G_6 = 2^k C_{2^k}$, $G_3 = (2^{k-2} - 1)C_{2^k}$ and $G_1 + G_4 + G_2 = K_{2^{k+1}+2} - F = a'C_{2^k} + bc_{2^{k+1}}$.

If $2^k + 2 \leqslant b \leqslant 2^k + 2^{k-1} + 1$, let $G_5 = (2^k + 2)C_{2^k}$, $G_6 = 2^{k-1}C_{2^{k+1}}$, $G_3 = (2^{k-1} + 1)C_{2^k}$ and $G_1 + G_4 + G_2 = K_{2^{k+1}+2} - F = a'C_{2^k} + (b - 2^{k-1})C_{2^{k+1}}$.

Finally, if $2^k + 2^{k-1} + 2 \leqslant b \leqslant 2^{k+1} + 2^{k+2} + 1$, let $G_1 = (2^{k-1} + 1)C_{2^k}$, $G_2 = G_3 =$

$(2^{k-1}-1)C_{2^k}$ and let the independent edges be, respectively $E_1 = E_1' \cup E_1''$ where $|E_1'| = |E_1''| = 2^{k-2}$, and $E_i = E_i' \cup E_1''$, $i = 2, 3$, where $|E_i'| = 2^{k-2}$ and $|E_i''| = 2^{k-2} - 1$. Let $G_4 = G_5$ have basic decomposition $K_{2^k+2,2^k} = (2^{k-1}+1)C_{2^{k+1}}$ and G_6 have basic decomposition $K_{2^k,2^k} = 2^{k-1}C_{2^{k+1}}$. Now switch on $b - (2^k + 2^{k-1} + 2)$ of the cycles determined by E_1', E_2' and G_4, E_1'', E_3' and G_5, and E_2'', E_3'' and G_6. Again care must be taken when positioning the basic cycles. Note that there remains a C_{2^k} in G_1. □

Theorem 3.10. *$K_n - F = aC_{2^k} + bC_{2^{k+1}}$, $k \geq 2$, if and only if $a2^k + b2^{k+1} = n(n-2)/2$.*

Proof. It is clear that if $K_n - F = aC_{2^k} + bC_{2^{k+1}}$, $k \geq 2$, then $a2^k + b2^{k+1} = n(n-2)/2$ and from this it follows that $n \equiv 0, 2 \pmod{2^k}$.

Suppose that $n \equiv 0, 2 \pmod{2^k}$ and $a2^k + b2^{k+1} = n(n-2)/2$. Let $n = t2^k$ or $t2^k + 2$. If $t = 1, 2$, or 3 the decompositions $K_n - F = aC_{2^k} + bC_{2^{k+1}}$ have all been determined in Lemmas 3.5 and 3.6, and Theorem 3.7, 3.8 and 3.9. We may therefore assume that $t \geq 4$.

If t is even, $t = 2r$, then we view $K_n - F$ as in Fig. 24 where $G_1 = K_{2^{k+1}} - F$ if $n \equiv 0 \pmod{2^k}$, $G_1 = K_{2^{k+1}+2} - F$ if $n \equiv 2 \pmod{2^k}$ and $G_2 = G_3 = \cdots = G_r = K_{2^{k+1}} - F$.

Now $G_1 = a_1C_{2^k} + b_1C_{2^{k+1}}$, $G_2 = a_2C_{2^k} + b_2C_{2^{k+1}}, \ldots, G_r = a_rC_{2^k} + b_rC_{2^{k+1}}$ and $K_{2^{k+1},2^{k+1}} = 2^{k+1}C_{2^{k+1}} = 2^{k+2}C_{2^k}$, $K_{2^{k+1}+2,2^{k+1}} = (2^{k+1}+2)C_{2^{k+1}} = (2^{k+2}+4)C_{2^k}$, $K_{2^{k+1},2^{k+1}} = (2^{k+2}-4)C_{2^k} + 2C_{2^{k+1}}$ (from Theorem 3.1, Lemma 3.3 and the fact that $K_{2^{k+1},2^{k+1}} = 4K_{2^k,2^k}$) and $K_{2^{k+1}+2,2^{k+1}} = 2^{k+2}C_{2^k} + 2C_{2^{k+1}}$ (from Theorem 3.1, Lemma 3.3 and the fact that $K_{2^{k+1}+2,2^{k+1}} = 2K_{2^k,2^k} + 2K_{2^k+2,2^k}$). Since each decomposition of G_i, $K_{2^{k+1},2^{k+1}}$ and $K_{2^{k+1}+2,2^{k+1}}$ can be chosen independently it is not difficult to see that all the required decompositions can be attained.

If t is odd, $t = 2r+1$, we again view $K_n - F$ as in Fig. 24 except that in this case $G_1 = K_{3.2^k} - F$ if $n \equiv 0 \pmod{2^k}$, and $G_1 = K_{3.2^k+2} - F$ if $n \equiv 2 \pmod{2^k}$. The proof now proceeds as in the case when t is even except that we use $K_{3.2^k,2^{k+1}} = (2^{k+1}+2^k)C_{2^{k+1}} = (2^{k+2}+2^{k+1})C_{2^k}$, $K_{3.2^k,2^{k+1}} = 2^{k+3}C_{2^k} + 2C_{2^{k+1}}$ (from Theorem 3.1, Lemma 3.3 and the fact that $K_{3.2^k,2^{k+1}} = 2K_{2^k,2^k} + 2K_{2^k,2^{k+1}}$) and $K_{3.2^k+2,2^{k+1}} = (2^{k+1}+2^k+2)C_{2^{k+1}} = (2^{k+2}+2^{k+1}+4)C_{2^k}$. □

$K_n - F =$

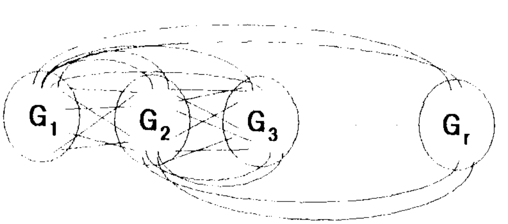


Fig. 24

Note that there are many other decompositions of "the pieces" that can be used to obtain the final decompositions of $K_n - F$.

We have now completely solved the case when n is even and next we look at the case n odd. If $K_n = C_{2^k} + bC_{2^{k+1}}$, then $n \equiv 1 \pmod{2^{k+1}}$. It remains to construct the decompositions in these cases. We begin with the case $n = 2^{k+1} + 1$. This is the critical case as from it all other decompositions are easily constructed.

Theorem 3.11. *If $a2^k + b2^{k+1} = 2^k(2^{k+1}+1)$, then $K_{2^{k+1}+1} = aC_{2^k} + bC_{2^{k+1}}$.*

In addition there is a decomposition $K_{2^{k+1}+1} = C_{2^k} + 2^kC_{2^{k+1}}$ with a set of edges $E = \{e_1, \ldots, e_{2^k}, e\}$ so that each e_i is from a different cycle of length 2^{k+1}, e lies in C_{2^k}, $E - \{e\}$ is an independent set of edges and e is incident with exactly two of the e_i. Moreover, the cycle C_{2^k} contains at most one vertex from each e_i, $1 \leq i \leq 2^k$.

Proof. When $k = 2$, $a2^2 + b2^3 = 4a + 8b = 36$ implies $a + 2b = 9$ and the only possible decompositions are $K_9 = C_4 + 4C_8 = 3C_4 + 3C_8 = 5C_4 + 2C_8 = 7C_4 + C_8 = 9C_4$. Letting $V(K_9) = (\{1, 2, \ldots, 9\}$ the cycles are given by

(a) $K_9 = C_4 + 4C_8$: (1, 2, 6, 5), (2, 7, 3, 9, 4, 6, 8, 5), (1, 4, 7, 9, 8, 2, 3, 6), (1, 7, 5, 3, 8, 4, 2, 9) and (1, 3, 4, 5, 9, 7, 8). Choosing $E = \{(4, 6), (2, 8), (1, 7), (5, 9), e = (5, 6)\}$ we see that this decomposition satisfies the requirements of the theorem.

(b) $K_9 = 3C_4 + 3C_8$: (2, 3, 4, 5), (1, 7, 9, 8), (1, 9, 3, 6), (2, 7, 3, 8, 4, 9, 5, 6), (1, 2, 4, 7, 6, 8, 5, 3) and (1, 4, 6, 9, 2, 8, 7, 5).

(c) $K_9 = 5C_4 + 2C_8$: (1, 4, 6, 8), (1, 2, 9, 3), (1, 6, 9, 7), (3, 6, 7, 5), (2, 8, 5, 4), (2, 7, 3, 8, 4, 9, 5, 6) and (1, 9, 8, 7, 4, 3, 2, 5).

(d) $K_9 = 7C_4 + C_8$: (1, 6, 7, 5), (1, 4, 6, 9), (1, 2, 9, 3), (1, 7, 9, 8), (2, 4, 3, 5), (2, 3, 6, 8), (4, 5, 8, 7), (2, 7, 3, 8, 4, 9, 5, 6).

(e) $K_9 = 9C_4$: (1, 2, 8, 3), (2, 3, 9, 4), (3, 4, 1, 5), (4, 5, 2, 6), (5, 6, 3, 7), (6, 7, 4, 8), (7, 8, 5, 9), (8, 9, 6, 1) and (9, 1, 7, 2).

Suppose $k \geq 3$, $a2^k + b2^{k+1} = 2^k(2^{k+1}+1)$ and that $a'2^t + b'2^{t+1} = 2^t(2^{t+1}+1)$, $t < k$, implies $K_{2^{t+1}+1} = a'C_{2^t} + b'C_{2^{t+1}}$ with the edges E and the cycle C_{2^t} as described above when $a' = 1$. Consider $K_{2^{k+1}+1}$ as in Fig. 25.

Let G_1 and G_2 denote the K_{2^k+1} with $V(G_1) = \{x_1, x_2, \ldots, x_{2^k}, \infty\}$ and $V(G_2) = \{y_1, y_2, \ldots, y_{2^k}, \infty\}$. By the induction hypothesis there is a decomposition $K_{2^k+1} = C_{2^{k-1}} + 2^{k-1}C_{2^k}$ with a set of edges E and $C_{2^{k-1}}$ as described. Denote this decomposition by $\mathscr{D}$.

Suppose $0 \leq b \leq 2^{k-1}$. Decompose G_1 as in $\mathscr{D}$ so that the cycle $C_{2^{k-1}}$ does not contain ∞, $e = (x_1, x_2)$, and $e_1 = (x_3, x_4)$. Decompose G_2 as in $\mathscr{D}$ so that $e = (y_1, y_2)$, $e_1 = (y_3, y_4)$ and the cycle represented here by e_1 does not contain ∞. Clearly the cycles represented by "e" are vertex disjoint as are those represented by "e_1".

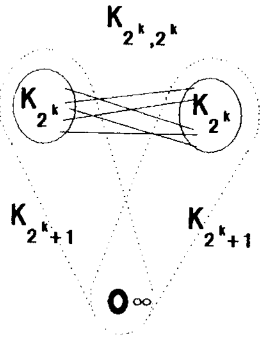


Fig. 25

According to Lemma 3.3, $K_{2^k,2^k} = sC_{2^k} + tC_{2^{k+1}}$ where $t = 2\lfloor b/2 \rfloor$. Position this decomposition so that one cycle contains the edges (x_1, y_1), (y_1, x_2), (x_2, y_2), (y_2, x_3), (x_3, y_3), (y_3, x_4) and (x_4, y_4). We now switch on the cycle (x_1, x_2, y_2, y_1). If b is odd we also switch on the cycle (x_3, x_4, y_4, y_3). This yields the required decompositions.

Suppose now that $2^{k-1} \leq b \leq 2^k$. Again using the induction hypothesis we position a decomposition $\mathcal{D}$ in G with cycles $B_1, B_2, \ldots, B_{2^{k-1}}, B$ so that $(x_{2i-1}, x_{2i}) \in E(B_i)$, $1 \leq i \leq 2^{k-1}$ and $(x_{2^k-3}, x_{2^k-1}) \in E(B)$ where B has length 2^{k-1} and, moreover, $V(B) \subseteq \{x_1, x_3, x_5, \ldots, x_{2^k-1}\}$.

Let $A = (a_{ij})$ be a latin square of order 2^{k-1} with at least three pairwise disjoint transversals $T_0 = \{a_{ii} = i : 1 \leq i \leq 2^{k-1}\}$, $T_1 = \{a_{ij(i)} : 1 \leq i \leq 2^{k-1}\}$ and $T_2 = \{a_{im(i)} : 1 \leq i \leq 2^{k-1}\}$. Since $2^{k-1} \geq 4$, these exist by [4]. Use Lemma 3.4 and A to construct a decomposition $K_{2^k,2^k} = 2^{k-1}C_{2^{k+1}}$ with cycles $H_1, H_2, \ldots, H_{2^{k-1}}$. Then (x_{2i-1}, y_{2i-1}), (y_{2i-1}, x_{2i}), (x_{2i}, y_{2i}), $(x_{2j(i)}, y_{2a_{ij(i)}})$, $(y_{2a_{im(i)}-1}, x_{2m(i)})$ and $(x_{2m(i)}, y_{2a_{im(i)}})$ are edges of H_i, $1 \leq i \leq 2^{k-1} - 1$, and $H_{2^{k-1}}$ contains the edges (x_{2^k-3}, y_d), (y_d, x_{2^k-2}), (x_{2^k-2}, y_{d+1}), (y_{d+1}, x_{2^k-1}), (x_{2^k-1}, y_{2^k-1}), $(x_{2j(i)}\, y_{2a_{ij(i)}})$, $(y_{2a_{im(i)}} - x_{2m(i)})$ and $(x_{2m(i)}, y_{2a_{im(i)}})$, where $d = 2a_{2^{k-1},2^{k-1}-1} - 1$ and $i = 2^{k-1}$.

Note that:

(1) the edges $(x_{2j(i)}, y_{2a_{ij(i)}})$, $1 \leq i \leq 2^{k-1}$ are independent,

(2) $\{y_{2a_{im(i)}-1}, y_{2a_{im(i)}} : 1 \leq i \leq 2^{k-1}\} = \{y_1, y_2, \ldots, y_{2^k}\}$ and

(3) the edge $(x_{2j(i)}, y_{2a_{ij(i)}})$ is disjoint from the vertices $x_{2i-1}, y_{2i-1}, x_{2i}$ and y_{2i}, for each i, $1 \leq i \leq 2^{k+1}$.

Finally, in $G_2 - \{\infty\}$, place the decomposition of $K_{2^k} - F$ as described in Lemma 3.5 so that the cycles $E_1, E_2, \ldots, E_{2^{k-1}-1}$ of length 2^k are represented by the edges $(y_{2i-1}, y_{2i}) \in E_i$, $1 \leq i \leq 2^{k-1} - 1$, and the edges of F are (y_1, y_{d+1}), (y_2, y_3), (y_4, y_5), $\ldots$, (y_{d-3}, y_{d-2}), (y_{d-1}, y_{d+2}), (y_d, y_{2^k-1}), (y_{d+3}, y_{d+4}), (y_{d+5}, y_{d+6}), $\ldots$, (y_{2^k-4}, y_{2^k-3}) and (y_{2^k-2}, y_{2^k}) where $d = 2a_{2^{k-1},2^{k-1}-1} - 1$.

We must now bring together all the cycles described and the edges (∞, y_i), $1 \leq i \leq 2^k$, for the desired decompositions.

In H_i, $1 \leq i \leq 2^{k-1}$ replace the edges $(y_{2a_{im(i)}-1}, x_{2m(i)})$ and $(x_{2m(i)}, y_{2a_{im(i)}})$ by the edges $(y_{2a_{im(i)}-1}, \infty)$ and $(\infty, y_{2a_{im(i)}})$. The new cycles H_i' have length 2^{k+1}.

The edges $\{(y_{2a_{im(i)}-1}, x_{2m(i)}), (x_{2m(i)}, y_{2a_{im(i)}}) : 1 \leq i \leq 2^{k-1}\}$ together with the edges of F form a cycle S of length 3.2^{k-1}. (To see this consider the union of F and the edges representing the E_i, $1 \leq i < 2^{k-1} - 1$.) This cycle contains the vertices $\{y_1, y_2, \ldots, y_{2^k}, x_2, x_4, \ldots, x_{2^k}\}$ and so is disjoint from the cycle B (of length 2^{k-1}). Using B and S and the cycle $H'_{2^{k-1}}$, and switching on the cycle $(x_{2^k-1}, x_{2^k-3}, y_d, y_{2^k-1})$ we replace B and S by a cycle W of length 2^{k+1} and obtain $H''_{2^{k-1}}$. We currently have a decomposition $K_{2^{k+1}+1} = (2^k - 1)C_{2^k} + (2^{k-1} + 1)C_{2^{k+1}}$ and now wish to switch on B_i, E_i and H'_i, $1 \leq i \leq 2^{k-1} - 1$, using the cycle $(x_{2i-1}, x_{2i}, y_{2i}, y_{2i-1})$. Doing these switchings one at a time enables us to get all decompositions $K_{2^{k+1}+1} = aC_{2^k} + bC_{2^{k+1}}$, $2^{k-1} + 1 \leq b \leq 2^k$. (Note that the 2^k-cycle $B_{2^{k-1}}$ remains unchanged.)

However, we still need to show that the decomposition $K_{2^{k+1}+1} = C_{2^k} + (2^k - 1)C_{2^{k+1}}$ obtained in this way satisfies the induction hypothesis.

Represent the cycles obtained by switching on B_i and E_i by the edge (x_{2i-1}, y_{2i-1}), $1 \leq i \leq 2^{k-1} - 1$. Represent the cycles H'_i, but with $H''_{2^{k-1}}$ instead of $H'_{2^{k-1}}$, by the edge $(x_{2j(i)}, y_{2a_{ij(i)}})$, $1 \leq i \leq 2^{k-1}$. Represent W by the edge (x_{2^k-1}, y_{2^k-1}). These edges are clearly all independent. The cycle of length 2^k is the cycle $B_{2^{k-1}}$ which can be represented by the edge (x_{2^k-1}, x_{2^k}) and the vertices of which occur in two of the independent edges already chosen, as required. Finally, since $B_{2^{k-1}}$ has all of its vertices in the set $\{\infty, x_1, x_2, \ldots, x_{2^k}\}$ it clearly has at most one vertex in common with each of the edges representing the cycles of length 2^{k+1}. This completes the proof. □

Theorem 3.12. *$K_n = aC_{2^k} + bC_{2^{k+1}}$, $k \geq 2$, if and only if $a2^k + b2^{k+1} = n(n-1)/2$.*

Proof. Clearly, if $K_n = aC_{2^k} + bC_{2^{k+1}}$, $k \geq 2$, then $a2^k + b2^{k+1} = n(n-1)/2$ and hence $n \equiv 1 \pmod{2^{k+1}}$.

Suppose that $n \equiv 1 \pmod{2^{k+1}}$ and $a2^k + b2^{k+1} = n(n-1)/2$. Let $n = t2^{k+1} + 1$ and note that $a \equiv t \pmod 2$. When $t = 1$ the decompositions are constructed in Theorem 3.11. Assuming $t > 1$ view K_n as in Fig. 26 where $G_1 = G_2 = \cdots = G_t = K_{2^{k+1}+1}$.

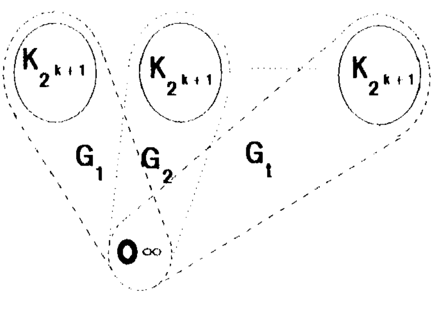


Fig. 26

Since $K_{2^{k+1},2^{k+1}} = 2^{k+1}C_{2^{k+1}} = 2^{k+2}C_{2^k}$ and each G_i can be decomposed independently, then, using Theorem 3.11, it follows that we have decompositions $K_n = aC_{2^k} + bC_{2^{k+1}}$ provided $a \geq t$ (each G_i decomposition has a cycle C_{2^k}). When $a < t$ let $G_i = C_{2^k} + 2^k G_{2^{k+1}}$, and in each, position the cycle of length 2^k so that it does not contain vertex ∞, and so that when basic decompositions $K_{2^{k+1},2^{k+1}} = 2^{k+1}C_{2^{k+1}}$ are chosen between G_{2i-1} and G_{2i}, $1 \leq i \leq \lfloor t/2 \rfloor$, a switch is possible so that the two cycles of length 2^k become one of length 2^{k+1}. □

Acknowledgements

The research of the first and the third author were supported by the Natural Sciences and Engineering Research Council of Canada under grants No. A7829 (K.H.) and A7268 (A.R.). This research was done while the second author was visiting McMaster University; he would like to thank the Department of Mathematics and Statistics for its hospitality.

References

[1] B. Alspach, Research problems, Problem 3, Discrete Math. 36 (1981) 333.
[2] B. Alspach, J.-C. Bermond, K. Heinrich, A. Rosa and D. Sotteau, A survey of cycle decompositions (to appear).
[3] T. Beth, D. Jungnickel and H. Lenz, Design Theory (Bibl. Inst., Zürich 1985).
[4] R. C. Bose, S. S. Shrikhande and E.T. Parker, Further results on the construction of mutually orthogonal latin squares and the falsity of Euler's conjecture, Canadian J. Math. 12 (1960) 189–203.
[5] H. Hanani, Balanced incomplete block designs and related designs, Discrete Math. 11 (1975) 255–369.
[6] E. Mendelsohn and A. Rosa, Embedding maximal packings of triples, Congr. Numer. 40 (1983) 235–247.
[7] R. Rees and D.R. Stinson, On resolvable group-divisible designs with block size 3, Ars Combinatoria 23 (1987) 107–120.
[8] A. Rosa, Alspach's conjecture is true for $n \leq 10$, Math. Reports, McMaster University (to appear).
[9] A. Rosa and D. Hoffman, The number of repeated blocks in twofold triple systems, J. Combin. Theory (A) 41 (1986) 61–88.
[10] D. Sotteau, Decomposition of $K_{m,n}$ ($K^*_{m,n}$) into cycles (circuits) of length $2k$, J. Combin. Theory (B) 30 (1981) 75–81.
[11] H.C. Sun, On the cycle decomposition of complete graphs (Chinese), Nanjing Daxue Xuebao Ziran Kexue Ban 21 (1985) 421–426.

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 123–135
North-Holland

SOME SELF-BLOCKING BLOCK DESIGNS

Dieter JUNGNICKEL
Mathematisches Institut, Justus-Liebig-Universität Giessen, Arndtstr. 2, D-6300 Giessen, F.R. Germany

To Haim Hanani on the occasion of his 75th birthday.

Let D be a block design which has a blocking set. We call D *self-blocking* if the following two conditions hold: (i) The committees of D (i.e. the blocking sets of minimum cardinality of D) form a block design, which we denote by D^C and (ii) The committees of D^C are precisely the blocks of D. (We also say that D and D^C are a pair of mutually blocking block designs, then.) We show that the classical projective planes $PG(2, q^2)$ are self-blocking; the same holds for $PG(2, 3)$ and $PG(2, 5)$ as well as for the classical affine planes $AG(2, q)$ with $q \geq 4$.

1. Introduction

Let D be a finite incidence structure. A subset S of the point set P of D is called a *hitting set* for D, if S meets every block of D. If moreover S does not contain any block of D, S is called a *blocking set* for D. There are incidence structures not containing any blocking set; for instance, this holds for every Steiner triple system (see Drake [15]). We shall only consider structures D admitting a blocking set in this paper. Then the blocking sets of smallest cardinality will be called the *committees* of D (following Hirschfeld [16]).

Blocking sets arose in the theory of games, cf. Richardson [19], and have been studied extensively. The systematic investigation of blocking sets begins with Bruen's papers [6, 7] on blocking sets in projective planes. Later blocking sets in more general incidence structures were studied, in particular in affine planes (see Bruen and Silverman [10]), in general block designs (see de Resmini [14] and Drake [15]) and in (r, λ)-designs (see Jungnickel and Leclerc [18]).

In the present paper, we shall consider blocking sets in block designs and introduce a new type of question about these structures. Let D be a block design admitting blocking sets. We denote by D^C the incidence structure formed by all committees of D (on the point set P of D). Our first condition will be as follows:

(1) The incidence structure D^C formed by the committees of D is a block design.

Note that this situation will arise quite often. (1) is certainly satisfied whenever D admits a 2-transitive automorphism group. We shall call D a *self-blocking* block design if it satisfies (1) and also the following condition (2).

(2) D^C admits blocking sets, and one has $(D^C)^C = D$; in other words, the committees of D^C are precisely the blocks of D (and vice versa).

In this case, we shall also say that D and D^C form a pair of *mutually blocking* block designs. The characterisation of all self-blocking block design seems to be a very hard problem, as we shall see. Our main result will be as follows.

Main Theorem. *The Desarguesian projective planes* $\mathrm{PG}(2, q^2)$ *and the Desarguesian affine planes* $\mathrm{AG}(2, q)$ (*with* $q \geq 4$) *are self-blocking block designs* (*for every prime power* q).

By a famous result of Bruen [7], the committees of $\mathrm{PG}(2, q^2)$ are exactly the Baer subplanes. Thus the first half of our Main Theorem will be an immediate consequence of the following slightly stronger assertion: Every subset of $\mathrm{PG}(2, q^2)$ which meets every Baer subplane has at least $q^2 + 1$ points; equality holds if and only if the subset is a line. We shall also use this result to study, more generally, the Baer subplanes of $\mathrm{PG}(n, q^2)$. Finally, we shall also show that the designs $\mathrm{PG}(2, 3)$ and $\mathrm{PG}(2, 5)$ are self-blocking.

It should be mentioned that a related question is studied by Cameron and Mazzocca [12]. These authors prove that the smallest hitting sets of the incidence structure D^b formed by all blocking sets of D are the lines, whenever D is a projective or affine plane containing blocking sets. Since most blocking sets do not contain a committee, this result is – though of a similar flavour – not related to our results. (Our Main Theorem is stronger, but it only applies for the planes $\mathrm{PG}(2, q^2)$.) In a sequel to [12], Cameron et al. [13] study those sets hitting every blocking set of D which do not contain a line of D (the so-called *dual blocking sets* of D).

We refer the reader to Beth et al. [1] for background from Design Theory and to Beutelspacher [3] and Hirschfeld [16] for background on blockings sets in projective planes and spaces.

2. Preliminaries

In this section we shall collect some well-known preliminary results on hitting sets and blocking sets of projective planes. The following simple lemma characterizes the smallest hitting sets:

Lemma 2.1. *Let D be a projective plane of order n, and let S be a hitting set for D. Then* $|S| \geq n + 1$; *equality holds if and only if S is a line of D.*

We next state a fundamental result of Bruen [7] which gives a lower bound for the size of a blocking set in a projective plane of order n and which implies a characterisation of the committees of $\mathrm{PG}(2, q^2)$. Bruen's original proof was somewhat involved; a simpler proof was given by Bruen and Thas [11]. An even simpler version is a special case of a proof given in Jungnickel and Leclerc [18] where Bruen's result was generalized to (r, λ)-designs following a previous generalization to symmetric designs, due to de Resmini [14] and Drake [15]. A similar proof is also contained in Bruen and Silverman [10].

Theorem 2.2 (Bruen). *Let D be a projective plane of order n, and let S be a blocking set for D. Then $|S| \geqslant n + \sqrt{n} + 1$; equality holds if and only if S is a Baer subplane of D.*

Corollary 2.3 (Bruen). *The committees of the Desarguesian projective plane* $\mathrm{PG}(2, q^2)$ *(q a prime power) are precisely the Baer subplanes.*

Writing $D = \mathrm{PG}(2, q^2)$, we thus have that the blocks of D^C are just the Baer subplanes of D. Since D has a 2-transitive group, it is clear that D^C is a design (and thus D satisfies condition (1)). We compute the parameters of D^C:

Proposition 2.4. *Let $D = \mathrm{PG}(2, q^2)$, q a prime power. Then the incidence structure D^C (the blocks of which are the Baer subplanes of D) is a block design with parameters*

$$v = q^4 + q^2 + 1, \qquad k = q^2 + q + 1, \qquad b = q^3(q^2 + 1)(q^3 + 1),$$
$$r = (q^2 + 1)q^3(q + 1) \quad \textit{and} \quad \lambda = q^2(q + 1)^2.$$

Proof. The number b of Baer subplanes of $\mathrm{PG}(2, q^2)$ is well-known, see e.g. Hirschfeld [16, p. 88]. (Since each quadrangle of D determines a unique Baer subplane this can be easily checked by the reader.) Then r is determined from $vr = bk$, and λ is obtained from $\lambda(v - 1) = r(k - 1)$. □

It is our aim to show that D^C also satisfies condition (2), i.e. that the blocking sets of D^C are the lines of D. We remark that the bounds of Drake [15] and of Jungnickel and Leclerc [18] yield only weak results here. The best result which can be obtained by standard inequalities seems to be the following: It is known that the minimum size of a blocking set S satisfies $s \geqslant r/\lambda$ (see Jungnickel and Leclerc [18]), which here results in the bound $s \geqslant q^2 - q + 1$. Thus we require special arguments.

3. Sets meeting all Baer subplanes of $\mathrm{PG}(2, q^2)$

In this section we shall prove that a hitting set S for the design D^C of Proposition 2.4 has at least $q^2 + 1$ points (with equality if and only if S is a line of $\mathrm{PG}(2, q^2)$). We will proceed by first proving the following result complementing Lemma 2.1:

Proposition 3.1. *Let D be a projective plane of order n, and let S be a set of at* *most $n+1$ points of D. Then one has one of the following alternatives:*

There are three non-concurrent lines L, L', L'' which are disjoint from S. (3)

S contains n collinear points. (4)

Proof. Assume that both (3) and (4) fail. Let G be a line that meets S in at least two points. Since (4) fails, there are two points x, x' in $G\backslash S$. Then x and x' are on lines L and L' disjoint from S, as $|S| \leqslant n+1$. Since (3) fails, every line must contain a point of $S \cup \{p\}$ where $p = L \cap L'$. Considering the lines through x one sees that $|S| = n+1$. Thus some line H through p meets S in two points. Choose a point q in $H\backslash(S \cup \{p\})$. Then q lines on a line L'' disjoint from $S \cup \{p\}$, a contradiction to the assumption that (3) fails. □

Theorem 3.2. *Let S be a set of points of* PG$(2, q^2)$ *which meets every Baer subplane. Then $|S| \geqslant q^2+1$, and equality holds if and only if S is a line.*

Proof. We may assume that $|S| \leqslant q^2+1$; the assertion is that S is a line, then. Assume otherwise. By Proposition 3.1, there are two cases to be considered.

Case 1. There are three non-concurrent lines L, L', L'' which are disjoint from S. Let p, q, r be the three points of intersection of these lines, and write $T = L \cup L' \cup L''$. Then each point not in T forms together with p, q, r a quadrangle and thus determines a unique Baer subplane of PG$(2, q^2)$. Each such Baer subplane contains exactly $(q-1)^2$ points not in T; thus there are $(q+1)^2$ Baer subplanes containing p, q, r, and these subplanes split the points off T into $(q+1)^2$ sets of $(q-1)^2$ each. Since $S \cap T = \emptyset$ and since $|S| \leqslant q^2+1$, S cannot meet all these Baer subplanes, a contradiction.

Case 2. S consists of n points of a line L and, possibly, of one further point p not on L. Denote the unique point of L not in S by r, and note that Aut PG$(2, q^2)$ is transitive on triples (L, p, r) with $r \in L$ and $p \notin L$, since it is transitive on triangles. Choose any Baer subplane B, and let L' be a line meeting B only once, say in r'. Moreover, choose a point p' not in $B' \cup L'$. Mapping (L', p', r') onto (L, p, r), we obtain a Baer subplane disjoint from S, a contradiction. □

Theorem 3.2 shows that the smallest hitting sets for the design D^C defined in Proposition 2.4 are the lines of the original design $D = $ PG$(2, q^2)$ Since no line contains a Baer subplane, we see that these hitting sets are in fact the committees of D^C; thus D^C satisfies condition (2) and we have proved the first half of our principal result:

Theorem 3.3. *The Desarguesian projective plane* PG$(2, q^2)$ *(q a prime power) is a self-blocking block design.*

We shall consider some other designs in the following sections. But first we mention the following consequence of Theorem 3.3.

Corollary 3.4. *Let* $D = \mathrm{PG}(2, q^2)$ *and* D^C *as in Proposition* 2.4. *Then* $\mathrm{Aut}\, D = \mathrm{Aut}\, D^C$. *In other words: Any bijection of the point set of* $\mathrm{PG}(2, q^2)$ *which maps every Baer subplane onto a Baer subplane is a collineation of* $\mathrm{PG}(2, q^2)$, *i.e. a member of* $P\Gamma L(3, q^2)$.

Cameron and Mazzocca [12] have shown that any bijection of a projective plane of order $\neq 2$ which preserves blockings sets is in fact a collineation. Corollary 3.4 strengthens this result for the planes $\mathrm{PG}(2, q^2)$. As already mentioned, the main interest in the sequel [13] is in sets meeting each blocking set of a projective plane and not containing any line. This leads us to the following problem.

Problem 3.5. Let S be a set of points of $\mathrm{PG}(2, q^2)$ meeting every Baer subplane and not containing any line. What is the minimum size of S? (Note that such sets exist: The simplest example is the complement of a line.)

4. Committees of $\mathrm{PG}(n, q^2)$

In this section we shall briefly consider the symmetric design $\mathrm{PG}_{n-1}(n, q)$ with $n \geq 3$, the blocks of which are the hyperplanes of $\mathrm{PG}(n, q)$. By the theorem of Bose and Burton [4], the committees of this design are the lines (if we use the standard definitions for arbitrary incidence structures given above). Thus we would have $D^C = \mathrm{PG}_1(n, q)$ for $D = \mathrm{PG}_{n-1}(n, q)$. Clearly D^C is a design, and the hitting sets of minimal size of D^C are the hyperplanes, i.e. the blocks of D (again using the theorem of Bose and Burton [4]). However, D is not self-blocking, since the hyperplanes are not blocking sets of D^C (they contain lines).

Since the correspondence between lines and hyperplanes sketched above is somewhat trivial, Bruen [8] and Beutelspacher [2] have suggested to impose the stronger condition

(*) S meets every hyperplane, but S contains no line

to define blocking sets in $\mathrm{PG}(n, q)$. To avoid confusion, we shall call such a set S a *strong blocking set.* Using Corollary 2.3 as the starting point for an induction argument, one can prove the following result.

Theorem 4.1 (Beutelspacher [2], Bruen [8]). *Let S be a strong blocking set of* $\mathrm{PG}_{n-1}(n, q)$. *Then one has* $|S| \geq q + \sqrt{q} + 1$; *equality holds if and only if S is a Baer subplane of some plane of* $\mathrm{PG}(n, q)$.

Thus the *strong committees* of $PG_{n-1}(n, q^2)$ are the Baer subplanes of the planes of $PG(n, q^2)$. Clearly all these Baer subplanes form a block design; we will not bother determining its parameters. We shall now show that Theorem 3.2 may be used to obtain a lower bound on the cardinality of hitting sets for this design.

Theorem 4.2. *Let S be a subset of* $PG(n, q)$, *q a square, which meets every Baer subplane. Then* $|S| \geq q^{n-1} + \cdots + q + 1$.

Proof. We use induction on n; the case $n = 2$ is true by Theorem 3.2. Now assume that the assertion holds for $n - 1$, where $n \geq 3$. Let H be any hyperplane of $PG(n, q)$, and put $S_H = S \cap H$. Clearly S_H meets every Baer subplane of $PG(n, q)$ contained in H. Since H is isomorphic to $PG(n-1, q)$, we obtain $|S_H| \geq q^{n-2} + \cdots + q + 1$. Now count flags (p, H) where p is a point in S and H a hyperplane to obtain

$$(q^n + \cdots + q + 1)(q^{n-2} + \cdots + q + 1) \leq |S|\,(q^{n-1} + \cdots + q + 1),$$

hence

$$|S| \geq q^{n-2} + \cdots + q + 1 + q^n(q^{n-2} + \cdots + q + 1)/(q^{n-1} + \cdots + q + 1)$$

which gives the assertion. □

We have not been able to characterize the case of equality in Theorem 4.2. Note that the hyperplanes do give examples, but there might be other ones. Of course, the hyperplanes are not blocking sets of the design formed by the Baer subplanes of $PG(n, q)$, q a square, and thus $PG_{n-1}(n, q)$ is not self-blocking for $n \geq 3$, no matter whether one considers ordinary or strong blockings sets. We conclude this section with the following conjecture.

Conjecture 4.3. *Let S be a subset of* $PG(n, q)$, *q a square, which meets every Baer subplane. Then $|S| = q^{n-1} + \cdots + q + 1$ if and only if S is a hyperplane.*

5. Committees of PG(2, 3) and PG(2, 5)

In this section we shall show that PG(2, 3) and PG(2, 5) are self-blocking. First let $D = PG(2, 3)$. It is known that the committees of D are precisely the *projective triangles*, see Hirschfeld [16, Th. 13.4.4]. This means the following (cf. *Fig. 1*). A committee consits of a triangle p_1, p_2, p_3 and of three collinear points q_1, q_2, q_3, where q_i is on $p_j p_k$ (i, j, k a permutation of 1, 2, 3). Note that the line $q_1 q_2 q_3$ contains a unique fourth point q_4 (which forms a quadrangle together with the p_i's) and that the line joining the q_j's is the unique line through q_4 not containing any p_i. So in fact the committees of D are determined by the quadrangles with a distinguished point q_4. This shows that any triangle $p_1 p_2 p_3$ is contained in precisely four committees as the complement of a collinear triple. But since the

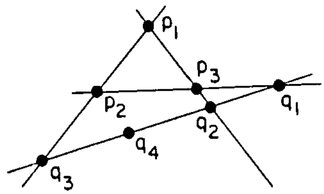


Fig. 1.

triangle $p_iq_jq_k$ together with the fourth point on $p_jp_kq_i$ determines the same committee as $p_1p_2p_3$ and q_4, each committee contains four triangles as the complement of a collinear triple. Thus the number of committees agrees with the number of triangles. Hence D^C is a block design with parameters

$$v = 13, \qquad b = 234, \qquad k = 6, \qquad r = 108 \quad \text{and} \quad \lambda = 45.$$

Note that PGL(3, 3) acts transitively on committees.

We now claim that the blocking sets of D^C have size at least 4, and that equality occurs only for the lines of D. (Clearly the lines of D are blocking sets for D^C.) Thus let S be a blocking set of D^C and assume $|S| \leq 4$. We have to show that S is a line. This is accomplished by proving that any other configuration of at most 4 points will be disjoint from a suitable committee. Because of the transitivity properties of PGL(3, 3) it is clearly sufficient to consider a committee and to show that every type of configuration of at most 4 points is contained in its complement, excepting lines. This can be seen by elaborating *Fig. 1* (see *Fig. 2*). Let $a = p_1q_4 \cap p_2p_3$, $b = p_1p_2 \cap aq_2$, $c = ab \cap p_1q_1$, $d = bq_1 \cap p_1a$, $e = bq_1 \cap p_1p_3$, $f = ae \cap p_1c$. This gives most of PG(2, 3), and the complement of our committee contains both the quadrangle $abeq_4$ and the three collinear points bde together with the point a not on bde. This proves the assertion. We collect our results:

Theorem 5.1. *Let D = PG(2, 3). Then D^C is a design $S_{45}(2, 6, 13)$, and the hitting sets of minimal size of D^C are the lines of D. Thus D is self-blocking.*

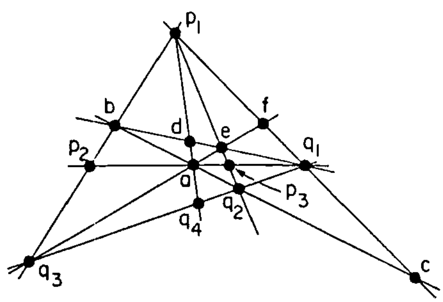


Fig. 2.

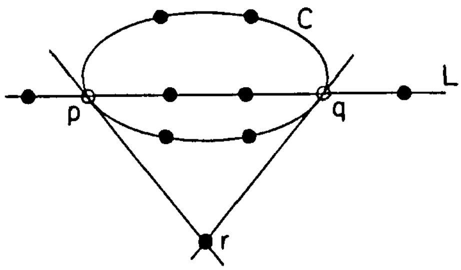


Fig. 3.

We now turn our attention to the case $D = \mathrm{PG}(2, 5)$. Here the committees are determined by a conic C together with two points p and q on C as follows (cf. Hirschfeld [16, Th. 13.4.7]). Let r be the point of intersection of the tangents at C in p and q, and let $L = pq$.

Then $S = (C \cup L \cup \{r\}) \setminus \{p, q\}$ is a committee. Note that PGL(2, 5) is transitive on committees. Cf. *Fig. 3.* Clearly the committees form a design D^C; the determination of its parameters will be omitted. One can then use arguments similar to those for PG(2, 3) to show that the smallest hitting sets of D^C are the lines of D. The case analysis is, however, more involved. We omit all details and just state the following result.

Theorem 5.2. PG(2, 5) *is a self-blocking block design.*

In the light of Theorems 5.1 and 5.2, the following problem is natural:

Problem 5.3. Is $\mathrm{PG}(2, q)$ self-blocking for all prime powers q?

Since at present not even the committees of $\mathrm{PG}(2, q)$ are known (unless q is a square or very small), there seems to be no hope of solving this problem with the present methods. David A. Drake has shown that PG(2, 7) is also self-blocking (private communication).

6. Committees of $\mathrm{AG}(2, q)$

In this section we discuss the committees of the Desagruesian affine plane $\mathrm{AG}(2, q)$, where $q \geq 4$. (It is well known that AG(2, 2) and AG(2, 3) do not contains any blocking sets.) We first recall the following fundamental result of Jamison [17].

Theorem 6.1 (Jamison). *Let S be a hitting set of* $\mathrm{AG}(2, q)$. *Then* $|S| \geq 2q - 1$.

A somewhat simpler proof of 6.1 is given in Brouwer and Schrijver [5]. It should be noted that 6.1 does not hold for non-Desarguesian affine planes, see

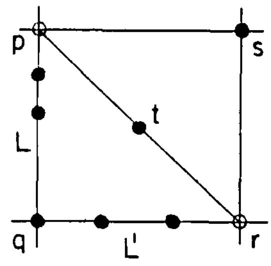


Fig. 4.

Bruen and de Resmini [9]. For example, the Hughes plane of order 9 gives rise to an affine plane of order 9 containing a blocking set with 16 points only.

Unfortunately, the case of equality in Theorem 6.1 has not been characterised. In fact it seems that the committees of AG(2, q) have not been discussed in the literature up to now (except for $q=4$). As we shall see, the case $q=4$ is exceptional. We thus start by exhibiting three classes of committees of AG(2, q), where $q \geq 5$.

Example 6.2. Let $q \geq 5$ be a prime power, and let $D = \mathrm{AG}(2, q)$. Choose a triangle p, q, r and put $L = pq$, $L' = qr$. Let s be the intersection point of the lines parallel to L (resp. L') passing through r (resp. p), and let t be any point $\neq p, r$ on pr. Then $S = (L \cup L' \cup \{s, t\}) \setminus \{p, r\}$ is a blocking set of cardinality $2q-1$ and thus (by 6.1) a committee of AG(2, q). Cf. *Fig. 4.*

Example 6.3. Let $q \geq 5$ be a prime power, and let $D = \mathrm{AG}(2, q)$. Choose a q-arc C meeting each line in the parallel class of some line L. (C is a parabola obtained from a conic in PG(2, q), where we take a tangent as line at infinity.) Let $p = C \cap L$, and choose a point $r \neq p$ on the tangent at C through p. Then $S = (C \cup L \cup \{r\}) \setminus \{p\}$ is a blocking set of cardinality $2q-1$ and thus a committee of AG(2, q). Cf. *Fig. 5.*

Example 6.4. Let q be any prime power ≥ 3 and consider a Baer subplane B of PG(2, q^2). Choose a tangent line L_∞ of B and use this line in defining the affine

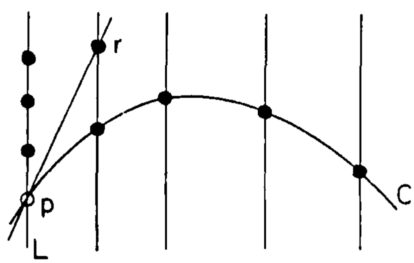


Fig. 5.

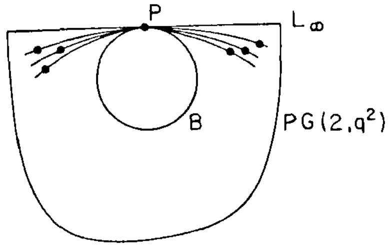


Fig. 6.

plane AG$(2, q^2)$. Denote the point of intersection of B and L_∞ by p and write $B' = B \setminus \{p\}$. Then the subset B' of AG$(2, q^2)$ meets every line of AG$(2, q^2)$ excepting the $q^2 - q - 1$ further tangents of B through p. Select one point on each of these tangents (arbitrarily, but not using $q^2 - q - 1$ collinear points). Adjoining these points to B' then results in a committee S of AG$(2, q^2)$. Cf. *Fig. 6.*

Problem 6.5. Determine all committees of AG$(2, q)$, where $q \geq 5$.

Since we do not know whether there are any committees of AG$(2, q)$ different from those described in 6.2, 6.3 and 6.4, we cannot compute the parameters of the design D^C formed by the committees of $D =$ AG$(2, q)$. However, D^C clearly is a design, since Aut AG$(2, q)$ is 2-transitive.

We now consider the case $q = 4$. Note that the constructions of 6.2, 6.3 and 6.4 do not necessarily result in blocking sets here but only in hitting sets: In 6.2, S may contain the line st, in 6.3, the point r may be on a line contained in S. We first exhibit a class of blocking sets of size 8 (which is a special case of blocking sets used by Cameron and Mazzocca [12]).

Example 6.6. Let L and L' be two parallel lines of AG(2, 4), and choose points p and p' on L and L', respectively. Let r, s be the remaining two points on the line pp'. Then $S = (L \cup L' \cup \{r, s\}) \setminus \{p, p'\}$ is a blocking set of size 8. Cf. *Fig. 7.*

There is some confusion in the literature regarding the size of the committees of AG(2, 4). By Theorem 6.1, each hitting set has at least 7 points. Now Bruen and Thas [11] claim that it is easy to construct a blocking set of size 7 in AG(2, 4) by using a Baer subplane of PG(2, 4). On the other hand, Bruen and Silverman

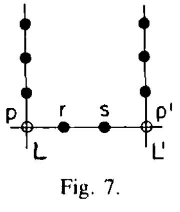


Fig. 7.

prove the following result in [10]:

If S is a blocking set in an affine plane of square order n,

$$\text{then } |S| \geqslant n + \sqrt{n} + 2. \quad (5)$$

(Note that this result has been misquoted in [9] where the condition that n is a square was omitted.) We shall provide a proof at the end of this section. Note that (5) implies that any blocking set of AG(2, 4) has at least 8 points. We shall now give a proof of this fact and also determine the structure of these sets. More precisely, we show the following:

Proposition 6.7. *All blocking sets of* AG(2, 4) *have* 8 *points and arise as described in Example* 6.6.

Proof. Let S be a blocking set of AG(2, 4); as already noted, 6.1 implies $|S| \geqslant 7$. Assume that $|S| = 7$. Embed AG(2, 4) into the projective plane PG(2, 4) and add any point p on the line at infinity to S. This results in a blocking set S' of size 8 of PG(2, 4). Now Theorem 3 of Bruen and Thas [11] yields two possible cases:

Case 1. S' is a Baer subplane B of PG(2, 4) together with a further point q. Clearly q is one of the points of S, since B has to meet the line at infinity (in p). Thus the point q has to be on the second line of PG(2, 4) which meets B exactly in p. But this line is met by each of the four lines of B not containing p, and so q is on one of these lines. Thus S contains a line of AG(2, 4) passing through q, a contradiction.

Case 2. There is a triangle p, q, r and a point s on qr, such that $S' = (pq \cup pr \cup \{s\}) \setminus \{q, r\}$, see *Fig. 8*. Note that p is indeed on the line at infinity. Thus the lines pq and pr are parallel in AG(2, 4), and S does not meet one of the parallels of these two lines, a contradiction.

This shows that each blocking set of AG(2, 4) contains at least 8 points. Since the complement of a blocking set is also a blocking set, we see that all blocking sets of AG(2, 4) have size 8. Standard counting arguments show that $b_3 = b_1 = 8$ and $b_2 = 4$ where b_i is the number of i-secants of a blocking set S (i.e., of lines that meet S in exactly i points). Thus some parallel class of AG(2, 4) contains two 3-secants of S. It now follows easily that S is of the type of Example 6.6. □

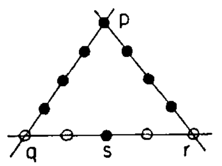


Fig. 8.

Corollary 6.8. *Let $D = \mathrm{AG}(2, 4)$. Then the committees of D form a resolvable design D^C with parameters*

$$v = 16, \qquad b = 120, \qquad k = 8, \qquad r = 60 \quad \text{and} \quad \lambda = 28.$$

Proof. Left to the reader. □

We conclude this section by proving (5); our proof will be different from the one in [10]. Let A be an affine plane of order n, where n is a square, and let S be a blocking set of A. Bruen and Thas [11] show that $|S| \geqslant n + \sqrt{n} + 1$. (It is in fact easy to deduce this from Theorem 2.2: Adding a point on the line at infinity to S results in a blocking set of the projective extension P of A.) Assume now $|S| = n + \sqrt{n} + 1$. Arguing as in the proof of 6.7, we get a blocking set S' of P with $|S'| = n + \sqrt{n} + 2$. We may assume $n > 4$; then only Case 1 above can occur (see [11, Th. 3]), and we obtain a contradiction as above. Thus we have:

Theorem 6.9 (Bruen and Silverman). *Let S be a blocking set in an affine plane of order n, where n is a square. Then $|S| \geqslant n + \sqrt{n} + 2$.*

7. Sets meeting all committees of AG(2, q)

In this section we prove our second principal result:

Theorem 7.1. *Let $D = \mathrm{AG}(2, q)$, $q \geqslant 4$, and let S be a set of points of D which meets every committee. Then $|S| \geqslant q$, and equality holds if and only if S is a line of D.*

Proof. We first assume $q \geqslant 5$. Assume that S meets all committees of D, where $|S| \leqslant q$. We have to show that S is a line, then. In fact we will prove that this assertion already follows from the assumption that S meets all committees of the type described in Example 6.2. To this end, we consider S as a subset of the projective extension PG(2, q) of D. By Proposition 3.1, we see that either S is a line of AG(2, q) or that there are three non-concurrent lines of PG(2, q) which are disjoint form S. We have to show that the second alternative is impossible. Assume otherwise; then there are two intersecting lines L and L' of D which are disjoint from S. We can choose any one of the $q^2 - 2q + 1$ points outside of $L \cup L'$ as the point s described in Example 6.2 by suitably selecting the points p and r on L and L', respectively. Thus there are at least $q^2 - 3q + 1$ choices of s for which $s \notin S$. A computation shows that we may then select s in such a way that there is a point t on pr which is not contained in s. But this means that S misses the committee just constructed, a contradiction.

It remains to consider the case $q = 4$. The committees of AG(2, 4) have been determined in Proposition 6.7 (see *Fig.* 7). Clearly the complement of the committee given in *Fig.* 7 contains all types of configurations of at most 4 points, excepting the lines. Using the transitivity properties of Aut AG(2, 4) this will yield the assertion (cf. the analysis for PG(2, 3)). The details are left to the reader. □

Corollary 7.2. *The Desarguesian affine plane* AG(2, q), $q \geq 4$, *is a self-blocking block design.*

Acknowledgements

The final version of this paper was written while the author was a visiting professor at the University of Waterloo. He would like to thank this institution for its hospitality and NSERC for financial support under grant IS-0367. He is also grateful to Lynn Batten for providing him with a preprint copy of [10]. Last but not least, thanks are due to a referee for his detailed comments which resulted in several improvements of the presentation of this paper.

References

[1] T. Beth, D. Jungnickel and H. Lenz, Design Theory (Bibliographisches Institut, Mannheim, 1985, and Cambridge University Press, Cambridge, 1986).
[2] A. Beutelspacher, Blocking sets and partial spreads in finite projective spaces, Geom. Ded. 9 (1980) 425–449.
[3] A. Beutelspacher, Einführung in die endliche Geometrie II (Bibliographisches Institut, Mannheim 1983).
[4] R.C. Bose and R.C. Burton, A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonald codes. J. Combin. Th. 1 (1966) 96–104.
[5] A.E. Brouwer and A. Schrijver, The blocking number of an affine space, J. Combin. Th. (A) 24 (1978) 251–253.
[6] A.A. Bruen, Baer subplanes and blocking sets, Bull. Amer. Math. Soc. 76 (1970) 342–344.
[7] A.A. Bruen, Blocking sets in finite projective planes, SIAM J. Appl. Math. 21 (1971) 380–392.
[8] A.A. Bruen, Blocking sets and skew subspaces of projective space, Canad. J. Math. 32 (1980) 628–630.
[9] A.A. Bruen and M.L. de Resmini, Blocking sets in affine planes, Ann. Discr. Math. 18 (1983) 169–176.
[10] A.A. Bruen and R. Silverman, Arcs and blocking sets II, Europ. J. Combin. 8 (1987) 351–356.
[11] A.A. Bruen and J.A. Thas, Blocking sets, Geom. Ded. 6 (1977) 193–203.
[12] P.J. Cameron and F. Mazzocca, Bijections which preserve blocking sets, Geom. Ded. 21 (1986) 219–229.
[13] P.J. Cameron, F. Mazzocca and R. Meshulam, Dual blocking sets in projective and affine planes, preprint.
[14] M.J. de Resmini, On blockings sets in symmetric BIBDs with $\lambda \geq 2$, J. Geom. 18 (1982) 194–198.
[15] D.A. Drake, Blocking sets in block designs, J. Combin. Th. (A) 40 (1985) 459–462.
[16] J.W.P. Hirschfeld. Projective geometries over finite fields (Oxford University Press, Oxford, 1979).
[17] R.E. Jamison, Covering finite fields with cosets of subspaces, J. Combin. Th. (A) 22 (1977) 253–266.
[18] D. Jungnickel and M. Leclerc, Blocking sets in (r, λ)-designs, Ars Combin. 22 (1986) 211–219.
[19] M. Richardson, On finite projective games, Proc. Amer. Math. Soc. 7 (1956) 458–465.

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 137–157
North-Holland

THE STEINER SYSTEMS $S(2,4,25)$ WITH NONTRIVIAL AUTOMORPHISM GROUP

Earl S. KRAMER
University of Nebraska, Lincoln, Nebraska 68588-0323, U.S.A.

Spyros S. MAGLIVERAS
University of Nebraska, Lincoln, Nebraska 68588-0115, U.S.A.

Rudolf MATHON
University of Toronto, Toronto, Ontario M5S 1A4, Canada

Dedicated to Haim Hanani on his 75th birthday.

There are exactly 16 non-isomorphic Steiner systems $S(2, 4, 25)$ with nontrivial automorphism group. It is interesting to note that each of these designs has an automorphism of order 3. These 16 designs are presented along with their groups and other invariants. In particular, we determine and tabulate substructures for each of the sixteen designs including Fano subplanes, ovals, complete 5-arcs, parallel classes and near-resolutions. One design has three mutually orthogonal near-resolutions and this leads to an (already known) elliptic semiplane. The sixteen designs are discriminated by means of the substructures mentioned above. Although not tabulated in this paper, we did compute the block-graph invariants which also discriminate the sixteen designs.

1. Introduction

A Steiner system $S(t, k, v)$ is an ordered pair (X, B) where X is a v-set of *points* and B a collection of k-subsets of X, called *blocks*, such that any t-subset of X appears exactly once among the blocks in B. For details and basic facts on Steiner systems and t-designs see [2, 9], or [15].

If H is a group of automorphisms of a t-design (X, B) let $X_1, X_2, \ldots, X_m$ be the point-orbits and $O_1, O_2, \ldots, O_n$ be the block-orbits of H. We define the *tactical decomposition* of (X, B) with respect to H to be the $m \times n$ matrix $T_H = (t_{ij})$ where $t_{ij} = |X_i \cap \mathrm{B}|$ with $\mathrm{B} \in O_j$. When σ is an automorphism of the design (X, B) we let T_σ be the tactical decomposition of the design with respect to the cyclic group generated by σ. For a more general and detailed treatment of tactical decompositions see [2].

Let r be the number of blocks passing through any given point of X and $\lambda = \lambda_2$ the number of blocks passing through any pair of points of X. If $A = (a_{ij})$ denotes any point-block incidence matrix of (X, B), then easily

$$AA^{\mathrm{T}} = \lambda J + (r - \lambda)I, \quad AJ = rJ \tag{1}$$

where I, J are the identity and all ones matrices. We immediately get:

$$\sum_{q=1}^{n} t_{iq}s_q = rr_i, \qquad \sum_{q=1}^{n} t_{iq}t_{jq}s_q = \lambda r_i r_j, \tag{2}$$

where $r_i = |X_i|$, $s_j = |O_j|$ and $1 \leq i, j \leq m$, $i \neq j$.

The *block-intersection graph* of the design (X, B) is the graph whose vertices are the blocks of B, where two blocks B_1 and B_2 are adjacent whenever $\mathrm{B}_1 \cap \mathrm{B}_2 \neq \emptyset$. For a given vertex v, let n_j be the number of pairs of $\dot{v}$, $\ddot{v}$ different from v such that exactly j other vertices are simultaneously adjacent to v, $\dot{v}$, $\ddot{v}$. The matrix of row vectors $(\cdots, n_j, \cdots)$ one for each representative v of a block orbit under the full automorphism group G of (X, B) is the *block-graph invariant* of (X, B). The block-graph invariant of a design is also related to the so called 4-vertex condition (see [11]). When (X, B) is a Steiner 2-design, the block-intersection graph is strongly regular (see [4]). The block-graph invariant provided a discriminant during early stages of our study of $S(2, 4, 25)$'s. Subsequently, we investigated substructures which had more interpretive value than block-graph invariants, and these substructure properties also discriminate the 16 known $S(2, 4, 25)$'s. Thus for each design we tabulate substructure data but we do not present the block-invariants.

2. Structure of automorphisms and other facts

In this section we develop some of the structural properties of automorphisms of $S(2, 4, 25)$'s. We denote by G the full automorphism group of an $S(2, 4, 25)$. The following theorem was proved in [12].

Theorem 2.1. *Let p be a prime dividing the order of the full automorphism group G of an $S(2, 4, 25)$. Then, $p = 2$, 3, 5 or 7. Further, if $\alpha \in G$ has order p and*
 (i) *$p = 3$, then α fixes 1 or 4 points;*
 (ii) *$p = 5$, then α fixes no points;*
 (iii) *$p = 7$, then α fixes 4 points.*

We presently establish the following:

Theorem 2.2. *Let α be an automorphism of an $S(2, 4, 25)$ where α has order 2. Then, α fixes 1 or 5 points.*

Proof. Let B be the 50 blocks of an $S(2, 4, 25)$ on the set $X = F \cup Y$, with $Y \cap F = \emptyset$, where F is the set of fixed points of α. Let $B_i = \{\mathrm{B} \in B : |\mathrm{B} \cap F| = i\}$, $0 \leq i \leq 4$, and set $b_i = |B_i|$. Let $f = |F|$ and $t = b_4$. Clearly f is odd and $b_3 = 0$. Let b_0' be the number of fixed blocks in B_0 and set $b_0'' = b_0 - b_0'$. We will argue that the possible values for our parameters are given in the following table:

b_4	f	b_0'	b_0''	b_1	b_2	b_3
t	f	$((25-f^2)/4)$ $+3t$	$((3f^2-34f+175)/4)$ $-6t$	$f(9-f)$ $+8t$	$(f(f-1)/2)$ $-6t$	0
0	1	6	36	8	0	0
0	5	0	20	20	10	0
1	5	3	14	28	4	0

Now, any block in B_2 is uniquely determined by a pair of points of F which are not covered by a block in B_4, so we easily get the formula for b_2. We call a pair of points of X appearing in a 2-cycle of α a *pure pair*. Note that each block of B_2 uses a unique pure pair. The blocks in B_0 that are fixed by α are formed by pairing-off the pure pairs which are not covered by B_2. An easy count yields the formula for b_0'. Observe that the number of fixed blocks $b_4+b_2+b_0'=(f-1)^2/4+2(3-t)$ must be even and hence $f\equiv 1 \pmod 4$. To cover pairs of points in Y we have that $b_2+3b_1+6b_0'+6b_0''=\binom{25-f}{2}$ and since $b_4+b_2+b_1+b_0'+b_0''=50$, we easily get the formulas for b_1 and b_0''. Now $0\leq b_0'$ and $0\leq b_0''$ easily gives $2(f^2-25)\leq 24t\leq 3f^2-34f+175$, and then $0\leq(f-25)(f-9)$. But α has order 2 so $f\neq 25$ and if $f=9$ then $b_0'b_0''<0$. Hence, $f=1$, or 5 and the possible values for t complete our table. □

An $S(2, 4, 25)$ with automorphism group of order 150 was constructed by R.C. Bose in 1939. In 1980 three $S(2, 4, 25)$'s with automorphism groups of orders 504, 63 and 21 respectively were constructed by A.E. Brouwer (unpublished) and independently by V.D. Tonchev (also unpublished). The four designs just mentioned appear listed in [4]. Brouwer and Tonchev show the following:

Theorem 2.3. *There are exactly* 3 *non-isomorphic Steiner systems* $S(2, 4, 25)$ *having an automorphism of order* 7 *and exactly one with an automorphism of order* 5. *The orders of G are* 504, 63, 21 *and* 150 *respectively.*

It was shown in [9] that 3^3 cannot divide the order of the automorphism group G of an $S(2, 4, 25)$ and that there are exactly five $S(2, 4, 25)$'s with 9 dividing the order of G. It was also shown that when 9 divides the order of G, a 3-Sylow subgroup of G is elementary abelian. An $S(2, 4, 25)$ with $|G|=9$ was announced by H. Gropp [5] but all eight of the designs mentioned above were constructed by L.P. and A.Y. Petrenyuk [16, 17], by means of transformations on an initial $S(2, 4, 25)$. We briefly discuss these methods in Section 6.

In what follows we obtain 8 new $S(2, 4, 25)$'s each admitting a full automorphism group of order 3, and we establish that there are no new $S(2, 4, 25)$'s in case 2 divides $|G|$. Thus, there are altogether sixteen nonisomorphic $S(2, 4, 25)$'s with nontrivial automorphism group.

3. Automorphism of order 3 and tactical decompositions

From Theorem 2.1 we see that an automorphism of order 3 fixes either 1 or 4 points. In what follows, when the automorphism fixes 1 point we denote it by α, when it fixes 4 points by β. Unfortunately these elements α and β are not the α, β used in [12]. We have chosen to present Designs 1 to 8 in exactly the same form and order as in [12]. To alleviate notational problems in this paper we denote by $\hat{\alpha}$, $\hat{\beta}$ the automorphisms α, β in [11]. Thus Design 1 has automorphism

$$\hat{\alpha}\hat{\beta} = (1\,5\,9)(2\,6\,7)(3\,4\,8)(10\,14\,18)(11\,15\,16)(12\,13\,17)(19\,20\,21)(22\,23\,24)(25)$$

which is conjugate to α in our present work. An isomorphic copy of Design 1 arises from *Case A* and has the fixed blocks $\{1, 5, 9, 25\}$, $\{2, 6, 7, 25\}, \ldots, \{22, 23, 24, 25\}$ in our presentation.

First we consider the automorphism

$$\alpha = (1\,2\,3)(4\,5\,6)(7\,8\,9)(10\,11\,12)(13\,14\,15)(16\,17\,18)(19\,20\,21)(22\,23\,24)(25).$$

Let $X_1 = \{1, 2, 3\}$, $X_2 = \{4, 5, 6\}, \ldots, X_8 = \{22, 23, 24\}$ be the point-orbits of X determined by the 3-cycles in α. Let O_j be an orbit of blocks in B. Then, $|O_j| = 1$, or 3. Note that $|O_j| = 1$ if and only if $O_j = \{X_i \cup \{25\}\}$ for some $i \in \{1, 2, \ldots, 8\}$. Our basic strategy is to construct all possible tactical decompositions corresponding to α and then determine whether any of these tactical decompositions leads to an $S(2, 4, 25)$. In general, when we display T_σ we will omit the rows and columns corresponding to fixed points and fixed blocks.

Now, any element of X appears exactly 8 times amongst the blocks B so that α must fix 8, 5, or 2 blocks. This yields three cases to be considered.

Case A. α fixes 8 blocks.

Clearly a tactical decomposition T_α has 8 columns with entries a single 3 and seven 0's. The remaining portion of T_α is an 8 by 14 matrix of 0's and 1's with row sums of 7, column sums of 4 and since each pair from X appears exactly once among the blocks of B, the inner products of distinct rows of T_α are all 3. Hence, the tactical decompositions in this case correspond to $2-(8, 4, 3)$ designs. There are exactly 4 such nonisomorphic designs which we label A_1, A_2, A_3, A_4. In *Table 1* we list A_3 and A_4 since $S(2, 4, 25)$'s arise only from these cases.

Case B. α fixes 5 blocks.

We can assume that the 5 fixed blocks are $X_i \cup \{25\}$, $4 \leq i \leq 8$ and that the remaining orbit of blocks containing the point 25 is generated by the block $\{1, 4, 7, 25\}$. The remaining 14 columns of our tactical decomposition consists of 3 columns with one 2 in rows 1, 2, 3 respectively and 11 columns with exactly four 1's. In *Table 1* we present the 8 by 15 portion of some tactical decompositions corresponding to the orbits of length 3. Note that inner products between distinct rows must again all be equal to 3. There are 8 nonisomorphic tactical

Table 1
Some Tactical Decompositions for Automorphisms α and β of Order 3

A_3	C_7	C_{57}	D_1	E_7
00000001111111	0000000001111111	0000000001111111	00000001111111	000101010001111
00011110000111	0000011110000111	0000011110000111	00011110000111	100001100110011
11100010001011	1000100120111000	1000100120111000	01100110011001	100110001010101
01101100110001	1001101102000001	1002001101001001	10001111101000	101010010201100
10110101010010	1011011000002010	1020011000011010	10110010110010	011001011021000
11010100101100	0101111000020100	0101210000010011	11011000011100	011010101000120
10101011100100	0111010100200001	0110101012000100	11100101000110	010100101101001
01011011011000	0120100011000110	0111010100200100		
A_4	C_{20}	C_{81}	D_2	
00000001111111	0000000001111111	0000000001111111	00000001111111	
00011110000111	0000011110000111	0000011110000111	00011110000111	
01100110011001	1000100120111000	1000200110011001	11100010001011	
01111001100001	1001102001001001	1002001010101010	00101110111000	
10101010101010	1010120001010010	1020001101001100	01110011010100	
10110101010010	0102010100110001	0101110102000010	10110101100010	
11001101001100	0111100011000200	0110111000200001	11011000101100	
11010010110100	0120001100101010	0111010010020100		
B_1	C_{31}	C_{84}	E_3	
100000000111112	0000000001111111	0000000001111111	000101010001111	
100001112000110	0000011110000111	0000011110000111	100100100110011	
100120110011000	1000100120111000	1000200110011001	100010011010101	
001101010101010	1001102001001001	1002001010101010	101001101012000	
010101100110100	1020011000110010	1020010011001100	011001010210100	
011010001101100	0101020101011000	0101110102000010	011010101000120	
011011100000011	0110200101000110	0110111000200001	010110001101001	
011100011010001	0112000010100101	0111001100020100		
B_2	C_{48}	C_{88}	E_4	
100000000111112	0000000001111111	0000000001111111	000101010001111	
100001112000110	0000011110000111	0000011110000111	100001100110011	
100120110011000	1000100120111000	1000200110011001	100110001010101	
001101010101010	1002001101001001	1002001010101010	101010010112000	
010111001100001	1011110000010020	1020010011010010	011010100100210	
011000101111000	0100112001110000	0101120001001100	011001012100001	
011011000010110	0111100100100200	0110102001100001	010100101011010	
011100110000101	0120010011001001	0111000200110100		
B_6	C_{54}	C_{91}	E_6	
100000000111112	0000000001111111	0000000001111111	000101010001111	
100001112000110	0000011110000111	0000011110000111	100100100110011	
101120010001010	1000100120111000	1001100020011001	100010011010101	
001101100110010	1002001101001001	1010100200101010	101001011201000	
010010110110100	1020010101010010	1011002001001100	010110101012000	
010101110001001	0101120000110001	0101110102000001	011010100100210	
011011001010001	0110102000101010	0110111000020010	011001001010011	
011100001101100	0111100011000200	0111010010200100		

decompositions but we list only B_1, B_2, and B_6 because only these give rise to designs.

Case C. α fixes 2 blocks.

Here we can assume that the fixed blocks are $\{1, 2, 3, 25\}$, $\{4, 5, 6, 25\}$ and that the design contains the orbits generated by $\{7, 10, 13, 25\}$ and $\{16, 19, 22, 25\}$. It easily follows that the tactical decompositions have a single 2 in each of rows 3, 4, 6, 7, 8. In *Table 1* we list 10 out of a total number of 91 tactical decompositions again presenting only the 8 by 16 portion related to the orbits of length 3.

We now consider the automorphism

$$\beta = (1\,2\,3)(4\,5\,6)(7\,8\,9)(10\,11\,12)(13\,14\,15)(16\,17\,18)(19\,20\,21)(22)(23)(24)(25),$$

fixing 4 points of X. Let $X_1 = \{1, 2, 3\}, \ldots, X_7 = \{19, 20, 21\}$. Since each point appears in exactly 8 blocks it is clear that the number of fixed blocks through each of 22, 23, 24, or 25 must be congruent to 2 modulo 3. It is easily seen that we must consider exactly two cases.

Case D. β fixes 8 blocks.

Since the blocks fixed by β are unions of point-orbits of the group $\langle\beta\rangle$, it is clear that the fixed blocks are $\{22,23,24,25\}$, $\{19,20,21,25\}$, $\{16,17,18,25\}$, $\{13,14,15,25\}$, $\{10,11,12,25\}$, $\{7,8,9,24\}$, $\{4,5,6,23\}$, and $\{1,2,3,22\}$. Exactly two tactical decompositions D_1, D_2 arise here and are given in *Table 1*.

Case E. β fixes 5 blocks.

Without loss of generality the five fixed blocks can be chosen to be $\{22,23,24,25\}$, $\{19,20,21,25\}$, $\{7,8,9,24\}$, $\{4,5,6,23\}$, $\{1,2,3,22\}$. Exactly 9 tactical decompositions arise in this case. In *Table 1* we list the four tactical decompositions E_3, E_4, E_6, and E_7 which produce $S(2, 4, 25)$'s.

Table 2

Some Tactical Decompositions for Automorphisms γ and δ of Order 2

A_{21}	B_1	C_1	D_{11}
100000000000000111111	100000000000000111111	100000000000000111111	0000000000001111111
100000000011111000001	100000000011111000001	100000000011111000001	0000000011111000011
100000011110000100010	100000011110000100010	100000011110000100010	0000011100011000 1100
010000100010001100110 0	010000000110011000110 0	010000000110011000110 0	0000101101100011 0000
010001000010110001001 0	010000101000001111000 0	001000001010101011000 0	1001000110001101 0000
010010001100001001000 1	010000110001100000011 0	000100011001010001010 0	1001110000100000 0101
001001110100011000000 0	001001101010110000000 0	010001101101100000000 0	1010010001010110 0000
001011001010000010010 0	001010110100000000110 00	001010110100000001001 00	0101011010000010 0010
001010100001100000110 00	000111000000101001010 0	000111000001001010100 0	0110101000001100 0001
000110000101010010001 0	001011000001000110001 0	000110100000100101001 0	0111000000110001 1000
000100111001000000010 1	000101010011000000100 1	010011010000010000011	
000101010000100110100 0	000110001100010010000 1	0010011000100001001001	

D_{19}	D_{21}	E_1
0000000000001111111	0000000000001111111	000000010010010001111
0000000011111000011	0000000011111000011	000010000100100110011
0000011100011000 1100	0000011100011000 1100	000100100001001010101
0000101101100011 0000	0000101101100011 0000	001001001000001101001
1001000110001101 0000	1001000110001101 0000	100100010010101100000
1001110000100000 0101	1001110000100000 0101	100011000100011000100
1010011001000100 0010	1010011001000100 0010	101000010101000011000
0101010011000010 1000	0101100001010100 1000	010010101000010011000
0110100110000000 0110	0110100110000000 0110	011000100011000100010
0111001000010001 0001	0111001000001010 0001	010101001000100000110

Table 3					
S(2,4,25)'s and the Tactical Decompositions from which they arise					
		$\lvert\alpha\rvert = \lvert\beta\rvert = 3$		$\lvert\gamma\rvert = \lvert\delta\rvert = 2$	
Design No.	$\lvert G\rvert$	α	β	γ	δ
1	504	A_4, C_{91}	E_4	A_{21}	
2	63	A_3, C_{84}	E_3, E_7		
3	9	B_2, C_{84}	D_2, E_3		
4	9	B_1, C_{84}	D_2, E_7		
5	9	B_6, C_{81}	D_1, E_4		
6	150	C_{20}			D_{19}
7	21		E_6		
8	6	C_{54}			D_{21}
9	3	C_7			
10	3	C_{31}			
11	3	C_{48}			
12	3	C_{57}			
13	3	C_{88}			
14	3	C_{88}			
15	3		E_6		
16	3		E_6		

4. Solutions to tactical decompositions

Consider the tactical decomposition A_4. In order for A_4 to actually give rise to an $S(2, 4, 25)$ for each column j of A_4 we need to select elements of a block B so that $|B \cap X_i| = t_{ij}$, $1 \leq i \leq 8$. Each such choice for $1 \leq j \leq 14$ will generate orbits O_j, $1 \leq j \leq 14$. Furthermore, for the $S(2, 4, 25)$ to exist each pair from X must be covered exactly once. A fairly fast algorithm run on a Mac+ microcomputer took about 1 minute to find all solutions for a given tactical decomposition.

A fast graph-isomorphism program, written by Brendan McKay was used to sift isomorphic designs. The public domain program, written in C, computes, among other invariants, generators for the automorphism group of the graph, a canonical form for the graph, and a *hash code* for this canonical form. Given a design $D = (X, B)$ we construct a graph with vertex set $X \cup B$ where $v_1, v_2 \in X \cup B$ are adjacent if $v_1 \in X$, $v_2 \in B$ and v_1 is incident with v_2. Clearly two designs D_1, D_2 are isomorphic if and only if their graphs are isomorphic and this can be checked by means of the hash codes computed for the graphs. A similar algorithm is used to sift out isomorphic tactical decompositions. In many cases there are no solutions and in some cases more than one nonisomorphic design arises from a single tactical decomposition. For the $S(2, 4, 25)$'s with an automorphism group of order 9, since conjugates of both α and β are present in the elementary abelian G, the $S(2, 4, 25)$'s naturally arise from more than one tactical decomposition.

Occurrences of solutions are listed in *Table 3*. Note that all eight previously known $S(2, 4, 25)$'s were rediscovered along with the 8 new $S(2, 4, 25)$'s with

Table 4
The S(2,4,25)'s with $|G| > 3$

Design 1	Design 2	Design 3	Design 4	Design 5	Design 6	Design 7	Design 8
1 2 3 19	1 2 3 19	1 2 3 19	1 2 3 19	1 2 3 19	1 2 6 25	1 2 4 14	1 2 4 25
1 4 10 11	1 4 7 22	1 4 7 22	1 4 7 22	1 4 10 15	1 3 11 19	1 3 7 13	1 3 8 11
1 5 9 25	1 5 9 25	1 5 9 25	1 5 9 25	1 5 9 25	1 4 14 17	1 5 6 11	1 5 9 24
1 6 14 22	1 6 10 11	1 6 10 11	1 6 10 14	1 6 11 22	1 5 10 24	1 8 15 25	1 6 7 15
1 7 16 17	1 8 17 18	1 8 17 18	1 8 12 17	1 7 12 16	1 7 8 12	1 9 17 22	1 10 13 17
1 8 12 23	1 12 14 24	1 12 13 23	1 11 13 21	1 8 18 23	1 9 16 18	1 10 19 23	1 12 19 21
1 13 18 20	1 13 16 20	1 14 16 20	1 15 20 24	1 13 17 20	1 13 15 23	1 12 16 24	1 14 18 22
1 15 21 24	1 15 21 23	1 15 21 24	1 16 18 23	1 14 21 24	1 20 21 22	1 18 20 21	1 16 20 23
2 4 15 23	2 4 11 12	2 4 11 12	2 4 11 15	2 4 12 23	2 3 7 21	2 3 5 8	2 3 14 19
2 5 11 12	2 5 8 23	2 5 8 23	2 5 8 23	2 5 11 13	2 4 12 20	2 6 7 12	2 5 8 16
2 6 7 25	2 6 7 25	2 6 7 25	2 6 7 25	2 6 7 25	2 5 15 18	2 9 16 25	2 6 9 12
2 8 17 18	2 9 16 18	2 9 16 18	2 9 10 18	2 8 10 17	2 8 9 13	2 10 18 22	2 7 18 23
2 9 10 24	2 10 15 22	2 10 14 24	2 12 14 21	2 9 16 24	2 10 17 19	2 11 20 23	2 10 11 22
2 13 21 22	2 13 21 24	2 13 21 22	2 13 20 22	2 14 18 20	2 11 14 24	2 13 17 24	2 13 15 20
2 14 16 20	2 14 17 20	2 15 17 20	2 16 17 24	2 15 21 22	2 16 22 23	2 15 19 21	2 17 21 24
3 4 8 25	3 4 8 25	3 4 8 25	3 4 8 25	3 4 8 25	3 4 8 22	3 4 6 9	3 4 10 15
3 5 13 24	3 5 10 12	3 5 10 12	3 5 12 13	3 5 10 24	3 5 13 16	3 10 17 25	3 5 7 13
3 6 10 12	3 6 9 24	3 6 9 24	3 6 9 24	3 6 12 14	3 6 18 20	3 11 19 22	3 6 21 25
3 7 11 22	3 7 16 17	3 7 16 17	3 7 11 16	3 7 17 22	3 9 10 14	3 12 21 23	3 9 16 22
3 9 16 18	3 11 13 23	3 11 15 22	3 10 15 21	3 9 11 18	3 12 15 25	3 14 18 24	3 12 17 23
3 14 21 23	3 14 21 22	3 13 18 20	3 14 20 23	3 13 21 23	3 17 23 24	3 15 16 20	3 18 20 24
3 15 17 20	3 15 18 20	3 14 21 23	3 17 18 22	3 15 16 20	4 5 9 23	4 5 7 10	4 5 11 20
4 5 6 20	4 5 6 20	4 5 6 20	4 5 6 20	4 5 6 20	4 6 10 15	4 8 19 24	4 6 8 14
4 7 13 14	4 9 13 14	4 9 13 14	4 9 13 17	4 7 13 18	4 7 16 19	4 11 18 25	4 7 16 21
4 9 17 22	4 10 16 21	4 10 17 21	4 10 12 23	4 9 14 22	4 11 13 21	4 12 20 22	4 9 17 18
4 12 16 21	4 15 17 24	4 15 16 23	4 14 16 19	4 11 16 21	4 18 24 25	4 13 15 23	4 12 13 24
4 18 19 24	4 18 19 23	4 18 19 24	4 18 21 24	4 17 19 24	5 6 7 11	4 16 17 21	4 19 22 23
5 7 18 23	5 7 14 15	5 7 14 15	5 7 14 18	5 7 15 23	5 8 17 20	5 9 20 24	5 6 17 22
5 8 14 15	5 11 17 21	5 11 18 21	5 10 11 24	5 8 14 16	5 12 14 22	5 12 19 25	5 10 21 23
5 10 17 21	5 13 18 22	5 13 17 24	5 15 17 19	5 12 17 21	5 19 21 25	5 13 21 22	5 12 14 15
5 16 19 22	5 16 19 24	5 16 19 22	5 16 21 22	5 18 19 22	6 8 16 24	5 14 16 23	5 18 19 25
6 8 16 24	6 8 13 15	6 8 13 15	6 8 15 16	6 8 13 24	6 9 19 22	5 15 17 18	6 10 19 20
6 9 13 15	6 12 18 21	6 12 16 21	6 11 12 22	6 9 15 17	6 12 13 17	6 8 17 23	6 11 23 24
6 11 18 21	6 14 16 23	6 14 18 22	6 13 18 19	6 10 18 21	6 14 21 23	6 10 21 24	6 13 16 18
6 17 19 23	6 17 19 22	6 17 19 23	6 17 21 23	6 16 19 23	7 9 17 25	6 13 20 25	7 8 19 24
7 8 9 21	7 8 9 21	7 8 9 21	7 8 9 21	7 8 9 21	7 10 20 23	6 14 15 22	7 9 10 25
7 10 15 19	7 10 13 19	7 10 18 23	7 10 17 20	7 10 14 19	7 13 14 18	6 16 18 19	7 11 14 17
7 12 20 24	7 11 18 24	7 11 13 19	7 12 19 24	7 11 20 24	7 15 22 24	7 8 16 22	7 12 20 22
8 10 20 22	7 12 20 23	7 12 20 24	7 13 15 23	8 11 15 19	8 10 18 21	7 9 18 23	8 9 15 23
8 11 13 19	8 10 20 24	8 10 20 22	8 10 19 22	8 12 20 22	8 11 23 25	7 11 15 24	8 10 12 18
9 11 20 23	8 11 14 19	8 11 16 24	8 11 18 20	9 10 20 23	8 14 15 19	7 14 21 25	8 13 21 22
9 12 14 19	8 12 16 22	8 12 14 19	8 13 14 24	9 12 13 19	9 11 15 20	7 17 19 20	8 17 20 25
10 13 16 23	9 10 17 23	9 10 15 19	9 11 19 23	10 11 12 25	9 12 21 24	8 9 11 21	9 11 13 19
10 14 18 25	9 11 20 22	9 11 20 23	9 12 16 20	10 13 16 22	10 11 12 16	8 10 14 20	9 14 20 21
11 14 17 24	9 12 15 19	9 12 17 22	9 14 15 22	11 14 17 23	10 13 22 25	8 12 13 18	10 14 16 24
11 15 16 25	10 14 18 25	10 13 16 25	10 13 16 25	12 15 18 24	11 17 18 22	9 10 12 15	11 12 16 25
12 13 17 25	11 15 16 25	11 14 17 25	11 14 17 25	13 14 15 25	12 18 19 23	9 13 14 19	11 15 18 21
12 15 18 22	12 13 17 25	12 15 18 25	12 15 18 25	16 17 18 25	13 19 20 24	10 11 13 16	13 14 23 25
19 20 21 25	19 20 21 25	19 20 21 25	19 20 21 25	19 20 21 25	14 16 20 25	11 12 14 17	15 16 17 19
22 23 24 25	22 23 24 25	22 23 24 25	22 23 24 25	22 23 24 25	15 16 17 21	22 23 24 25	15 22 24 25

automorphism group of order exactly 3. All 16 designs are listed in *Tables 4* and *5*.

5. Automorphisms of order 2 and their tactical decompositions

From Theorem 2.2 an automorphism of order 2 fixes 1 or 5 points. First consider the automorphism fixing a single point:

$$\gamma = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)(11\ 12)(13\ 14)(15\ 16)(17\ 18)(19\ 20)(21\ 22)(23\ 24)(25).$$

Table 5
The S(2,4,25)'s with $|G| = 3$

Design 9	Design 10	Design 11	Design 12	Design 13	Design 14	Design 15	Design 16
1 2 3 25	1 2 3 25	1 2 3 25	1 2 3 25	1 2 3 25	1 2 3 25	1 2 3 22	1 2 3 22
1 4 16 24	1 4 20 24	1 4 19 20	1 4 20 22	1 4 16 23	1 4 18 23	1 4 13 24	1 4 13 24
1 5 12 21	1 5 11 23	1 5 11 23	1 5 10 18	1 5 7 21	1 5 7 19	1 5 17 21	1 5 16 20
1 6 13 22	1 6 14 21	1 6 13 14	1 6 15 17	1 6 12 14	1 6 12 14	1 6 8 20	1 6 8 19
1 7 14 15	1 7 15 17	1 7 15 18	1 7 12 14	1 8 10 18	1 8 15 24	1 7 11 25	1 7 17 18
1 8 17 18	1 8 12 16	1 8 10 24	1 8 13 16	1 9 13 22	1 9 11 16	1 9 16 18	1 9 10 25
1 9 19 20	1 9 13 22	1 9 16 21	1 9 23 24	1 11 20 24	1 10 20 22	1 10 14 15	1 11 14 15
1 10 11 23	1 10 18 19	1 12 17 22	1 11 19 21	1 15 17 19	1 13 17 21	1 12 19 23	1 12 21 23
2 4 14 23	2 4 15 19	2 4 14 15	2 4 13 18	2 4 10 15	2 4 10 15	2 4 9 21	2 4 9 20
2 5 17 22	2 5 21 22	2 5 20 21	2 5 21 23	2 5 17 24	2 5 16 24	2 5 14 24	2 5 14 24
2 6 10 19	2 6 12 24	2 6 12 24	2 6 11 16	2 6 8 19	2 6 8 20	2 6 18 19	2 6 17 21
2 7 20 21	2 7 14 23	2 7 17 19	2 7 22 24	2 7 14 23	2 7 12 17	2 7 16 17	2 7 11 25
2 8 13 15	2 8 13 18	2 8 13 16	2 8 10 15	2 9 11 16	2 9 13 22	2 8 12 25	2 8 16 18
2 9 16 18	2 9 10 17	2 9 11 22	2 9 14 17	2 12 21 22	2 11 21 23	2 10 20 23	2 10 19 23
2 11 12 24	2 11 16 20	2 10 18 23	2 12 19 20	2 13 18 20	2 14 18 19	2 11 13 15	2 12 13 15
3 4 11 20	3 4 10 22	3 4 10 22	3 4 12 17	3 4 9 20	3 4 9 21	3 4 16 20	3 4 18 19
3 5 15 24	3 5 13 20	3 5 13 15	3 5 14 16	3 5 11 13	3 5 11 13	3 5 7 19	3 5 7 21
3 6 18 23	3 6 19 23	3 6 19 21	3 6 19 24	3 6 18 22	3 6 17 22	3 6 15 24	3 6 15 24
3 7 16 17	3 7 11 18	3 7 12 23	3 7 15 18	3 7 12 17	3 7 14 23	3 8 17 18	3 8 12 25
3 8 19 21	3 8 15 24	3 8 18 20	3 8 22 23	3 8 15 24	3 8 10 18	3 9 10 25	3 9 16 17
3 9 13 14	3 9 14 16	3 9 14 17	3 9 11 13	3 10 19 23	3 12 19 24	3 11 21 23	3 10 13 14
3 10 12 22	3 12 17 21	3 11 16 24	3 10 20 21	3 14 16 21	3 15 16 20	3 12 13 14	3 11 20 23
4 5 6 25	4 5 6 25	4 5 6 25	4 5 6 25	4 5 6 25	4 5 6 25	4 5 6 23	4 5 6 23
4 7 12 19	4 7 16 21	4 7 11 21	4 7 11 23	4 7 22 24	4 7 22 24	4 7 10 22	4 7 10 22
4 8 9 22	4 8 9 23	4 8 9 23	4 8 9 21	4 8 12 13	4 8 12 13	4 8 15 19	4 8 14 21
4 10 15 18	4 11 12 13	4 12 16 18	4 10 14 19	4 11 19 21	4 11 19 20	4 11 12 17	4 11 12 16
4 13 17 21	4 14 17 18	4 13 17 24	4 15 16 24	4 14 17 18	4 14 16 17	4 14 18 25	4 15 17 25
5 7 9 23	5 7 9 24	5 7 9 24	5 7 9 19	5 8 22 23	5 8 22 23	5 8 11 22	5 8 11 22
5 8 10 20	5 8 17 19	5 8 12 19	5 8 12 24	5 9 10 14	5 9 10 14	5 9 13 20	5 9 15 19
5 11 13 16	5 10 12 14	5 10 16 17	5 11 15 20	5 12 19 20	5 12 20 21	5 10 12 18	5 10 12 17
5 14 18 19	5 15 16 18	5 14 18 22	5 13 17 22	5 15 16 18	5 15 17 18	5 15 16 25	5 13 18 25
6 7 8 24	6 7 8 22	6 7 8 22	6 7 8 20	6 7 11 15	6 7 11 15	6 7 14 21	6 7 13 20
6 9 11 21	6 9 18 20	6 9 10 20	6 9 10 22	6 9 23 24	6 9 23 24	6 9 12 22	6 9 12 22
6 12 14 17	6 10 11 15	6 11 17 18	6 12 13 21	6 10 20 21	6 10 19 21	6 10 11 16	6 10 11 18
6 15 16 20	6 13 16 17	6 15 16 23	6 14 18 23	6 13 16 17	6 13 16 18	6 13 17 25	6 14 16 25
7 10 13 25	7 10 13 25	7 10 13 25	7 10 13 25	7 8 16 20	7 8 16 21	7 8 9 24	7 8 9 24
7 11 18 22	7 12 19 20	7 14 16 20	7 16 17 21	7 9 18 19	7 9 18 20	7 12 15 20	7 12 14 19
8 11 14 25	8 10 20 21	8 11 14 25	8 11 14 25	7 10 13 25	7 10 13 25	7 13 18 23	7 15 16 23
8 12 16 23	8 11 14 25	8 15 17 21	8 17 18 19	8 9 17 21	8 9 17 19	8 10 13 21	8 10 15 20
9 10 17 24	9 11 19 21	9 12 15 25	9 12 15 25	8 11 14 25	8 11 14 25	8 14 16 23	8 13 17 23
9 12 15 25	9 12 15 25	9 13 18 19	9 16 18 20	9 12 15 25	9 12 15 25	9 11 14 19	9 11 13 21
10 14 16 21	10 16 23 24	10 11 15 19	10 11 17 24	10 11 17 22	10 11 17 24	9 15 17 23	9 14 18 23
11 15 17 19	11 17 22 24	10 12 14 21	10 12 16 23	10 12 16 24	10 12 16 23	10 17 19 24	10 16 21 24
12 13 18 20	12 18 22 23	11 12 13 20	11 12 18 22	11 12 18 23	11 12 18 22	11 18 20 24	11 17 19 24
13 19 23 24	13 14 19 24	13 21 22 23	13 14 20 24	13 14 19 24	13 14 20 24	12 16 21 24	12 18 20 24
14 20 22 24	13 15 21 23	14 19 23 24	13 15 19 23	13 15 21 23	13 15 19 23	13 16 19 22	13 16 19 22
15 21 22 23	14 15 20 22	15 20 22 24	14 15 21 22	14 15 20 22	14 15 21 22	14 17 20 22	14 17 20 22
16 19 22 25	16 19 22 25	16 19 22 25	16 19 22 25	16 19 22 25	16 19 22 25	15 18 21 22	15 18 21 22
17 20 23 25	17 20 23 25	17 20 23 25	17 20 23 25	17 20 23 25	17 20 23 25	19 20 21 25	19 20 21 25
18 21 24 25	18 21 24 25	18 21 24 25	18 21 24 25	18 21 24 25	18 21 24 25	22 23 24 25	22 23 24 25

Up to relabeling we can assume that the fixed blocks are: $\{1,2,13,14\}$, $\{3,4,15,16\}$, $\{5,6,17,18\}$, $\{7,8,19,20\}$, $\{9,10,21,22\}$, $\{11,12,23,24\}$. We distinguish three cases regarding the way γ relates to the blocks containing the point 25.

Case A.

Our design has the blocks $\{1,3,5,25\}$, $\{7,9,11,25\}$, $\{13,15,17,25\}$, and $\{19,21,23,25\}$. In this case there arise 21 tactical decompositions but only A_{21}

produces a design, namely the $S(2, 4, 25)$ with automorphism group of order 504 (see *Table 2*).

Case B.

Here B contains $\{1,3,5,25\}$, $\{7,9,11,25\}$, $\{13,15,19,25\}$, and $\{17,21,23,25\}$. There are 19 tactical decompositions here but none leads to an $S(2, 4, 25)$ with automorphism γ. Even though no designs arise here *Table 2* lists tactical decomposition B_1 as an example of this case.

Case C.

In this case B contains $\{1,3,5,25\}$, $\{7,13,21,25\}$, $\{9,15,23,25\}$, and $\{11,17,19,25\}$. There are 25 tactical decompositions here but none of these gives rise to an $S(2, 4, 25)$ with automorphism γ. *Table 2* lists C_1 as an example of a tactical decomposition for Case C.

Now consider the automorphism:

$$\delta = (1\ 2)(3\ 4)(5\ 6)(7\ 8)(9\ 10)(11\ 12)(13\ 14)(15\ 16)(17\ 18)(19\ 20)(21)(22)(23)(24)(25).$$

There are two cases for δ related to the way the fixed points $\{21,22,23,24,25\}$ are distributed among the fixed blocks as follows:

Case D.

In this case our design has the fixed blocks $\{21,22,1,2\}$, $\{21,23,3,4\}$, $\{21,24,5,6\}$, $\{21,25,7,8\}$, $\{22,23,9,10\}$, $\{22,24,11,12\}$, $\{22,25,13,14\}$, $\{23,24,15,16\}$, $\{23,25,17,18\}$, and $\{24,25,19,20\}$. In other words, the fixed points of δ form an arc (see Section 7). There are 45 tactical decompositons here with designs arising from D_{19}, and D_{21} with groups of orders 150 and 6 respectively.

Interestingly enough, in cases D_{11}, D_{32}, D_{41}, and D_{45} there are partial solutions to the tactical decompositions which yield each time 20 blocks of size 3 and 20 of size 4. We have checked however that there is no way of completing these partial designs to $S(2, 4, 25)$'s by adding 5 points and 10 blocks.

Case E.

In this case our design has as fixed blocks $\{21,22,23,24\}$, $\{21,25,1,2\}$, $\{22,25,3,4\}$, $\{23,25,5,6\}$ and $\{24,25,7,8\}$, i.e. four out of the five fixed points lie on a block. There arise 3 tactical decompositions here, but none leads to an $S(2, 4, 25)$. We list E_1 in *Table 2* as an example of this case.

6. Transformation of designs

Given an $S(2, 4, 25)$ it is sometimes possible to obtain a non-isomorphic system with the same parameters by transforming a selected subset of blocks. In order to describe such a transformation we require some definitions.

Let $\mathrm{B} \in B$ be a block of an $S(2, 4, 25)$ system (X, B) and denote by S_{B} all blocks in B which have no point in common with B. Note that S_{B} is a symmetric configuration (1-design) with $v = b = 21$ and $k = r = 4$. We associate with S_{B} a *graph* G_{B} as follows. The vertices of G_{B} are the points of S_{B}, two vertices are adjacent if the corresponding points are not collinear in S_{B} (do not appear in the same block). Clearly G_{B} has 21 vertices and is regular of valency 8. We say that G_{B} has a *triangulation* T if the 84 edges of G_{B} can be partitioned into 28 triangles. T is called *resolvable* if its triangles can be partitioned into 4 parallel classes each of 7 disjoint triangles. A resolution of T will be denoted by T_R. Suppose that for some S_{B} we know a resolution T_R of G_{B}. Then adding a new point x_i to every triangle in the ith parallel class, $i = 1, \ldots, 4$, we obtain 28 blocks of size 4 on 25 points. Adding a new block $\{x_1, x_2, x_3, x_4\}$ and the blocks in S_{B} we obtain an $S(2, 4, 25)$. Since S_{B} is symmetric we can consider its dual S_{B}^d and the corresponding G_{B}^d and repeat the procedure.

We are now in a position to describe the *transformations* T_{B} and T_{B}^d of a design (X, B) with respect to a block $\mathrm{B} \in B$.

T_{B}: Find all resolutions T_R of G_{B} and complete each to a system.

T_{B}^d: Find all resolutions T_R of G_{B}^d and complete each to a system.

We note that T_{B} and T_{B}^d, $\mathrm{B} \in B$, generate sets Σ_{B}, Σ_{B}^d of system $S(2, 4, 25)$. From the construction it follows that $|\Sigma_{\mathrm{B}}| \geq 1$, since Σ_{B} always contains the original system (X, B).

We have applied the transformations T_{B}, T_{B}^d to all 16 systems with non-trivial

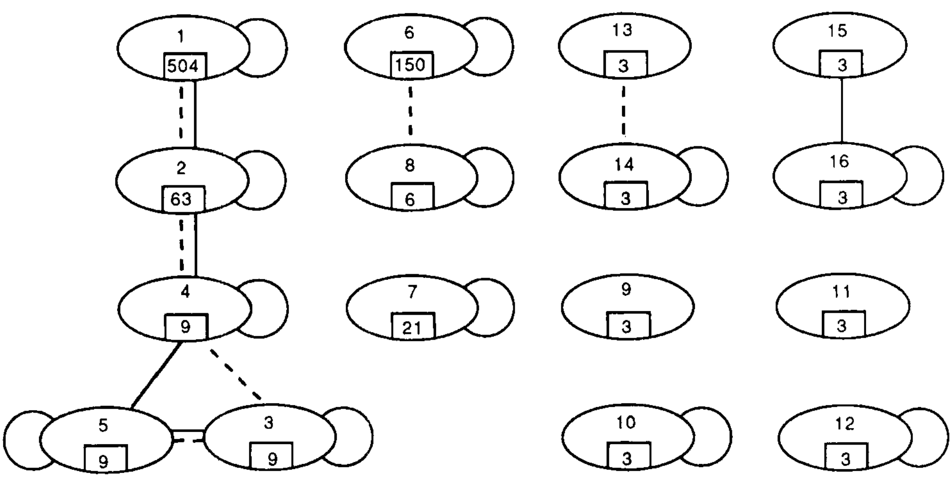


Fig. 1.

automorphism groups. For each design we consider a representative from every orbit of blocks. The results are summarized in the transformation graph of Fig. 1. Two designs are connected by a line (broken line) if one can be obtained from the other by T_B^d (T_B) for some $B \in B$. The graph has 9 connected components, each representing an equivalence class of designs under the transformations T_B, T_B^d.

The transformation T_B has been used by Petrenyuk [16, 17] to obtain from the previously known designs 1, 2, 6 and 7, in our numbering, the designs 3, 4, 5 and 8. The same approach in a different setting has been applied by Gropp [8] to obtain Design No. 3, with a group of order 9. He also traces the origins of transformations based on symmetric configurations to the nineteenth century Italian geometers.

7. Subdesigns, parallel classes and near-resolutions

In this section we investigate the possible embedding of subdesigns in our $S(2, 4, 25)$ systems. A subdesign is understood to be a substructure in the usual sense. Thus, an $S(2, l, w)$ system (Y, D) is a *subdesign* of an $S(2, k, v)$ system (X, B), if $Y \subset X$, and each $D \in D$ is contained in a block $B \in B$. Points of Y are called *interior*, while those of $X - Y$ *exterior*. We let $b = |B|$, $r = bk/v$ and denote by B_i the collection of all blocks of (X, B) which intersect Y in exactly i points. Easy counting yields the following

Lemma 7.1. *Suppose that (Y, D) is an $S(2, l, w)$ subdesign of an $S(2, k, v)$ design (X, B). Let u_i be the number of blocks on an exterior point which intersect Y in i points, v_i the number of blocks on an interior point which intersect Y in i points, and let $t_i = |B_i|$, then*

$$t_0 + t_1 + t_l = b, \quad t_1 + l \cdot t_l = rw, \quad l(l-1) \cdot t_l = w(w-1),$$
$$u_0 + u_1 + u_l = r, \quad u_1 + l \cdot u_l = w, \quad v_1 + v_l = r, \quad \textit{and} \quad (l-1)v_l = w - 1.$$

Proposition 7.2. *If (Y, D) is an $S(2, l, w)$ subdesign of an $S(2, 4, 25)$ and if $l \geq 3$ then (Y, D) is a Fano plane $S(2, 3, 7)$.*

Proof. Suppose that (Y, D) is an $S(2, l, w)$ subsystem occurring in an $S(2, 4, 25)$ system (X, B). In the case where $l = k = 4$ an inequality of Wilson's requires that $w \leq r = 8$. This rules out the possibility of non-trivial subsystems $S(2, 4, w)$ in an $S(2, 4, 25)$. When $l = 3$ we have that $t_0 + t_1 + t_3 = 50$, $t_1 + 3t_3 = 8w$, and $6t_3 = w(w-1)$. Thus, $t_1 \geq 0$ implies that $w \leq 17$ and since $w \in \{7, 9, 13, 15, 21\}$, we have that $w \leq 15$. On the other hand, $t_0 \geq 0$ implies $w \leq 9$ or $w \geq 15$. Case $w = 15$ is ruled out by de Resmini [6], Proposition 4. Alternatively, the existence of a subsystem $S(2, 3, 15)$ would imply $u_0 = 0$, $u_1 + u_3 = 8$, and $u_1 + 3u_3 = 15$. Hence, $2u_3 = 7$, a contradiction. If $w = 9$, then $t_0 = 2$, $t_1 = 36$, and $t_3 = 12$. From Lemma

7.1 we get $(u_1 + 3u_3) - (u_0 + u_1 + u_3) = 1$, that is $2u_3 = 1 + u_0$. Therefore, since $u_0 \leq t_0 = 2$, we have that $u_0 = u_3 = 1$, that is, through each exterior point there is one block of B_0. This is a contradiction since there are altogether $t_0 = 2$ exterior blocks covering 7 or 8 points of $X - Y$, while $|X - Y| = 25 - 9 = 16$. □

There remains to investigate whether $S(2, 3, 7)$ systems occur in our 16 $S(2, 4, 25)$ designs. A complete search through each of the 16 designs establishes that embedded Fano planes are found in eleven out of the sixteen. We acknowledge J. DiPaola for bringing to our attention the existence of some embedded Fano planes. The number of Fano planes in each of the 16 designs is given in *Table 7*, together with other structural information. These Fano planes break up into orbits under the action of the automorphism group of each design. The number of orbits, orbit representatives and orbit lengths is presented in Section 8.

It is of interest to investigate further the existence of certain subdesigns with $l = 2$. By an *s-arc*, or simply an *arc*, we mean a collection Y of s points of X no three of which are collinear in (X, B). An arc can then be viewed as a subdesign (Y, D) of (X, B) where D is the collection of all pairs of Y. An arc Y is called *complete* if no point of $X - Y$ can be adjoined to Y to obtain a larger arc. A block B of (X, B) is a *secant* (*tangent*) of arc Y if it intersects Y in two (one) points. Clearly, Y is a complete arc in (X, B) if and only if each point of X lies on at least one secant of Y. An arc of maximum possible size is called an *oval* if there is exactly one tangent to the arc at each of its points; it is called a *hyperoval* if it has no tangents. Any arc of maximum possible size is of course complete. Using Lemma 7.1, it is easy to verify that the size of a complete arc cannot exceed 8, moreover, the same equations imply that any 8-arc might be an oval. Ovals occur in each of our sixteen $S(2, 4, 25)$ designs except for Design 7, and their number is presented in *Table 7*. We present orbit representatives and orbit lengths of ovals in Section 8.

Complete 5-arcs occur in all of our $S(2, 4, 25)$ designs with the exception of Design 10. The number of complete 5-arcs appear in *Table 7*. The number of orbit representatives, orbit lengths and the maximum number of mutually disjoint complete 5-arcs is given in Section 8. It is noteworthy that in the case of Design 6, there are two orbits of complete 5-arcs, one of size 15 and the other of size 75. The 15 arcs in the first orbit are partitioned into three sets of five mutually disjoint complete arcs. These three sets are carried into one another by an automorphism of order 3. One of these sets consists of the arcs $\{1, 2, 3, 4, 5\}$, $\{6, 7, 8, 9, 10\}, \ldots, \{21, 22, 23, 24, 25\}$. We wish to thank Marialuisa de Resmini for bringing this interesting fact to our attention, as well as for other helpful discussions and comments related to this section. In her paper [7] she is interested in the existence of complete 5-arcs embedded in $S(2, 4, 25)$ designs, and this question has been answered here.

Two distinct blocks of a design (X, B) are said to be *parallel* if they are disjoint. The maximal number of mutually parallel blocks in an $S(2, 4, 25)$ is six and such a set of blocks is called a *parallel class*. In *Table 7* we give the number of parallel classes in each of our 16 designs and in Section 8 we display the orbit representatives and orbit lengths for all parallel classes in each of our designs. If we remove a point x together with the eight blocks through x, we say that we have a *near-resolution* if the remaining 42 blocks partition into seven parallel classes. We thank Frank Bennett for suggesting that we look for possible near-resolutions in our designs. Near-resolutions exist only for Design 1, where there are exactly 11 such near-solutions occurring only with the special point 25. These 11 fall into orbits of lengths 1, 7 and 3 under the full automorphism group of the design. In *Table 6* the near-resolution No. 1 constitutes the orbit of length 1; the near-resolution No. 2 is a representative of the orbit of size 7; and the near-resolutions 3, 4, 5 constitute the orbit of size 3.

Two near-resolutions $n_1 = \{P_1, \ldots, P_7\}$, $N_2 = \{Q_1, \ldots, Q_7\}$, where each P_i and Q_j is a parallel class, are said to be *orthogonal* if $|P_i \cap Q_j| \leq 1$ for all i, j. Near-resolutions 3, 4, and 5 are in fact mutually orthogonal. From these three orthogonal near-resolutions one can construct the unique elliptic semiplane on 45

Table 6
Some Near-Resolutions for Design 1

	1	2	3	19	4	5	6	20	7	8	9	21	10	13	16	23	11	14	17	24	12	15	18	22
	2	24	10	9	14	6	22	1	23	18	7	5	20	3	15	17	16	21	4	12	8	11	19	13
	24	12	20	7	21	22	13	2	17	19	23	6	1	10	11	4	15	5	14	8	18	16	9	3
1	12	8	1	23	5	13	3	24	4	9	17	22	2	20	16	14	11	6	21	18	19	15	7	10
	8	18	2	17	6	3	10	12	14	7	4	13	24	1	15	21	16	22	5	19	9	11	23	20
	18	19	24	4	22	10	20	8	21	23	14	3	12	2	11	5	15	13	6	9	7	16	17	1
	19	9	12	14	13	20	1	18	5	17	21	10	8	24	16	6	11	3	22	7	23	15	4	2
	1	2	3	19	4	5	6	20	7	8	9	21	10	13	16	23	11	14	17	24	12	15	18	22
	2	24	10	9	14	6	22	1	23	18	7	5	20	3	15	17	16	21	4	12	8	11	19	13
	24	12	20	7	21	22	13	2	17	19	23	6	1	10	11	4	15	5	14	8	18	16	9	3
2	1	7	16	17	2	4	15	23	3	5	13	24	6	11	18	21	8	10	20	22	9	12	14	19
	8	18	2	17	6	3	10	12	14	7	4	13	24	1	15	21	16	22	5	19	9	11	23	20
	1	8	12	23	2	14	16	20	3	7	11	22	4	18	19	24	5	10	17	21	6	9	13	15
	1	13	18	20	2	5	11	12	3	14	21	23	4	9	17	22	6	8	16	24	7	10	15	19
	1	2	3	19	4	7	13	14	5	10	17	21	6	8	16	24	9	11	20	23	12	15	18	22
	1	4	10	11	2	8	17	18	3	14	21	23	5	16	19	22	6	9	13	15	7	12	20	24
	1	6	14	22	2	5	11	12	3	15	17	20	4	18	19	24	7	8	9	21	10	13	16	23
3	1	8	12	23	2	13	21	22	3	9	16	18	4	5	6	20	7	10	15	19	11	14	17	24
	1	13	18	20	2	9	10	24	3	7	11	22	4	12	16	21	5	8	14	15	6	17	19	23
	1	7	16	17	2	4	15	23	3	5	13	24	6	11	18	21	8	10	20	22	9	12	14	19
	1	15	21	24	2	14	16	20	3	6	10	12	4	9	17	22	5	7	18	23	8	11	13	19
	2	3	1	19	5	8	14	15	6	11	18	21	4	9	17	22	7	12	20	24	10	13	16	23
	2	5	11	12	3	9	18	16	1	15	21	24	6	17	19	23	4	7	14	13	8	10	20	22
	2	4	15	23	3	6	12	10	1	13	18	20	5	16	19	22	8	9	7	21	11	14	17	24
4	2	9	10	24	3	14	21	23	1	7	17	16	5	6	4	20	8	11	13	19	12	15	18	22
	2	14	16	20	3	7	11	22	1	8	12	23	5	10	17	21	6	9	15	13	4	18	19	24
	2	8	17	18	3	5	13	24	1	6	14	22	4	12	16	21	9	11	20	23	7	10	15	19
	2	13	21	22	3	15	17	20	1	4	11	10	5	7	18	23	6	8	16	24	9	12	14	19
	3	1	2	19	6	9	15	13	4	12	16	21	5	7	18	23	8	10	20	22	11	14	17	24
	3	6	12	10	1	7	16	17	2	13	21	22	4	18	19	24	5	8	15	14	9	11	20	23
	3	5	13	24	1	4	10	11	2	14	16	20	6	17	19	23	9	7	8	21	12	15	18	22
5	3	7	11	22	1	15	21	24	2	8	18	17	6	4	5	20	9	12	14	19	10	13	16	23
	3	15	17	20	1	8	12	23	2	9	10	24	6	11	18	21	4	7	13	14	5	16	19	22
	3	9	18	16	1	6	14	22	2	4	15	23	5	10	17	21	7	12	20	24	8	11	13	19
	3	14	21	23	1	13	18	20	2	5	12	11	6	8	16	24	4	9	17	22	7	10	15	19

points with block size 7 first discovered by Baker [1]. This provides an interesting connection between the $S(2, 4, 25)$ Design 1 and an elliptic semiplane. We refer the reader to the paper by Lamken and Vanstone [13] for details of the construction.

8. Designs, their groups, and other invariants

We presently display the 16 designs and various invariants. For each of the sixteen $S(2, 4, 25)$ designs, we present generators of the corresponding automorphism group G, representatives of the block orbits under the action of G, and orbit lengths. A block orbit is presented in the form $[1\,2\,3\,19]^{42}$ where $\{1, 2, 3, 19\}$ is a design block representative of an orbit of length 42. In a similar fashion we exhibit the orbits of Fano subdesigns by exhibiting the point sets of orbit representative Fano planes and corresponding orbit lengths. We also display orbits of ovals, complete 5-arcs and orbits of parallel classes of blocks. Here, $\{1, 23, 36, 43, 45, 48\}^7$ indicates that blocks with indices $1, 23, \ldots, 48$ form a parallel class which is moved into a G-orbit of 7 parallel classes.

Although we have computed the block-graph invariants for each of the 16 designs, because of the bulk of the data involved we are not displaying this information here. It is worth noticing however that the sixteen designs are discriminated by means of their block-graph invariants. We begin by listing the union of generators of the automorphism groups.

$$\alpha = (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9)(10\ 11\ 12)(13\ 14\ 15)(16\ 17\ 18)(19\ 20\ 21)\ (22\ 23\ 24)(25)$$

$$\beta = (1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9)(10\ 11\ 12)(13\ 14\ 15)(16\ 17\ 18)(19\ 20\ 21)\ (22)(23)(24)(25)$$

$$\hat{\alpha} = (1\ 2\ 3)(4\ 5\ 6)\ (7\ 8\ 9)(10\ 11\ 12)\ (13\ 14\ 15)(16\ 17\ 18)\ (19)(20)(21)(22\ 23\ 24)(25)$$

$$\hat{\beta} = (1\ 4\ 7)(2\ 5\ 8)\ (3\ 6\ 9)(10\ 13\ 16)\ (11\ 14\ 17)(12\ 15\ 18)\ (19\ 20\ 21)(22)(23)(24)(25)$$

$$\gamma_1 = (1\ 2\ 24\ 12\ 8\ 18\ 19\ 9\ 7\ 23\ 17\ 4\ 14\ 21\ 5\ 6\ 22\ 13\ 3\ 10\ 20)(11\ 16\ 15)(25)$$

$$\gamma_2 = (1\ 21\ 13\ 18\ 4\ 15\ 2\ 5\ 19\ 17\ 10\ 8\ 16\ 6\ 9\ 20\ 12\ 14\ 3\ 11\ 7)(22\ 23\ 24)(25)$$

$$\gamma_3 = (1\ 23)(2\ 24)(3\ 25)(4\ 21)(5\ 22)(6\ 17)(7\ 18)(8\ 19)(9\ 20)(10\ 16)(11)(12)(13)(14)(15)$$

$$\gamma_4 = (1\ 25\ 5)(2\ 19\ 10)(3\ 13\ 15)(4\ 7\ 20)(6\ 21\ 24)(8\ 14\ 9)(11\ 22\ 18)(12\ 16\ 23)(17)$$

$$\gamma_5 = (1\ 2\ 3\ 4\ 5\ 6\ 7)(8\ 9\ 10\ 11\ 12\ 13\ 14)(15\ 16\ 17\ 18\ 19\ 20\ 21)(22)(23)(24)(25)$$

$$\gamma_6 = (1\ 2\ 4)(3\ 6\ 5)(7)(8\ 9\ 11)(10\ 13\ 12)(14)(15\ 16\ 18)(17\ 20\ 19)(21)(22\ 23\ 24)(25)$$

$$\gamma_7 = (1\ 20\ 16)(2\ 10\ 3)(5\ 17\ 18)(4\ 19\ 22)(6\ 9\ 25)(11\ 15\ 14)(7\ 21\ 12)(8\ 13\ 24)(23)$$

$$\gamma_8 = (1)(2\ 18)(3\ 5)(4\ 22)(6\ 15)(7)(8\ 24)(9\ 11)(10\ 17)(12\ 21)(13)(14\ 25)(16\ 20)(19)(23)$$

Design 1. $H = \langle \hat{\alpha}, \hat{\beta} \rangle \leq G = \langle \hat{\alpha}, \gamma_1 \rangle$, $|G| = 7 \cdot 8 \cdot 9 = 504$. It should be remarked that the automorphism group G above is isomorphic to $\mathbb{Z}_3 \times \mathrm{PSL}_2(7)$.

Block Orbits	[1 2 3 19]^{42} ; [1 5 9 25]^{8}
Fano Planes	[1 2 3 16 17 18 20]^{24}
Ovals	[1 2 4 5 7 8 22 25]^{42}
Complete 5−arcs	[1 2 15 18 25]^{42}
Parallel Classes	{1,23,36,43,45,48}^{7} ; {1,24,30,32,41,48}^{21}

Design 2. $H = <\hat{\alpha},\hat{\beta}> \leq G = <\hat{\alpha},\gamma_2>$, $|G| = 7 \cdot 9 = 63$.

Block Orbits	[1 2 3 19]^{21} ; [1 4 7 22]^{21} ; [19 20 21 25]^{7} ; [22 23 24 25]^{1} ;
Fano Planes	[1 2 3 16 17 18 20]^{3} ; [1 2 6 7 10 19 22]^{21}
Ovals	[1 2 5 6 12 15 16 17]^{21} ; [1 2 6 9 12 13 22 23]^{21}
Complete 5−arcs	[1 2 15 17 25]^{21} ; [1 6 13 22 24]^{21}
Parallel Classes	None

Design 3. $G = <\hat{\alpha},\hat{\beta}>$, $|G| = 9$,

Block Orbits	[1 6 10 11]^{9} ; [1 12 13 23]^{9} ; [1 14 16 20]^{9} ; [1 15 21 24]^{9} ; [1 2 3 19]^{3} ; [1 4 7 22]^{3} ; [1 5 9 25]^{3} ; [10 13 16 25]^{3} ; [19 20 21 25]^{1} ; [22 23 24 25]^{1}
Fano Planes	[1 2 3 16 17 18 20]^{3}
Ovals	[1 2 4 5 10 13 15 18]^{9} ; [10 11 12 13 14 15 20 21]^{3}
Complete 5−arcs	[10 11 12 20 25]^{3}
Parallel Classes	{2,10,21,33,43,47}^{3}

Design 4. $G = <\hat{\alpha},\hat{\beta}>$, $|G| = 9$.

Block Orbits	[1 6 10 14]^{9} ; [1 11 13 21]^{9} ; [1 15 20 24]^{9} ; [1 16 18 23]^{9} [1 2 3 19]^{3} ; [1 4 7 22]^{3} ; [1 5 9 25]^{3} ; [10 13 16 25]^{3} [19 20 21 25]^{1} ; [22 23 24 25]^{1}
Fano Planes	[1 6 11 12 14 17 21]^{9} ; [10 11 12 19 22 23 24]^{3}
Ovals	[1 2 4 8 10 16 20 21]^{9} ; [1 2 5 7 10 12 15 16]^{9} [10 11 12 13 14 15 19 20]^{3}
Complete 5−arcs	[10 11 12 20 21]^{3}
Parallel Classes	{2,10,20,34,44,47}^{3}

Design 5. $G = <\hat{\alpha},\hat{\beta}>$, $|G| = 9$.

Block Orbits	[1 4 10 15]^{9} ; [1 6 11 22]^{9} ; [1 13 17 20]^{9} ; [1 14 21 24]^{9} ; [1 2 3 19]^{3} ; [1 5 9 25]^{3} ; [10 11 12 25]^{3} ; [10 13 16 22]^{3} ; [19 20 21 25]^{1} ; [22 23 24 25]^{1}
Fano Planes	[1 4 7 12 15 18 23]^{3}
Ovals	[1 2 4 5 7 8 22 24]^{3}
Complete 5−arcs	[1 4 7 24 25]^{3}
Parallel Classes	{1,23,36,44,45,46}^{1}

Design 6. $G = <\gamma_3, \gamma_4>$, $|G| = 2 \cdot 3 \cdot 25 = 150$,

Block Orbits	[1 2 6 25]^{25};[1 3 11 19]^{25}
Fano Planes	None
Ovals	[1 2 3 8 10 15 16 20]^{75}
Complete 5−arcs	[1 2 3 4 5]^{15} ; [1 2 9 10 20]^{75}
Parallel Classes	{1,17,36,41,43,46}^{25}

Block Orbits	[1 9 17 22]^{21};[1 2 4 14]^{7} ; [1 8 15 25]^{7} ; [1 18 20 21]^{7} ; [8 9 11 21]^{7} ; [22 23 24 25]^{1}
Fano Planes	[1 2 3 4 5 6 7]^{3}
Ovals	None
Complete 5−arcs	[1 2 6 10 25]^{7}
Parallel Classes	None

Design 8. $G = <\gamma_7, \gamma_8>$, $|G| = 6$.

Block Orbits	[1 2 4 25]^{6} ; [1 3 8 11]^{6} ; [2 3 14 19]^{6} ; [2 6 9 12]^{6} ; [1 6 7 15]^{3} ; [1 10 13 17]^{3} ; [1 12 19 21]^{3} ; [2 7 18 23]^{3} ; [2 17 21 24]^{3} ; [4 6 8 14]^{3} ; [4 12 13 24]^{3} ; [8 9 15 23]^{3} ; [1 16 20 23]^{1} ; [4 19 22 23]^{1}
Fano Planes	None
Ovals	[1 2 5 6 11 13 14 21]^{6} ; [1 4 9 10 11 12 14 23]^{6} ; [1 7 8 9 12 13 14 16]^{3} ; [2 3 4 5 12 18 21 22]^{3} ; [2 3 5 9 11 15 17 25]^{3} ; [2 5 7 9 15 19 21 22]^{3} ; [2 8 9 11 14 18 24 25]^{3}
Complete 5−arcs	[1 7 13 19 23]^{3} ; [2 3 4 5 17]^{3} ; [2 4 5 12 23]^{3} ; [2 6 13 14 17]^{6}
Parallel Classes	{1,17,33,40,44,49}^{3} ; {2,15,27,30,34,36}^{3} ; {8,9,26,28,36,47}^{3}

Design 9, $G = <\alpha>$, $|G| = 3$.

Block Orbits	[1 4 16 24]^{3} ; [1 5 12 21]^{3} ; [1 6 13 22]^{3} ; [1 7 14 15]^{3} ; [1 8 17 18]^{3} ; [1 9 19 20]^{3} ; [1 10 11 23]^{3} ; [4 7 12 19]^{3} ; [4 8 9 22]^{3} ; [4 10 15 18]^{3} ; [4 13 17 21]^{3} ; [7 10 13 25]^{3} ; [7 11 18 22]^{3} ; [10 14 16 21]^{3} ; [13 19 23 24]^{3} ; [16 19 22 25]^{3} ; [1 2 3 25]^{1} ; [4 5 6 25]^{1}
Fano Planes	None
Ovals	[4 5 10 11 19 21 22 24]^{3} ; [7 8 10 14 17 19 22 23]^{3}
Complete 5−arcs	[1 2 4 17 19]^{3} ; [13 16 19 20 21]^{3}
Parallel Classes	{2,13,22,31,33,49}^{3}

Design 10, $G = <\alpha>$, $|G| = 3$.

Block Orbits	[1 4 20 24]^{3} ; [1 5 11 23]^{3} ; [1 6 14 21]^{3} ; [1 7 15 17]^{3} ; [1 8 12 16]^{3} ; [1 9 13 22]^{3} ; [1 10 18 19]^{3} ; [4 7 16 21]^{3} ; [4 8 9 23]^{3} ; [4 11 12 13]^{3} ; [4 14 17 18]^{3} ; [7 10 13 25]^{3} ; [7 12 19 20]^{3} ; [10 16 23 24]^{3} ; [13 15 21 23]^{3} ; [16 19 22 25]^{3} ; [1 2 3 25]^{1} ; [4 5 6 25]^{1}
Fano Planes	[1 5 10 12 16 18 23]^{3}
Ovals	[1 2 9 11 14 15 18 24]^{3} ; [1 4 8 11 15 18 21 22]^{3} ; [1 6 8 13 15 19 20 25]^{3} ; [4 5 9 12 16 17 20 22]^{3} ; [10 11 13 14 16 18 21 22]^{3}
Complete 5−arcs	None
Parallel Classes	None

Design 11, $G = <\alpha>$, $|G| = 3$

Block Orbits	$[1\ 4\ 19\ 20]^3$; $[1\ 5\ 11\ 23]^3$; $[1\ 6\ 13\ 14]^3$; $[1\ 7\ 15\ 18]^3$; $[1\ 8\ 10\ 24]^3$; $[1\ 9\ 16\ 21]^3$; $[1\ 12\ 17\ 22]^3$; $[4\ 7\ 11\ 21]^3$; $[4\ 8\ 9\ 23]^3$; $[4\ 12\ 16\ 18]^3$; $[4\ 13\ 17\ 24]^3$; $[7\ 10\ 13\ 25]^3$; $[7\ 14\ 16\ 20]^3$; $[10\ 12\ 14\ 21]^3$; $[13\ 21\ 22\ 23]^3$; $[16\ 19\ 22\ 25]^3$; $[1\ 2\ 3\ 25]^1$; $[4\ 5\ 6\ 25]^1$
Fano Planes	None
Ovals	$[1\ 2\ 4\ 5\ 9\ 10\ 12\ 13]^3$; $[1\ 2\ 4\ 7\ 16\ 22\ 23\ 24]^3$; $[1\ 5\ 8\ 9\ 13\ 20\ 22\ 25]^3$; $[7\ 12\ 13\ 15\ 16\ 19\ 21\ 24]^3$
Complete 5–arcs	$[1\ 6\ 12\ 15\ 19]^3$
Parallel Classes	$\{3,11,16,37,39,41\}^1$

Design 12, $G = <\alpha>$, $|G| = 3$.

Block Orbits	$[1\ 4\ 20\ 22]^3$; $[1\ 5\ 10\ 18]^3$; $[1\ 6\ 15\ 17]^3$; $[1\ 7\ 12\ 14]^3$; $[1\ 8\ 13\ 16]^3$; $[1\ 9\ 23\ 24]^3$; $[1\ 11\ 19\ 21]^3$; $[4\ 7\ 11\ 23]^3$; $[4\ 8\ 9\ 21]^3$; $[4\ 10\ 14\ 19]^3$; $[4\ 15\ 16\ 24]^3$; $[7\ 10\ 13\ 25]^3$; $[7\ 16\ 17\ 21]^3$; $[10\ 12\ 16\ 23]^3$; $[13\ 15\ 19\ 23]^3$; $[16\ 19\ 22\ 25]^3$; $[1\ 2\ 3\ 25]^1$; $[4\ 5\ 6\ 25]^1$
Fano Planes	None
Ovals	$[1\ 2\ 5\ 6\ 8\ 14\ 19\ 22]^3$; $[1\ 2\ 7\ 9\ 13\ 15\ 20\ 21]^3$; $[1\ 2\ 10\ 11\ 13\ 14\ 22\ 23]^3$ $[1\ 8\ 10\ 12\ 17\ 21\ 22\ 25]^3$; $[1\ 8\ 12\ 15\ 18\ 20\ 21\ 23]^3$
Complete 5–arcs	$[7\ 15\ 20\ 22\ 25]^3$
Parallel Classes	None

Design 13, $G = <\alpha>$, $|G| = 3$.

Block Orbits	$[1\ 4\ 16\ 23]^3$; $[1\ 5\ 7\ 21]^3$; $[1\ 6\ 12\ 14]^3$; $[1\ 8\ 10\ 18]^3$; $[1\ 9\ 13\ 22]^3$; $[1\ 11\ 20\ 24]^3$; $[1\ 15\ 17\ 19]^3$; $[4\ 7\ 22\ 24]^3$; $[4\ 8\ 12\ 13]^3$; $[4\ 11\ 19\ 21]^3$; $[4\ 14\ 17\ 18]^3$; $[7\ 8\ 16\ 20]^3$; $[7\ 10\ 13\ 25]^3$; $[10\ 11\ 17\ 22]^3$; $[13\ 14\ 19\ 24]^3$; $[16\ 19\ 22\ 25]^3$; $[1\ 2\ 3\ 25]^1$; $[4\ 5\ 6\ 25]^1$
Fano Planes	$[1\ 2\ 3\ 7\ 12\ 14\ 21]^3$
Ovals	$[1\ 2\ 5\ 11\ 14\ 18\ 19\ 22]^3$; $[1\ 7\ 8\ 12\ 19\ 23\ 24\ 25]^3$; $[1\ 7\ 9\ 14\ 16\ 17\ 24\ 25]^3$; $[7\ 8\ 10\ 12\ 14\ 15\ 19\ 21]^3$
Complete 5–arcs	$[1\ 7\ 9\ 12\ 16]^3$
Parallel Classes	None

Design 14, $G = <\alpha>$, $|G| = 3$.

Block Orbits	$[1\ 4\ 18\ 23]^3$; $[1\ 5\ 7\ 19]^3$; $[1\ 6\ 12\ 14]^3$; $[1\ 8\ 15\ 24]^3$; $[1\ 9\ 11\ 16]^3$; $[1\ 10\ 20\ 22]^3$; $[1\ 13\ 17\ 21]^3$; $[4\ 7\ 22\ 24]^3$; $[4\ 8\ 12\ 13]^3$; $[4\ 11\ 19\ 20]^3$; $[4\ 14\ 16\ 17]^3$; $[7\ 8\ 16\ 21]^3$; $[7\ 10\ 13\ 25]^3$; $[10\ 11\ 17\ 24]^3$; $[13\ 14\ 20\ 24]^3$; $[16\ 19\ 22\ 25]^3$; $[1\ 2\ 3\ 25]^1$; $[4\ 5\ 6\ 25]^1$
Fano Planes	$[1\ 2\ 3\ 7\ 12\ 14\ 19]^3$
Ovals	$[4\ 5\ 11\ 12\ 14\ 15\ 23\ 24]^3$; $[4\ 8\ 9\ 10\ 16\ 20\ 24\ 25]^3$; $[7\ 8\ 10\ 12\ 14\ 15\ 19\ 20]^3$
Complete 5–arcs	$[1\ 12\ 13\ 19\ 22]^3$; $[4\ 15\ 20\ 24\ 25]^3$
Parallel Classes	None

Design 15, $G = <\beta>$, $|G| = 3$.

Block Orbits	$[1\ 4\ 13\ 24]^3$; $[1\ 5\ 17\ 21]^3$; $[1\ 6\ 8\ 20]^3$; $[1\ 7\ 11\ 25]^3$; $[1\ 9\ 16\ 18]^3$; $[1\ 10\ 14\ 15]^3$; $[1\ 12\ 19\ 23]^3$; $[4\ 7\ 10\ 22]^3$; $[4\ 8\ 15\ 19]^3$; $[4\ 11\ 12\ 17]^3$; $[4\ 14\ 18\ 25]^3$; $[7\ 12\ 15\ 20]^3$; $[7\ 13\ 18\ 23]^3$; $[10\ 17\ 19\ 24]^3$; $[13\ 16\ 19\ 22]^3$; $[1\ 2\ 3\ 22]^1$; $[4\ 5\ 6\ 23]^1$; $[7\ 8\ 9\ 24]^1$; $[19\ 20\ 21\ 25]^1$; $[22\ 23\ 24\ 25]^1$
Fano Planes	$[1\ 2\ 3\ 13\ 14\ 15\ 24]^1$; $[4\ 5\ 6\ 10\ 11\ 12\ 22]^1$; $[7\ 8\ 9\ 16\ 17\ 18\ 23]^1$
Ovals	$[7\ 10\ 13\ 14\ 16\ 20\ 24\ 25]^3$
Complete 5-arcs	$[4\ 5\ 8\ 9\ 18]^3$; $[16\ 17\ 18\ 24\ 25]^1$
Parallel Classes	None

Design 16, $G = <\beta>$, $|G| = 3$.

Block Orbits	$[1\ 4\ 13\ 24]^3$; $[1\ 5\ 16\ 20]^3$; $[1\ 6\ 8\ 19]^3$; $[1\ 7\ 17\ 18]^3$; $[1\ 9\ 10\ 25]^3$; $[1\ 11\ 14\ 15]^3$; $[1\ 12\ 21\ 23]^3$; $[4\ 7\ 10\ 22]^3$; $[4\ 8\ 14\ 21]^3$; $[4\ 11\ 12\ 16]^3$; $[4\ 15\ 17\ 25]^3$; $[7\ 12\ 14\ 19]^3$; $[7\ 15\ 16\ 23]^3$; $[10\ 16\ 21\ 24]^3$; $[13\ 16\ 19\ 22]^3$; $[1\ 2\ 3\ 22]^1$; $[4\ 5\ 6\ 23]^1$; $[7\ 8\ 9\ 24]^1$; $[19\ 20\ 21\ 25]^1$; $[22\ 23\ 24\ 25]^1$
Fano Planes	$[1\ 2\ 3\ 13\ 14\ 15\ 24]^1$; $[4\ 5\ 6\ 10\ 11\ 12\ 22]^1$; $[7\ 8\ 9\ 16\ 17\ 18\ 23]^1$
Ovals	$[1\ 2\ 6\ 9\ 11\ 16\ 23\ 24]^3$; $[1\ 2\ 6\ 15\ 18\ 20\ 23\ 25]^3$; $[1\ 8\ 12\ 15\ 16\ 17\ 22\ 24]^3$
Complete 5-arcs	$[1\ 2\ 4\ 6\ 11]^3$; $[4\ 5\ 18\ 20\ 22]^3$; $[16\ 17\ 18\ 24\ 25]^1$
Parallel Classes	None

Table 7
Summary of Properties of the 16 Designs

DESIGN NO.	$\|G\|$	NO. FANO PLANES	NO. OVALS	NO. COMPLETE 5-ARCS	MAX. NO. DISJOINT COMPLETE 5-ARCS	NO. PARALLEL CLASSES
1	504	24	42	42	1	28
2	63	24	42	42	2	0
3	9	3	12	3	1	3
4	9	12	21	3	1	3
5	9	3	3	3	1	1
6	150	0	75	90	5	25
7	21	3	0	7	1	0
8	6	0	27	15	3	9
9	3	0	6	6	1	3
10	3	3	15	0	0	0
11	3	0	12	3	3	1
12	3	0	15	3	1	0
13	3	3	12	3	1	0
14	3	3	9	6	4	0
15	3	3	3	4	1	0
16	3	3	9	7	2	0

9. Concluding remarks

The above analysis establishes that there are precisely 16 pairwise non-isomorphic Steiner systems $S(2, 4, 25)$'s with a nontrivial automorphism group, and provides us with a number of invariant substructures which discriminate the 16 designs. For convenience we present in *Table 7* a summary of properties of the 16 $S(2, 4, 25)$'s with non-trivial automorphism group.

For emphasis we state:

Theorem 9.1. *There are exactly* 16 *non-isomorphic Steiner systems* $S(2, 4, 25)$ *with non-trivial automorphism group. Each such design has an automorphism of order* 3. *These designs are distinguished from one another either by the substructures summarized in Table* 7, *or by their block-graph invariants.*

An immediate problem is suggested:

Problem 1. Determine if there are any, or find all, $S(2, 4, 25)$'s with identity automorphism group.

Another natural question concerns the extendability of each of our 16 $S(2, 4, 25)$'s. A single extension would yield an $S(3, 5, 26)$ and such a design was first given by Hanani [10]. The group of this $S(3, 5, 26)$ is transitive on the 26 points so a quick check establishes that all derived $S(2, 4, 25)$'s of Hanani's design are isomorphic to Design 1. Also, Denniston [5] has constructed an $S(5, 7, 28)$ which would be a triple extension of some $S(2, 4, 25)$. Since Denniston's design has $PSL_2(27)$ as its automorphism group, acting as a 3-homogeneous group on the 28 points, all doubly derived $S(3, 5, 26)$ designs are isomorphic. In fact these designs are isomorphic to Hanani's $S(3, 5, 26)$. Thus, the triply derived $S(2, 4, 25)$'s from Denniston's design are all isomorphic to Design 1.

The necessary arithmetic conditions for an $S(8, 10, 31)$ are satisfied so it is theoretically possible that some $S(2, 4, 25)$ could extend 6 times. We state:

Problem 2. How far does any given $S(2, 4, 25)$ extend?

Note added in proof. The chromatic index of a design is the smallest number of colors needed to color the points so that no blocks are monochromatic. Kevin Phelps has determined that Design 9 and Design 10 have chromatic index 2. The other fourteen designs in our list have chromatic index 3.

References

[1] R.D. Baker, Elliptic semiplanes I: existence and classification, Proc. 8th S.E. Conf. Combinatorics, Graph Theory and Computing, LSU, Baton Rouge, LA (1977) Congressus Numerantium XIX, 61–73.

[2] T. Beth, D. Jungnickel and H. Lenz, Design Theory (Bibliographisches Institut, Mannheim–Wien–Zurich, and Cambridge University Press, Cambridge, 1985).

[3] A.E. Brouwer, personal communication.

[4] F.C. Bussemaker, R. Mathon and J.J. Seidel, Tables of two-graphs, Combinatorics and Graph Theory, Proc. Conf. Calcutta 1980, Lecture Notes Math. 885, (Springer 1981) 70–112.

[5] R.H.F. Denniston, Some new 5-designs, Bull. London Math. Soc. 8 (1976) 263–267.

[6] M.J. de Resmini, On k-sets of type (m, n) in a Steiner system $S(2, l, v)$, Finite Geometries and Designs, LMS Lecture Note Series 49 (1981) 104–113.

[7] M.J. de Resmini, Some remarks on Steiner systems $S(2, 3, v)$ and $S(2, 4, v)$, this volume.

[8] H. Gropp, Il metodo Di Martinetti (1887) or configurations and Steiner systems $S(2, 4, 25)$, Catania Combinatorial Conference, September 1986 (preprint).

[9] M. Hall, Combinatorial Theory (Wiley, New York, 1986).

[10] H. Hanani, A class of 3-designs, Combinatorial Mathematics, Proc. Conf. Canberra (1977) Lecture Notes Math. 686 (Springer, Berlin, 1978) 34–46.

[11] M.D. Hestenes and D.G. Higman, Rank 3 groups and strongly regular graphs, Computers in Algebra and Number Theory, SIAM-AMS Proceedings, 4 (1971) 141–159.

[12] E.S. Kramer, S.S. Magliveras and V.D. Tonchev, On the Steiner systems $S(2, 4, 25)$ invariant under a group of order 9, Annals of Discrete Mathematics, 34 (1987) 307–314.

[13] E.R. Lamken and S.A. Vanstone, Elliptic semiplanes and group divisible designs with orthogonal resolutions, Aequationes Mathematicae 30 (1986) 80–92.

[14] R. Mathon, Symmetric (31, 10, 3) designs with non-trivial automorphism group, preprint.

[15] R. Mathon and A. Rosa, Tables of parameters of BIBDs with $r \leq 41$ including existence, enumeration, and resolvability results, Annals of Discrete Math. 26 (1985) 275–308.

[16] A.Y. Petrenyuk, O postroenii neisomorfnykh blok-skhem s pomosciu isograficeskikh naborov blokov, Kirovogr. Inst. S.-Kh. Masinostr., No. 985 (Kirovograd, 1983) 16pp.

[17] L.P. Petrenyuk and A.Y. Petrenyuk, O neisomorfnykh $B(25, 4, 1)$ i $KST(21)$, Kirovogr. Inst. S.-Kh. Masinostr., No. 84 (Kirovograd, 1984) 9pp.

[18] V.D. Tonchev, Two new Steiner systems $S(2, 4, 25)$, Comt. Rend. Acad. Bulg. Sci. 39 (1986) 47–48.

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 159–176
North-Holland

BALANCED TOURNAMENT DESIGNS AND RELATED TOPICS

E.R. LAMKEN and S.A. VANSTONE
Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

A balanced tournament design of order n, BTD(n), is an $n \times (2n-1)$ array defined on a set of $2n$ elements V such that (1) each cell of the array contains a pair of distinct elements from V, (2) every pair of distinct elements from V is contained in some cell, (3) each element is contained in each column, and (4) no element is contained in more than 2 cells of each row. BTD(n)s are very useful for scheduling certain types of round robin tournaments such as tennis and curling. Their existence has been completely settled. In this paper we survey the known results and discuss various extensions and generalizations.

1. Introduction

A round robin tournament is played among $2n$ players in $2n-1$ rounds. There are n courts of unequal attractiveness available for the matches and each round is played at one time using all the courts. To balance the effect of the different courts it is desired to arrange the tournament so that no player competes more than twice on any one court.

Haselgrove and Leech [10] established the existence of such designs for $n \equiv 0$ or 1 (mod 3). Schellenberg, van Rees and Vanstone [33] completed the spectrum of existence. In the sequel we consider this problem and related topics. We begin by giving a formal definition of the problem.

A tournament design, TD(n), defined on a $2n$-set, V, is an arrangement of the $\binom{2n}{2}$ distinct unordered pairs of the elements of V into an $n \times (2n-1)$ array such that

(1) every element of V is contained in precisely one cell of each column.

The parameter n is called the side of the TD(n). Clearly a TD(n) is equivalent to a 1-factorization of the complete graph on $2n$ vertices. Such 1-factorizations have been extensively studied ([28]).

Gelling and Odeh [8] introduced the problem of constructing TD(n)s with the following property:

(2) no element of V is contained in more than 2 cells of any row.

A TD(n) with property (2) is called a balanced tournament design and is denoted BTD(n). If we let the elements of V correspond to the players in a round robin tournament, the columns correspond to the rounds and the rows correspond to the court assignments, then a BTD(n) represents a round robin tournament as described at the beginning of this section.

A simple but very important observation is stated in the next lemma.

Lemma 1.1. *Every element of a* BTD(n) *is contained twice in* ($n-1$) *rows and once in the remaining row.*

An element which is contained only once in row i is called a *deficient element* of row i. The two deficient elements of row i are referred to as the deficient pair of row i. We note that the deficient pair of row i need not occur in a common cell of that row.

Lemma 1.2. *The deficient pairs of a* BTD(n) *on V partition the elements of V into pairs.*

As previously mentioned, the existence of BTD(n)s was established in [33]. The proof uses a particular class of BTD(n)s called factored BTD(n)s. A factored BTD(n) is a BTD(n) with the property that in each row there exists n cells, called a factor, which contain all $2n$ elements of V. Note that the pairs in a factor correspond to a 1-factor of the complete graph on $2n$ vertices. An example of a FBTD(4) is given in Fig. 1.

The following results are established in [33].

Theorem 1.3. *There exists a* FTBD(n) *for each odd positive integer n.*

The proof of this result is by a direct construction for the stated designs.

Theorem 1.4. *If there exists a* FBTD(n) *and if there exists a pair of mutually orthogonal Latin squares of order $2n$, then there exists a* FBTD($2n$).

Since a pair of orthogonal Latin squares of order n is known to exist ([2]) for all positive integers n, $n \neq 2$ or 6, the existence of a FBTD(4), and a FBTD(6) along with Theorems 1.3 and 1.4 is enough to prove that a FBTD(n) exists for all positive integers n, $n \neq 2$. A FBTD(6) was recently found ([17]) and is displayed in Fig. 2. We summarize this in the following statement.

$\underline{34}$	$\underline{56}$	$\underline{12}$	$\underline{78}$	45	67	83
16	24	35	$\underline{46}$	$\underline{28}$	$\underline{13}$	$\underline{57}$
$\underline{27}$	18	47	$\underline{15}$	$\underline{36}$	$\underline{48}$	26
58	$\underline{37}$	$\underline{68}$	23	17	$\underline{25}$	$\underline{14}$

Fig. 1. A FBTD(4).

$e8$	$\underline{46}$	62	$\underline{t0}$	03	$\underline{e3}$	$\underline{91}$	17	$t5$	$\underline{58}$	$\underline{27}$
$\underline{69}$	$e9$	$\underline{57}$	73	$\underline{t1}$	14	$\underline{e4}$	$\underline{02}$	28	$t6$	$\underline{38}$
$t7$	$\underline{70}$	$e0$	$\underline{68}$	84	$\underline{t2}$	25	$\underline{e5}$	$\underline{13}$	39	$\underline{49}$
40	$t8$	$\underline{81}$	$e1$	$\underline{79}$	95	$\underline{t3}$	36	$\underline{e6}$	$\underline{42}$	$\underline{50}$
$\underline{53}$	51	$t9$	$\underline{92}$	$e2$	$\underline{80}$	06	$\underline{t4}$	47	$\underline{e7}$	$\underline{61}$
$\underline{12}$	23	$\underline{34}$	45	$\underline{56}$	67	$\underline{78}$	89	$\underline{90}$	01	$\underline{te}$

Fig. 2. A FBTD(6).

Theorem 1.5 (Lamken and Vanstone [17]). *A* FBTD(n) *exists if and only if n is a positive integer and $n \neq 2$.*

An alternate proof of the existence of FBTD(n)s can be given which requires the direct construction of only a small number of designs. We state the result in two theorems and give an outline of the proofs.

Theorem 1.6. *There exists a* FBTD(n) *for* $n \equiv 1 \pmod 2$.

Proof. If $n \equiv 1 \pmod 4$ and $n > 13$, we apply Theorem 3.1 of [18] and if $n \equiv 3 \pmod 4$ and $n > 7$ we apply Theorem 3.1 of [19]. The cases $n = 3$, 5, 7, 9 and 13 must be done directly. □

Theorem 1.7. *There exists a* FBTD(n) *for* $n \equiv 0 \pmod 2$.

Proof. Use the doubling construction stated in Theorem 1.4. As before, a FBTD(4) and a FBTD(6) must be constructed directly. □

In Section 2 we will consider BTD(n)s with additional properties. Section 3 looks at some graph theoretic properties of these designs and Section 4 discusses an application of BTD(n)s to the construction of resolvable balanced incomplete block designs. Finally, a generalization of the problem is considered in Section 5.

2. Factor balanced tournament designs and partitioned balanced tournament designs

When designing a balanced tournament for $2n$ players it may be desirable to have the property that each player plays exactly once on each court during the first n rounds. Hence, we say that a BTD(n) is factor balanced, denoted FBBTD(n), if it satisfies

(3) each row of the BTD(n) has a factor in the first n columns of the array.

In addition to property (3), if the BTD(n) also satisfies

(4) each row of the BTD(n) has a factor in the last n columns of the array, then the BTD(n) is called a partitioned balanced tournament design and is denoted by PBTD(n).

To show that property (3) does not imply property (4), we construct FBBTD(n)s which are not PBTD(n)s for all n, $n \neq 2$, 3, or 4. We require several definitions to do this.

A Howell design, $H(s, 2n)$, is an $s \times s$ array A defined on a $2n$-set V of elements such that

(i) every cell of A is either empty or contains a 2-subset of V,

(ii) every element of V is contained in precisely one cell of each row and column of A;

(iii) every pair of distinct elements from V is contained in at most one cell of the array.

It is not difficult to see that $n \leq s \leq 2n - 1$. A number of papers on Howell designs culminated in the following result.

Theorem 2.1 (Stinson [35]). *An $H(s, 2n)$ exists if and only if $(2n, s)$ satisfies $n \leq s \leq 2n - 1$ and $(2n, s) \notin \{(4, 3), (4, 2), (6, 5), (8, 5)\}$.*

An $H(2n - 1, 2n)$ is called a Room square of side $2n - 1$. A Room square is said to be in *standard form* if some element of V is contained in each cell of the main diagonal. Any Room square can be put into standard form by an appropriate permutation of rows and columns. A standardized Room square is said to be *skew* if it has the property that cell (i, j) of A contains a pair implies cell (j, i) is empty for $i \neq j$. The spectrum for the existence of skew Room squares is known.

Theorem 2.2 (Stinson [35]). *A skew Room square of side n exists if and only if n is an odd positive integer and $n \neq 3$ or 5.*

We also require the following two theorems which are stated in modified form [33]. In a PBTD(n), the deficient pairs must form a column of the array. A careful inspection of the next two constructions [33] shows that the deficient pairs of the resulting FBTDs will never form a column of the array. In addition, both constructions use a pair of orthogonal Latin squares which insures that the BTDs are factor balanced.

Theorem 2.3 (Schellenberg, van Rees, Vanstone [33]). *If there exists a skew Room square of side r, and if there exists a pair of orthogonal Latin squares of side r, then there exists a* FBBTD(r) *which is not a* PBTD(r).

Theorem 2.4 (Schellenberg, van Rees, Vanstone [33]). *If there exists a* FBTD(n) *and if there exists a pair of orthogonal Latin squares of side $2n$, then there exists a* FBBTD($2n$) *which is not a* PBTD($2n$).

We can now state and prove our existence result.

16	35	23	45	24
25	46	14	13	36
34	12	56	26	15

Fig. 3. A BTD(3).

Theorem 2.5. (i) *There is no* FBBTD(n) *for* $n = 2$, 3, *or* 4. (ii) *There exists a* FBBTD(n) *which is not a* PBTD(n) *if and only if* $n \geqslant 5$.

Proof. (i) It is easily checked that no BTD(2) exists. Up to isomorphism there is precisely one BTD(3) (Fig. 3). It is easily checked that this design is not a FBBTD(3). Suppose A is a FBBTD(4). Let B be the subarray of A consisting of the first 4 columns. B must be an $H(4, 8)$. Rosa and Stinson [31] have proven that any $H(4, 8)$ is equivalent to a pair of orthogonal Latin squares of order 4. It is a simple matter to check that a pair of orthogonal Latin squares cannot be extended to a FBBTD(4).

(ii) The proof of this part follows from Theorems 2.2, 2.3, the existence of orthogonal Latin squares and the existence of FBBTD(n)s for $n = 5$, 6 and 8 which are displayed in Figs 4, 5 and 6, respectively. □

$\infty 0$	$\bar{2}\bar{3}$	13	$\alpha\bar{1}$	$\bar{0}2$	$\bar{0}\bar{3}$	12	$\alpha 0$	$\infty\bar{1}$
23	$\infty 1$	$\alpha\bar{3}$	$\bar{0}\bar{2}$	$\bar{1}0$	03	$\bar{1}\bar{2}$	$\infty\bar{3}$	$\alpha 2$
$\bar{1}\bar{3}$	$\alpha\bar{0}$	$\infty 2$	01	$\bar{2}3$	$\alpha 1$	$\infty\bar{0}$	$2\bar{2}$	$3\bar{3}$
$\alpha\bar{2}$	02	$\bar{0}\bar{1}$	$\infty 3$	$\bar{3}1$	$\infty\bar{2}$	$\alpha 3$	$1\bar{1}$	$0\bar{0}$
$1\bar{0}$	$\bar{1}3$	$\bar{2}0$	$\bar{3}2$	$\alpha\infty$	$\bar{1}2$	$0\bar{3}$	$\bar{3}0$	$1\bar{2}$

Fig. 4. A FBBTD(5).

$0\bar{1}$	$\alpha\bar{4}$	34	$\bar{2}\bar{3}$	$\infty 2$	$\bar{0}1$	$1\bar{1}$	$\infty\bar{4}$	24	$\bar{0}\bar{2}$	$\alpha 3$
$\infty 3$	$1\bar{2}$	$\alpha\bar{0}$	40	$\bar{3}\bar{4}$	$\bar{1}2$	$\alpha 4$	$2\bar{2}$	$\infty\bar{0}$	30	$\bar{1}\bar{3}$
$\bar{4}\bar{0}$	$\infty 4$	$2\bar{3}$	$\alpha\bar{1}$	01	$\bar{2}3$	$\bar{2}\bar{4}$	$\alpha 0$	$3\bar{3}$	$\infty\bar{1}$	41
12	$\bar{0}\bar{1}$	$\infty 0$	$3\bar{4}$	$\alpha\bar{2}$	$\bar{3}4$	02	$\bar{3}\bar{0}$	$\alpha 1$	$4\bar{4}$	$\infty\bar{2}$
$\alpha\bar{3}$	23	$\bar{1}\bar{2}$	$\infty 1$	$4\bar{0}$	$\bar{4}0$	$\infty\bar{3}$	13	$\bar{4}\bar{1}$	$\alpha 2$	$0\bar{0}$
$\bar{2}4$	$\bar{3}0$	$\bar{4}1$	$\bar{0}2$	$\bar{1}3$	$\alpha\infty$	$\bar{0}3$	$\bar{1}4$	$\bar{2}0$	$\bar{3}1$	$\bar{4}2$

Fig. 5. A FBBTD(6).

$0\bar{0}$	$\infty\bar{3}$	$\bar{1}\bar{6}$	25	$\bar{2}\bar{5}$	16	$\alpha 4$	$3\bar{4}$	$\bar{5}2$	$\infty 1$	$3\bar{1}$	60	$\alpha\bar{4}$	$4\bar{6}$	$\bar{2}\bar{3}$
$\alpha 5$	$1\bar{1}$	$\infty\bar{4}$	$\bar{2}\bar{0}$	36	$\bar{3}\bar{6}$	20	$4\bar{5}$	$\bar{3}\bar{4}$	$\bar{6}3$	$\infty 2$	$4\bar{2}$	01	$\alpha\bar{5}$	$5\bar{0}$
31	$\alpha 6$	$2\bar{2}$	$\infty\bar{5}$	$\bar{3}\bar{1}$	40	$\bar{4}\bar{0}$	$5\bar{6}$	$6\bar{1}$	$\bar{4}\bar{5}$	$\bar{0}4$	$\infty 3$	$5\bar{3}$	12	$\alpha\bar{6}$
$\bar{5}\bar{1}$	42	$\alpha 0$	$3\bar{3}$	$\infty\bar{6}$	$\bar{4}\bar{2}$	51	$6\bar{0}$	$\alpha\bar{0}$	$0\bar{2}$	$\bar{5}\bar{6}$	$\bar{1}5$	$\infty 4$	$6\bar{4}$	23
62	$\bar{6}\bar{2}$	53	$\alpha 1$	$4\bar{4}$	$\infty\bar{0}$	$\bar{5}\bar{3}$	$0\bar{1}$	34	$\alpha\bar{1}$	$1\bar{3}$	$\bar{6}\bar{0}$	$\bar{2}6$	$\infty 5$	$0\bar{5}$
$\bar{6}\bar{4}$	03	$\bar{0}\bar{3}$	64	$\alpha 2$	$5\bar{5}$	$\infty\bar{1}$	$1\bar{2}$	$1\bar{6}$	45	$\alpha\bar{2}$	$2\bar{4}$	$\bar{0}\bar{1}$	$\bar{3}0$	$\infty 6$
$\infty\bar{2}$	$\bar{0}\bar{5}$	14	$\bar{1}\bar{4}$	05	$\alpha 3$	$6\bar{6}$	$2\bar{3}$	$\infty 0$	$2\bar{0}$	56	$\alpha\bar{3}$	$3\bar{5}$	$\bar{1}\bar{2}$	$\bar{4}1$
$\bar{3}4$	$\bar{4}5$	$\bar{5}6$	$\bar{6}0$	$\bar{0}1$	$\bar{1}2$	$\bar{2}3$	$\alpha\infty$	$\bar{2}5$	$\bar{3}6$	$\bar{4}0$	$\bar{5}1$	$\bar{6}2$	$\bar{0}3$	$\bar{1}4$

Fig. 6. A FBBTD(8).

The existence of PBTD(n)s is a much more difficult question and its spectrum has not yet been completely determined; however, significant progress has been made and only seven possible values of n are now in question. We state this result in the next theorem. Since the constructions needed for the proof are quite complicated and different from those used for BTD(n)s and FBBTD(n)s, we omit even an outline of it.

Theorem 2.6 (Lamken and Vanstone [18, 19, 20], Lamken [21]). *There exists a* PBTD(n) *for all* $n \geq 5$ *except possibly* $n \in \{9, 11, 15, 26, 28, 34, 44\}$.

The PBTD(n) problem was first considered by Stinson [36] in a different form. We note that in a PBTD(n) the columns of the array can be partitioned to give subarrays C_1, C_2, and C_3 where C_1 consists of the first $n-1$ columns, C_2 is simply the nth column and C_3 is the last $n-1$ columns. Clearly, C_1 and C_2 form an $H(n, 2n)$ as do C_2 and C_3. These two designs are referred to as an almost disjoint pair of Howell designs. Stinson [36] found the first example of a PBTD(5) while investigating Howell designs on 10 points.

Recall that a Room square is an $H(2n-1, 2n)$. Each row of such an array contains precisely $n-1$ empty cells. Hence, the largest possible empty subarray in a Room square of side $2n-1$ is $(n-1)\times(n-1)$. A Room square which contains such a subarray is called a maximum empty subarray Room square of side $2n-1$ and is denoted MESRS($2n-1$). Since all Room squares of side 7 have been enumerated ([38]) it is a simple matter to see than no MESRS(7) exists. Since a MESRS($2n-1$) is equivalent to a PBTD(n), the non-existence of a MESRS(7) also follows from Theorem 2.5. We should point out that the constructions used to prove the existence of Room squares, in general, do not apply to the more restrictive class of MESRS. Constructions which could exploit the very powerful PBD-closure technique do not appear to apply to this class of designs. Stinson [36] conjectured that MESRS(r) exist for all odd values of r greater than 7. Theorem 2.6 confirms this conjecture in all but 7 possible cases. We conclude this section with an example of a PBTD(5) ([36]) and its associated MESRS(9). These are displayed in Figs 7 and 8 respectively. We note that the existence of PBTD(n)s provides an alternate proof of the existence of Room squares.

α 4	∞ 2	1 3	5 7	0 6	2 3	4 5	∞ 7	α 1
∞ 3	α 5	4 6	0 2	1 7	∞ 4	α 2	0 5	6 3
5 6	0 3	α 7	∞ 1	4 2	6 7	0 1	α 3	∞ 5
1 2	4 7	∞ 0	α 6	5 3	α 0	∞ 6	1 4	7 2
0 7	1 6	2 5	4 3	α ∞	1 5	3 7	2 6	0 4

C_1 C_2 C_3

Fig. 7. PBTD(5).

06					23	45	$\infty 7$	$\alpha 1$
	17				$\infty 4$	$\alpha 2$	05	36
		24			67	01	$\alpha 3$	$\infty 5$
			35		$\alpha 0$	$\infty 6$	14	27
				$\alpha \infty$	15	37	26	04
$\alpha 4$	$\infty 3$	56	12	07				
$\infty 2$	$\alpha 5$	03	47	16				
13	46	$\alpha 7$	$\infty 0$	25				
57	02	$\infty 1$	$\alpha 6$	34				

Fig. 8. MESRS(9).

3. Graph theoretic aspects

We begin this section by defining a class of designs which is closely related to a class of BTD(n)s. An odd balanced tournament design, OBTD(n), is an $n \times (2n + 1)$ array of pairs defined on a $(2n + 1)$-set V such that

(i) each pair of distinct elements from V is contained in precisely one cell of the array,

(ii) each column of the array is a near resolution class,

(iii) each element of V is in at most 2 cells of each row.

We note that (iii) implies that each element occurs exactly twice in each row. Unlike BTD(n)s, it is a relatively simple task to construct OBTD(n)s for every positive integer n by using a patterned starter [38]. The method is illustrated in Fig. 9 where an OBTD(3) is displayed. The design is formed by developing column 1 through the integers modulo 7.

A near 1-factor of K_{2n+1} is a set of disjoint edges spanning $2n$ vertices of the complete graph. A near 1-factorization is a partition of K_{2n+1} into near 1-factors. Clearly, an OBTD(n) induces a near 1-factorization of K_{2n+1} with each column of the array giving a near 1-factor. The rows of the array determine 2-factors in the complete graph. If each row gives a 2-factor which is Hamiltonian cycle, then the OBTD(n) is called a Kotzig factorization of order $2n + 1$ ([4]). The existence question for Kotzig factorizations has been completely settled.

Theorem 3.1 (Colbourn and Mendelsohn [4], Horton [11]). *For each positive integer n, there exists a Kotzig factorization of order* $2n + 1$.

We now consider the analogue of Kotzig factorizations for BTD(n)s. Clearly, a row of a BTD(n) cannot give a Hamiltonian cycle in K_{2n} since there are precisely 2

16	27	31	42	53	64	75
25	36	47	51	62	73	14
34	45	56	67	71	12	23

Fig. 9. An OBTD(3).

12	13	58	37	47	28	46
34	57	14	26	25	36	18
56	24	67	48	38	17	35
78	68	23	15	16	45	27

Fig. 10. An HBTD(4).

vertices with degree one in the induced subgraph. It is possible that this subgraph could be a Hamiltonian path. If each row of a BTD(n) gives a Hamiltonian path in K_{2n}, then we call the design a Hamiltonian balanced tournament design and denote it by HBTD(n). The existence of HBTD(n)s is far from settled. An HBTD(1) trivially exists but an HBTD(2) and an HBTD(3) do not. The first non-trivial case is an HBTD(4). Recently, Corriveau [5] has done an exhaustive search and found that there are precisely 47 non-isomorphic BTD(4)s and, of these, exactly 18 are HBTD(4)s. It is interesting to note that of the 6 non-isomorphic 1-factorizations ([38]) of K_8 only 4 give rise to balanced tournament designs. Corriveau [5] has also shown that each of the 396 non-isomorphic 1-factorizations of K_{10} ([7]) gives rise to at least one BTD(5). At present there is no HBTD(n) known for $n \geq 5$. We display in Fig. 10 an example of an HBTD(4) from Corriveau's list.

We note that an HBTD(n) is a FBTD(n). The converse is false as the example in Fig. 11 illustrates. The deficient pair of row 4 is 78 which actually occurs as a pair in that row. Hence, the graph of this row must contain a component which is a path of length one.

The graph theoretic questions posed above can be generalized.

Let G be a spanning subgraph of K_{2n} (or K_{2n+1}). Is it possible to construct a BTD(n) (or an OBTD(n)) such that the graph associated with each row of the array is isomorphic to G? The question, of course, is open since even the case where G is a Hamiltonian path is not yet solved. For OBTD(n)s some interesting results do exist.

Theorem 3.2 (Colbourn and Mendelsohn [4]). *Let G be a spanning subgraph of K_{2n+1} which consists of disjoint triangles. There exists an* OBTD(n) *in which the graph of each row is isomorphic to G if and only if there exists a Kirkman triple system of order* $2n+1$.

The analogous result for BTD(n)s would have a spanning subgraph G of K_{2n}

12	57	14	36	28	38	47
34	68	58	27	45	17	26
56	13	67	48	37	25	18
78	24	23	15	16	46	35

Fig. 11. A FBTD(4).

which consists of $(2n-1)/3$ disjoint triangles and an edge. No general result is known. In fact, no example has been constructed yet. It is known ([5]) that such a design does not exist for $n = 4$. Of course, n must be congruent to 1 modulo 3 for this to be possible.

4. Balanced tournament designs and resolvable designs

Balanced tournament designs can be used to construct various types of resolvable and near resolvable balanced incomplete block designs (BIBDs). A (v, k, λ)-BIBD D is said to be resolvable (and denoted by (v, k, λ)-RBIBD if the blocks of D can be partitioned into classes $R_1, R_2, \ldots, R_t$ (resolution classes) where $t = (\lambda(v-1))/k - 1$ such that each element of D is contained in precisely one block of each class. A necessary condition for the existence of a (v, k, λ)-RBIBD is $v \equiv 0 \pmod k$. *A* (v, k, λ)-BIBD D is said to be near resolvable (and denoted by NR(v, k, λ)-BIBD) if the blocks of D can be partitioned into classes $R_1, R_2, \ldots, R_v$ (resolution classes) such that for each element of D there is precisely one class which does not contain x in any of its blocks and each class contains precisely $v-1$ distinct elements of the design. Necessary conditions for the existence of NR(v, k, λ)-BIBDs are $v \equiv 1 \pmod k$ and $\lambda = k - 1$.

In this section, we describe several constructions which use balanced tournament designs to produce $(v, 3, 2)$-BIBDs. We will use several well known existence results for designs with block size $k = 3$.

Theorem 4.1 (Hanani [9]). (i) *There exists a* $(v, 3, 2)$-RBIBD *if and only if* $v \equiv 0 \pmod 3$ and $v \neq 6$. (ii) *There exists a* $NR(v, 3, 2)$-BIBD *if and only if* $v \equiv 1 \pmod 3$, $v \geq 4$.

A resolvable $(v, 3, 1)$-BIBD is also known as a Kirkman triple system of order v and is denoted by KTS(v).

Theorem 4.2 (Ray-Chaudhuri and Wilson [30]). *There exists a* KTS(v) *if and only if* $v \equiv 3 \pmod 6$.

We will also use nearly Kirkman triple systems in one of our constructions. A nearly Kirkman triple system of order v (NKTS(v)) is a resolvable group divisible design with block size 3, group size 2 and index $\lambda = 1$ for pairs meeting distinct groups. Except for a few isolated cases the following result was proven by Baker and Wilson [1]. (See also [3, 12].)

Theorem 4.3 (Baker and Wilson [1]). *There exists a* NKTS(v) *if and only if* $v \equiv 0 \pmod 6$ *and* $v \neq 6$ *or* 12.

Balanced tournament designs and the designs described above can be used to construct $(v, 3, 2)$-RBIBDs containing various subconfigurations. These constructions are described in detail in [22]; for completeness, we include the proof of the first construction.

Theorem 4.4 (Lamken and Vanstone [22]). *If there exists a* BTD$(3n+1)$, *a* KTS$(6n+3)$ *and a* NR$(3n+1, 3, 2)$-BIBD, *then there exists a* $(9n+3, 3, 2)$-RBIBD.

Proof. Let $V_1 = \{x_1, x_2, \ldots, x_{3n+1}, y_1, y_2, \ldots, y_{3n+1}\}$ and let $V_2 = \{z_1, z_2, \ldots, z_{3n+1}\}$.

Let B' be the $3n+1 \times 6n+1$ array constructed from a BTD$(3n+1)$ defined on V_1. Suppose the deficient pair of elements for row i of B' is $\{x_i, y_i\}$ for $i = 1, 2, \ldots, 3n+1$. Let D' be a resolvable $(6n+3, 3, 1)$-BIBD defined on $V_1 \cup \{\infty\}$ so that the blocks containing ∞ are $\{\infty, x_i, y_i\}$ for $i = 1, 2, \ldots, 3n+1$. Let D_i' be the resolution class of D which contains the triple $\{\infty, x_i, y_i\}$ for $i = 1, 2, \ldots, 3n+1$. N will denote a NR$(3n+1, 3, 2)$-BIBD defined on V_2 and N_i will denote the resolution class of N which does not contain the element z_i.

We construct a resolvable $(9n+2, 3, 2)$-BIBD on $V_1 \cup V_2$ as follows. To each pair in row i of B' add the element z_i $(i = 1, 2, \ldots, 3n+1)$. Denote the resulting array of triples by B. Let $C_1, C_2, \ldots, C_{6n+1}$ be the columns of B. Replace each triple $\{\infty, x_i, y_i\}$ in D' with the triple $\{z_i, x_i, y_i\}$ for $i = 1, 2, \ldots, 3n+1$. D will denote the resulting configuration. Let D_i be the corresponding resolution class of D which contains the triple $\{z_i, x_i, y_i\}$ $(i = 1, 2, \ldots, 3n+1)$.

The triples of $B \cup D \cup N$ form a $(9n+3, 3, 2)$-BIBD. Every pair in V_1 occurs once in B and once in D. Every pair $\{z_i, v_i\}$ where $v_i \in V_1$ and $z_i \in V_2$ occurs twice in $B \cup D$. Every pair in V_2 occurs twice in N. It is easy to verify that $\{C_1, C_2, \ldots, C_{6n+1}, D_1 \cup N_1, D_2 \cup N_2, \ldots, D_{3n+1} \cup N_{3n+1}\}$ is a resolution for this $(9n+3, 3, 2)$-BIBD defined on $V_1 \cup V_2$. $\square$

Theorem 4.5 (Lamken and Vanstone [22]). *If there exists a* BTD$(3n)$, *a* NKTS$(6n)$ *and a* $(3n, 3, 2)$-RBIBD, *then there exists a* $(9n, 3, 2)$-RBIBD.

As noted above, the complete spectrum of $(v, 3, 2)$-RBIBDs was determined by Hanani [9]. The constructions used in the proofs of Theorems 4.4 and 4.5 provide several classes of these designs which contain various subconfigurations. In Section 5, we will show how these results can be generalized to construct resolvable $(v, k, k-1)$-BIBDs.

Before we generalize these results to use OBTDs and to construct doubly resolvable designs, we illustrate Theorem 4.4 with an example. A KTS(9) defined on the elements $V = \{1, 2, \ldots, \infty\}$ is displayed in Fig. 12. A BTD(4) defined on $V - \{\infty\}$ where the deficient pairs are the pairs which occur with ∞ in the KTS(9) is displayed in Fig. 12, and a NR$(4, 3, 2)$-BIBD defined on $W = \{a, b, c, d\}$ is

∞12	∞35	∞46	∞78
347	148	157	245
586	267	238	136

Fig. 12. A KTS(9).

displayed in Fig. 13. The design which is constructed from these designs is a (12, 3, 2)-RBIBD defined on $V \cup W$ and it appears in Fig. 14.

Similar constructions for NR(v, 3, 2)-BIBDs can be obtained from OBTD(n)s.

Theorem 4.6 (Lamken and Vanstone [22]). *If there exists an* OBTD($3n+1$), *a* KTS($6n+3$) *and a* NR($3n+1$, 3, 2)-BIBD, *then there is a* NR($9n+4$, 3, 2)-BIBD.

We note than an analogous result to Theorem 4.5 using OBTD(n)s would require a NR($6n+1$, 3, 1)-BIBD which cannot exist. As with (v, 3, 2)-RBIBDs, the spectrum of NR(v, 3, 2)-BIBDs was settled by Hanani [9]. Theorem 4.6 can also be generalized to provide near resolvable (v, k, $k-1$)-BIBDs [25].

Two interesting and useful applications of balanced tournament designs are found in constructions of doubly resolvable (v, 3, 2)-BIBDs or Kirkman squares and doubly near resolvable (v, 3, 2)-BIBDs [16].

A (v, k, λ)-BIBD is said to be doubly (near) resolvable if there exist two (near) resolutions R and R' of the blocks such that $|R_i \cap R'_j| \le 1$ for all $R_i \in R$, $R'_j \in R'$. (It should be noted that the blocks of the design are considered as being labeled so that if a subset of the elements occurs as a block more than once the blocks are treated as distinct.) The (near) resolutions R and R' are called orthogonal resolutions of the design. A doubly resolvable (v, k, λ)-BIBD is denoted by DR(v, k, λ)-BIBD and a doubly near resolvable (v, k, λ)-BIBD by DNR(v, k, λ)-BIBD.

A Kirkman square with block size k, order v and index λ, $\mathrm{KS}_k(v; 1, \lambda)$, is an $r \times r$ array K ($r = (\lambda(v-1))/k - 1$) defined on a v-set V such that

(i) each cell of K is either empty or contains a k-subset of V,

abc	abd	acd	bcd

Fig. 13. A NR(4, 3, 2)-BIBD.

a34	a56	a12	a78	a45	a67	a83
b16	b24	b35	b46	b28	b13	b57
c27	c18	c47	c15	c36	c48	c26
d58	d37	d68	d23	d17	d25	d14

a12	b78	c35	d46
347	245	148	157
586	136	267	238
bcd	acd	abd	abc

Fig. 14. A resolvable (12, 3, 2)-BIBD.

(ii) each element of V is contained in precisely one cell of each row and column of K,

(iii) the non-empty cells of K are the blocks of a (v, k, λ)-BIBD.

We can use a pair of orthogonal resolutions of a DR(v, k, λ)-BIBD to construct a $\mathrm{KS}_k(v; 1, \lambda)$. The rows of the array form one resolution of the DR(v, k, λ)-BIBD and the columns form an orthogonal resolution. Similarly, we can use a pair of orthogonal resolutions of a DNR(v, k, λ)-BIBD to construct a $v-1 \times v-1$ array. The rows of the array will form one resolution of the design and the columns will form an orthogonal resolution. If the DNR(v, k, λ)-BIBD has the additional property that under an appropriate ordering of the resolution classes of the orthogonal resolutions R and R', $R_i \cup R_i'$ contains precisely $v-1$ distinct elements of the design for all i, then the array is called a $(1, \lambda; k, v, 1)$-frame [16]. Note that the diagonal of a $(1, \lambda; k, v, 1)$-frame is empty and a unique element of the design can be associated with each cell (i, i). This distinction between $(1, \lambda; k, v, 1)$-frames and DNR(v, k, λ)-BIBDs is important in recursive constructions.)

In general, the spectrum of doubly resolvable and doubly near resolvable (v, k, λ)-BIBDs remains open. Although several infinite classes of DR(v, k, λ)-BIBDS are known for $k \geqslant 3$ [15], [37], the existence of DR(v, k, λ)-BIBDs has been settled only for $k=2$ and $\lambda=1$, [29]. (DR$(v, 2, 1)$-BIBDs are also called Room squares.) We should also note that the generalization of the Kirkman square defined above has been studied and we refer to [13], [14] for some of these results. We will use balanced tournament designs with additional properties to construct DR and DNR$(v, 3, 2)$-BIBDs. Progress has been made in the past few years in determining the spectrums of these designs. Surveys of these results can be found in [15]. In this paper, we are only interested in the constructions which use balanced tournament designs. We proceed to describe the additional properties of BTDs and OBTDs that we require.

Let B be an OBTD(n). Let $R_1, R_2, \ldots, R_n$ be the rows of B and let $C_1, C_2, \ldots, C_{2n+1}$ be the columns of B. $C=\{C_1, C_2, \ldots, C_{2n+1}\}$ is a near resolution of the underlying $(2n+1, 2, 1)$-BIBD. A resolution D, $D=\{D_1, D_2, \ldots, D_{2n+1}\}$ is called an orthogonal resolution to C if

(i) $|C_i \cap D_j| \leqslant 1$ for $1 \leqslant i, j \leqslant 2n+1$;

(ii) $|D_j \cap R_i| = 1$ for $1 \leqslant j \leqslant 2n+1$, $1 \leqslant i \leqslant n$.

If D exists, then we say that the OBTD(n) has a pair of orthogonal resolutions (ORs). With respect to these objects, the following existence result is known.

Theorem 4.7 (Lamken and Vanstone [23]). *Let n be a positive integer, $n \geqslant 3$ and $2n+1 \neq 3m$ where $(m, p)=1$ for p a prime less than 333. Then there is an OBTD(n) with a pair of orthogonal resolutions.*

A similar definition for a BTD(n) with a pair of orthogonal resolutions can be made but no non-trivial examples of these objects have been found to date. For BTD(n)s we make the following definition.

Let B be a BTD($n+1$). Let $R_1, R_2, \ldots, R_{n+1}$ be the rows of B and let $C_1, C_2, \ldots, C_{2n+1}$ be the columns of B. $C = \{C_1, C_2, \ldots, C_{2n+1}\}$ is the resolution of B. A resolution $D = \{D_1, D_2, \ldots, D_{2n+1}\}$ will be called almost orthogonal to C if

(i) $C_{2n+1} = D_{2n+1}$,

(ii) $|C_i \cap D_j| \leq 1$ for $1 \leq i, j \leq 2n$;

(iii) $|D_j \cap R_i| = 1$ for $1 \leq j \leq 2n$, $1 \leq i \leq n+1$.

If D exists, we say that B has a pair of almost orthogonal resolutions (denoted by AORs). If B is a BTD($n+1$) with a pair of almost orthogonal resolutions with the property that the deficient pairs of B are contained in the shared resolution class C_{2n+1}, then we say that B has property C'. Fig. 15 displays the smallest example of such an array.

Balanced tournament designs with AORs are more difficult to construct than OBTDs with ORs. Several infinite classes of these designs are known to exist and we refer to [27] for the descriptions of these classes. We include just one example of these results for BTDs with AORs.

Theorem 4.8 (Lamken and Vanstone [27]). *Let n be a positive integer, $n \neq 8$ or 33. There exists a* BTD(m) *with* AORs *for $m = 8n+3$ and $m = 16n+5$.*

Our constructions will also require the existence of $KS_3(v; 1, 1)$s with complementary $(1, 2; 3, (v-1)/2, 1)$-frames. We give a brief description of these designs and refer the interested reader to [24] for details.

Let K be a $KS_3(6n+3; 1, 1)$ defined on $V \cup \{\infty\}$ where ∞ occurs in each cell of the main diagonal ($|V| = 6n+2$). We say K has a complementary $(1, 2; 3, 3n+1, 1)$-frame (or a complementary DNR($3n+1$, 3, 2)-BIBD) if there exists a $(1, 2; 3, 3n+1, 1)$-frame (or a DNR($3n+1$, 3, 2)-BIBD) which can be written in the empty cells of K. Although the spectrum has not been determined for either $KS_3(v; 1, 1)$s or $(1, 2; 3, v, 1)$-frames, we can construct infinite classes of $KS_3(6n+3; 1, 1)$s with complementary $(1, 2; 3, 3n+1, 1)$-frames [24].

Theorem 4.9 (Lamken [24]). *Let i and j be nonnegative integers. There exists a* $KS_3(2n+1; 1, 1)$ *with a complementary* $(1, 2; 3, n, 1)$*-frame for* $n = 19^i 31^j$.

12	15	45	24	03
35	20	23	05	14
04	34	01	13	25

12	15	45	24	03
05	23	20	53	14
34	04	13	01	25

Fig. 15. A BTD(3) with AORs.

We can now state our constructions which use BTDs with AORs and OBTDs with ORs to produce DR(v, 3, 2)-BIBDs and DNR(v, 3, 2)-BIBDs respectively. These constructions are applied and the resulting classes of designs described in detail in [24].

Theorem 4.10 (Lamken and Vanstone [22]). *If there is a* BTD($3n + 1$) *with a pair of almost orthogonal resolutions and Property C' and if there is a* $KS_3(6n + 3; 1, 1)$ *with a complementary* $(1, 2; 3, 3n + 1, 1)$*-frame, then there is a* $KS_3(9n + 3; 1, 2)$ *or a* DR($9n + 3$, 3, 2)-BIBD.

Theorem 4.11 (Lamken and Vanstone [22]). *If there is an* OBTD($3n + 1$) *with a pair of orthogonal resolutions and a* $KS_3(6n + 3; 1, 1)$ *with a complementary* $(1, 2; 3, 3n + 1, 1)$*-frame, then there is a* DNR($9n + 4$, 3, 2)-BIBD.

We conclude this section by noting that the two smallest cases where these theorems can be applied are $n = 6$ and $n = 10$. Using Theorems 4.10 and 4.11, we can construct DR(v, 3, 2)-BIBDs for $v = 57$ and $v = 93$ and DNR(v, 3, 2)-BIBDs for $v = 58$ and $v = 93$ and DNR(v, 3, 2)-BIBDs for $v = 58$ and $v = 94$. These designs were not previously known to exist.

5. A generalization

In this section we consider a generalization of balanced tournament designs from pairs to k-subsets. We begin with a definition.

Definition 5.1. A generalized balanced tournament design, GBTD(n, k), defined on a kn-set V, is an arrangement of the blocks of a $(kn, k, k-1)$-BIBD defined on V into an $n \times (kn - 1)$ array such that
(1) every element of V is contained in precisely one cell of each column,
(2) every element of V is contained in at most k cells of each row.

Let G be a GBTD(n, k). An element which is contained in only $k - 1$ cells of row R_i of G is called a deficient element of R_i. It is easily seen that each row of G contains exactly k deficient elements. These elements are called the deficient k-tuple of row i. These deficient elements of row i need not occur in a common block of this row. The deficient k-tuples of G partition the points of this design. We illustrate the definition by displaying a GBTD(3, 3) in Fig. 16. The deficient triples of rows 1, 2 and 3 are respectively $\{4, 6, 8\}$, $\{1, 2, 9\}$, and $\{3, 5, 7\}$.

Let $C = (C_1, C_2, \ldots, C_n)^T$ where C_i, $1 \leqslant i \leqslant n$, is the deficient k-tuple of row R_i of G. If C occurs as a column in G $k - 1$ times, G is said to have property C. The GBTD(3, 3) displayed above does not have property C. A GBTD(4, 3) with a property C is illustrated in Fig. 17. Suppose the blocks in row R_i can be

129	349	569	145	357	178	238	267
357	167	138	236	468	245	749	589
468	258	247	789	129	369	165	134

Fig. 16. A GBTD(3, 3).

partitioned into k sets of n blocks each, $F_{i1}, F_{i2}, \ldots, F_{ik}$ so that every element in V occurs precisely once in F_{ij}, $1 \leq j \leq k-1$, and every element of V occurs precisely once in $F_{ik} \cup C_i$ for $1 \leq i \leq k$. A GBTD(n, k) with this property is called a factored generalized balanced tournament design and is denoted FGBTD(n, k) and each of $F_{i1}, F_{i2}, \ldots, F_{ik-1}$, $G_{ik} \cup C_i$ is called a factor of row R_i. The GBTD(4, 3) given above is factored with factors shown in Fig. 18.

We can now state a generalization of Theorem 1.4.

Theorem 5.1 (Lamken [25]). *If there exists an* FGBTD(n, k) *and if there exists k mutually orthogonal Latin squares of order kn, then there exists an* FGBTD(nk, k).

A number of other recursive constructions for GTBD(n, k)s exist (see [25]). These and existence results for GBTD(n, k)s can be found in [25].

We conclude this section by showing how the results of Section 4 can be generalized. Only two generalizations will be given to illustrate the ideas involved. For a complete description the reader is referred to [26].

Theorem 5.2 (Lamken [25]). *If there exists a* GBTD(n, k), *a* ($kn+1$, $k+1$, 1)-RBIBD *and a near resolvable* (n, $k+1$, k)-BIBD *then there is a* (($k+1$)n, $k+1$, k)-RBIBD.

This result generalizes Theorem 4.4. The next example (Fig. 19) shows how Theorem 5.2 can be used to construct a resolvable (20, 4, 3)-BIBD. Since a GBTD(5, 3) exists, a (16, 4, 1)-RBIBD exists and a near resolvable (5, 4, 3)-BIBD exists, then a resolvable (20, 4, 3)-BIBD exists.

We conclude this section with a generalization of Theorem 4.5. The theorem requires the existence of a $\mathrm{RGDD}_{n-1}(nk; k+1; k; 0, 1)$ which is a resolvable

FGJ	EIL	DHK	FHL	EGK	DIJ	FIK	DGL	EHJ	ABC	ABC
AIL	CHK	CIJ	BGJ	BHL	AGK	AHJ	BIK	CGL	DEF	DEF
BEK	BFJ	AEL	CDK	ADJ	CFL	BDL	CEJ	AFK	GHI	GHI
CDH	ADG	BFG	AEI	CFI	BEH	CEG	AFH	BDI	JKL	JKL

Fig. 17. A GBTD(4, 3) with property C.

Row 1:	ABC	FGJ	EIL	DHK
	ABC	FHL	EGK	DIJ
	ABC	FIK	DGL	EHJ
Row 2:	DEF	BIK	AHJ	CGL
	DEF	AIL	CHK	BGL
	DEF	CIJ	BHL	AGK
Row 3:	GHI	BEK	ADJ	CFL
	GHI	BFJ	AEL	CDK
	GHI	BDL	CEJ	AFK
Row 4:	JKL	CDH	BFG	AEI
	JKL	AFH	CEG	BDI
	JKL	BEH	CFI	ADG

Fig. 18. Factors of a GBTD(4, 3).

group divisible design having nk elements, group size k, block size $k+1$, replication number $n-1$ and pair balance 1 for pairs formed from elements in distinct groups and pair balance 0 otherwise.

Theorem 5.3 (Lamken [26]). *If there exists a* GBTD(n, k), *a* RGDD$_{n-1}(nk; k+1; k; 0, 1)$ *and a* $(n, k+1, k)$-RBIBD, *then there exists a* $(kn+n, k+1, k)$-RBIBD.

Proof. Let $D_i = \{x_{i1}, x_{i2}, \ldots, x_{ik}\}$, $1 \leq i \leq n$, $V_1 = \bigcup_{i=1}^{n} D_i$ and $V_2 = \{y_1, y_2, \ldots, y_n\}$.

Let G' be a GBTD(n, k) defined on V_1 such that the deficient k-tuple of row i is D_i. Let D be a RGDD$_{n-1}(nk; k+1; k; 0, 1)$ defined on V_1 so that the groups of D are D_i, $1 \leq i \leq n$. Let $R_1, R_2, \ldots, R_{n-1}$ be the resolution classes of D. Let N be a $(n, k+1, k)$-RBIBD defined on V_2. We let $N_1, N_2, \ldots, N_{n-1}$ denote the resolution classes of N.

A $(kn+n, k+1, k)$-RBIBD can be constructed as follows. To each block in row i of G' add the element y_i, $1 \leq i \leq n$. Denote the resulting array of blocks of size $k+1$ by G. Let $C_1, C_2, \ldots, C_{nk-1}$ be the columns of G. Let $C_{nk} = \{D_i \cup \{y_i\}: 1 \leq i \leq n\}$. The blocks in $G \cup D \cup N \cup C_{nk}$ form a $(kn+n, k+1, k)$-BIBD. Every distinct pair in V_1 occurs $k-1$ times in G and once in $D \cup C_{nk}$. Every pair

2 3 4	β 2 8	α 8 11	γ 11 2	6 7 8	β 6 0	α 0 3	γ 3 6	10 11 0	β 10 4	α 4 7	γ 7 10	1 5 9	1 5 9
γ 8 11	3 4 5	β 3 9	α 9 0	γ 0 3	7 8 9	β 7 1	α 1 4	γ 4 7	11 0 1	β 11 5	α 5 8	2 6 10	2 6 10
α 6 9	γ 9 0	4 5 6	β 4 10	α 10 1	γ 1 4	8 9 10	β 8 2	α 2 5	γ 5 8	0 1 2	β 0 6	3 7 11	3 7 11
β 1 7	α 7 10	γ 10 1	5 6 7	β 5 11	α 11 2	γ 2 5	9 10 11	β 9 3	α 3 6	γ 6 9	1 2 3	4 8 0	4 8 0
0 5 10	1 6 11	2 7 0	3 8 1	4 9 2	5 10 3	6 11 4	7 0 5	8 1 6	9 2 7	10 3 8	11 4 9	$\alpha\beta\gamma$	$\alpha\beta\gamma$

Fig. 19. A GBTD(5, 3).

$\{y_i, x_{jl}\}$ occurs k times in $G \cup C_{nk}$. Every pair in V_2 occurs k times in N. It is easy to verify that $\{C_1, C_2, \ldots, C_{nk}, D_1 \cup N_1, D_2 \cup N_2, \ldots, D_{n-1} \cup N_{n-1}\}$ is a resolution for this $(kn+n, k+1, k)$-BIBD defined on $V_1 \cup V_2$. This completes the proof. □

The following is an example of this construction. Since a GBTD(8, 3) exists [25], a $\mathrm{RGDD}_7(24; 4; 3; 0, 1)$ exists [34] and a (8, 4, 3)-RBIBD is easily constructed, then Theorem 5.3 establishes the existence of a (32, 4, 3)-RBIBD.

References

[1] R.D. Baker and R.M. Wilson, Nearly Kirkman triple systems, Utilitas Math. 11 (1977) 289–296.

[2] R.C. Bose, S.S. Shrikhande and E.T. Parker, Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjuecture, Can. J. Math. 12 (1960) 189–203.

[3] A.E. Brouwer, Two new nearly Kirkman triple systems, Utilitas Math. 13 (1978) 311–314.

[4] C. Colbourn and E. Mendelsohn, Kotzig factorizations: existence and computational results, Annals Discrete Math. 12 (1982) 65–78.

[5] J. Corriveau Ars Combinatoria (to appear).

[6] R. Fujihara and S.A. Vanstone, The existence of orthogonal resolutions of lines in AG(n, q), J. Comb. Theory (A) 45 (1987) 139–147.

[7] E.N. Gelling, On one-factorizations of the complete graph and the relationship to round robin schedules, M.Sc. Thesis, University of Victoria, 1973.

[8] E.N. Gelling and R.E. Odeh, On 1-factorizations of the complete graph and the relationship to round robin schedules, Proc. Third Manitoba Conference on Numerical Math., Winnipeg (1973) 213–221.

[9] H. Hanani, On resolvable balanced incomplete block designs, J. Comb. Theory (A) 17 (1974) 275–289.

[10] J. Haselgrove and J. Leech, A tournament design problem, Amer. Math. Monthly 8 (1977) 198–201.

[11] J.D. Horton, The constructions of Kotzig factorizations, Discrete Math. 43 (1983) 199–206.

[12] A. Kotzig and A. Rosa, Nearly Kirkman systems Proc. 5th Southeastern Conf. Combinatorics, Graph Theory and Computing, *Congressus Numerantium* X (1974) 607–614.

[13] E.R. Lamken and S.A. Vanstone, The existence of $KS(v; \mu, \lambda)$: Main constructions, Utilitas Math. 27 (1985), 111–130.

[14] E.R. Lamken and S.A. Vanstone, The existence of $KS_2(v; \mu, \lambda)$: Special constructions, Utilitas Math. 27 (1985), 131–155.

[15] E.R. Lamken and S.A. Vanstone, The existence of a class of Kirkman squares of index 2, J. Australian Math. Soc. (Ser. A) 44 (1988) 33–44.

[16] E.R. Lamken and S.A. Vanstone, Existence results for doubly near resolvable (v, 3, 2)-BIBDs (submitted).

[17] E.R. Lamken and S.A. Vanstone, The existence of factored balanced tournament designs, Ars Combinatoria 19 (1985) 157–160.

[18] E.R. Lamken and S.A. Vanstone, The existence of partitioned balanced tournament designs of side $4n+1$, Ars Combinatoria 20 (1985) 29–44.

[19] E.R. Lamken and S.A. Vanstone, The existence of partitioned balanced tournament designs of side $4n+3$, Annals Discrete Math. 34 (1987) 319–338.

[20] E.R. Lamken and S.A. Vanstone, The existence of partitioned balanced tournament designs, Annals Discrete Math. 34 (1987) 339–352.

[21] E.R. Lamken, A note on partitioned balanced tournament designs, Ars Combinatoria 24 (1987) 5–16.

[22] E.R. Lamken and S.A. Vanstone, Balanced tournament designs and resolvable $(v, 3, 2)$-BIBDs, Discrete Math. (to appear).
[23] E.R. Lamken and S.A. Vanstone, Orthogonal resolutions in odd balanced tournament designs, Graphs and Combinatorics 4 (1988) 244–255.
[24] E.R. Lamken, On classes of doubly resolvable $(v, 3, 2)$-BIBDs from balanced tournament designs, Ars Combinatoria 24 (1987) 85–91.
[25] E.R. Lamken, A generalization of balanced tournament designs (in preparation).
[26] E.R. Lamken, Constructions for generalized balanced tournament designs (in preparation).
[27] E.R. Lamken and S.A. Vanstone, Balanced tournament designs with almost orthogonal resolutions (preprint).
[28] E. Mendelsohn and A. Rosa, One-factorizations of the complete graph – a survey, J Graph Theory 9 (1985) 43–65.
[29] R.C. Mullin and W.D. Wallis, The existence of Room squares, Aequationes Math. 1 (1975) 1–7.
[30] D.K. Ray-Chaudhuri and R.M. Wilson, Solution of Kirkman's schoolgirl problem, Proc. Symp. Pure Math. 19 (1971) 187–203.
[31] A. Rosa and D.R. Stinson, One-factorizations of regular graphs and Howell designs of small order, Utilitas Math. 29 (1986) 99–124.
[32] A. Rosa and S.A. Vanstone, Starter-adder techniques for Kirkman squares and Kirkman cubes of small sides, Ars Combinatoria 14 (1982) 199–212.
[33] P.J. Schellenberg, G.H.J. van Rees and S.A. Vanstone, The existence of balanced tournament designs, Ars Combinatoria 3 (1977) 303–318.
[34] P. Smith, A doubly divisible nearly Kirkman system, Discrete Math. 18 (1977) 93–96.
[35] D.R. Stinson, Some classes of frames and the spectrum of skew Room squares and Howell designs, Ph.D. Thesis, University of Waterloo, 1981.
[36] D.R. Stinson, Room squares with maximum empty subarrays, Ars Combinatoria 20 (1985) 159–166.
[37] S.A. Vanstone, Doubly resolvable designs, Discrete Math. 29 (1980) 77–86.
[38] W.D. Wallis, Anne Penfold Street, and Jennifer Seberry Wallis, Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices, Springer-Verlag Lecture Notes No. 292 (1972).

Discrete Mathematics 77 (1989) 177–189
North-Holland

AUTOMORPHISMS OF 2-(22, 8, 4) DESIGNS

I. LANDGEV and V.D. TONCHEV*
Institute of Mathematics, Sofia 1090, P.O. Box 373, Bulgaria and Department of Mathematics and Computing Science, University of Technology, Eindhoven, The Netherlands

Dedicated to Professor Haim Hanani on the occasion of his 75th birthday.

It is shown that a 2-(22, 8, 4) design cannot possess any nontrivial automorphisms of an odd order.

1. Introduction

The smallest, with respect to the number of points or blocks, parameter set for a balanced incomplete block design, i.e. a 2-(v, k, λ) design, for which the existence question is still unsolved, is 2-(22, 8, 4), i.e. $v = 22$, $b = 33$, $r = 12$, $k = 8$, $\lambda = 4$. This is the smallest case left open in Table 5.23 of the remarkable Hanani's article [7]. Many of the open problems from that table have been resolved during the last decade, some of then by Professor Hanani himself (cf. Mathon and Rosa [11]). However, the existence of the smallest and most challenging 2-(22, 8, 4) design is still in doubt.

In this paper we investigate possible automorphism groups of a design with such parameters and show that if one exists, its full automorphism group must be either a 2-group, or trivial. Our method is based on examination of possible orbit structures of cyclic automorphism groups of a prime order by use of tactical decompositions.

An essential case of automorphisms of order 3 fixing exactly one point has been recently investigated by Kapralov [9], who found all (exactly 53) possible orbit structures and showed (partially by computer) that none of those yields a design. We show in this paper that for an odd prime order automorphism of any other type, there is no possible orbit structure at all. Our proof does not involve any computer computations.

2. Preliminaries

We asssume that the reader is familiar with the basic notions and facts from design theory (cf. e.g. [3, 4, 5, 8, 13]).

* On leave from the University of Sofia, Bulgaria.

As usual, the total number of blocks in a 2-(v, k, λ) design is denoted by b, and the number of blocks containing a given point – by r.

The following easily checked statement is a variation of a similar but stronger result for symmetric 2-designs (cf. [1]).

Lemma 2.1. *If p is a prime being an order of an automorphism of a* 2-(v, k, λ) *design with $v > k$, then either p divides v or $p \leq r$.*

Applied for the parameters 2-(22, 8, 4), this gives as a corollary the following

Lemma 2.2. *The only primes which might be orders of automorphisms of a* 2-(22, 8, 4) *design, are* 2, 3, 5, 7 *or* 11.

The next result is a special case of Theorem 1.46 from [8] (see also [3, Th. 4, 17]).

Lemma 2.3. *If v' (resp. b') is the number of point (resp. block) orbits of a nontrivial* 2-(v, k, λ) *design with respect to a given automorphism group, then*

$$0 \leq b' - v' \leq b - v.$$

In the sequal we shall use frequently the following result due to Hamada and Kobayashi [6]:

Lemma 2.4. *Any two blocks in a* 2-(22, 8, 4) *design can have at most* 4 *common points. More precisely, if n_i denotes the number of blocks intersecting a given block in exactly i points, then there are* 4 *possible types of blocks according to their block intersection numbers* (*Table* 1).

Given a design D with an automorphism group G, the orbit matrix $M = (m_{ij})$ of D with respect to G is defined as a matrix whose rows and columns are indexed by the point and block orbits of D under G respectively, where m_{ij} is the number of points from the ith point orbit contained in a block from the jth block orbit. In other words, M is a matrix corresponding to the tactical decomposition of D defined by the action of G.

Let r_j (resp. k_i) denote the length of the jth block (resp. ith point) orbit, and let

Table 1. Block intersection numbers of a 2-(22, 8, 4) design.

Type	n_0	n_1	n_2	n_3	n_4
1	0	0	12	16	4
2	0	1	9	19	3
3	0	2	6	22	2
4	1	0	6	24	1

b' (resp. v') be the total number of block orbits. In this notation, the orbit matrix M satisfies the following equations:

$$\sum_{j=1}^{b'} r_j m_{ij} = k_i r, \quad 1 \leq i \leq v', \tag{2.1}$$

$$\sum_{j=1}^{b'} r_j m_{ij}(m_{ij} - 1) = k_i(k_i - 1)\lambda, \quad 1 \leq i \leq v', \tag{2.2}$$

$$\sum_{j=1}^{b'} r_j m_{cj} m_{dj} = k_c k_d \lambda \quad \text{for } c \neq d. \tag{2.3}$$

If G is a cyclic group of a prime order p then any orbit length is either p or 1. In particular, considering a nontrivial (i.e. of length p) point orbit and denoting by $s = s_i$ the number of blocks fixed by G and containing all points from that (ith) orbit, equations (2.1)–(2.3) reduce to the following:

$$\sum_{j:r_j=p} m_{ij} = r - s_i, \tag{2.4}$$

$$\sum_{j:r_j=p} m_{ij}(m_{ij} - 1) = (p - 1)(\lambda - s_i), \tag{2.5}$$

$$\sum_{j:r_j=p} m_{cj} m_{dj} = p(\lambda - s_{cd}), \quad (c \neq d), \tag{2.6}$$

where s_{cd} denotes the number of fixed blocks containing the cth and dth point orbit. Combined with (2.4), (2.5) gives also

$$\sum_{j:r_j=p} m_{ij}^2 = p(\lambda - s_i) + r - \lambda. \tag{2.7}$$

An evident necessary condition for the existence of a design with a given automorphism group is the existence of an integral matrix $M = (m_{ij})$ satisfying the above system of equations.

3. Automorphisms of order 11

According to Lemma 2.2, the largest prime which can possibly be an order of an automorphism of a 2-(22, 8, 4) design, is 11.

The impossibility of an automorphism without fixed points has been mentioned by Baartmans and Danhof [2]: the system of Equations (2.4)–(2.6) then has no solution.

Suppose f is an automorphism of order 11 fixing 11 points. Then by Lemma 2.3 f must fix at least 11 blocks. Any two blocks fixed by f must consist entirely of points fixed by f and hence they have at least 5 common points, a contradiction to Lemma 2.4.

4. Automorphisms of order 7

Since $b = 33 \equiv 5 \pmod 7$, an automorphism of order 7 must fix at least 5 blocks. Since a point orbit of length 7 can be contained in at most one fixed block (by Lemma 2.4), this rules out immediately an automorphism fixing 1 or 8 points. If there are 15 fixed points then by Lemma 2.3 there have to be at most 2 blocks orbits of length 7. However, the corresponding system (2.4)–(2.7) has no solution for $p = 7$ and $s_i < 2$.

5. Automorphisms of order 5

Since $b = 33 \equiv 3 \pmod 5$, there must be at least 3 fixed blocks. According to Lemma 2.4, a point orbit of length 5 can be contained in at most one fixed block. The only (up to permutation) solutions of (2.4)–(2.7) for $p = 5$ and $s_i < 2$ are $(1,1,2,2,3,3)$ $(s_i = 0)$ and $(1,1,2,2,2,3)$ $(s_i = 1)$. Therefore, there are 3 fixed blocks, whence by Lemma 2.3 there are only 2 fixed points. However, a fixed block must contain at least 3 fixed points, a contradiction.

6. Automorphisms of order 3

The following lemma gives an upper bound for the number of blocks fixed by an automorphism of order 3.

Lemma 6.1. *An automorphism of order* 3 *of a* 2-(v, k, λ) *design can fix at most* $b - 3r + 3\lambda$ *blocks.*

Proof. Let S be a point orbit of length 3 and let n_i be the number of blocks containing exactly i points from S. Evidently

$$\begin{aligned} n_0 + n_1 + n_2 + n_3 &= b, \\ n_1 + 2n_2 + 3n_3 &= 3r, \\ n_2 + 3n_3 &= 3\lambda. \end{aligned}$$

Since each fixed block contains either 3 or none points from S, the total number of fixed blocks does not exceed

$$n_0 + n_3 = b - 3(r - \lambda). \quad \square$$

Corollary 6.2. *An automorphism of order* 3 *of a* 2-(22, 8, 4) *design fixes at most* 9 *blocks.*

Lemma 6.3. *Given a* 2-(22, 8, 4) *design* D *with an automorphism* f *of order* 3, *and* *a block B not fixed by f, there are at least 4 point orbits of length 3 intersecting B in either 1 or 2 points.*

Proof. Let B be a block not fixed by f. Denote by t the number of points fixed by f and contained in B, and let m_i $(i = 1, 2, 3)$ denote the number of point orbits of length 3 intersecting B in exactly i points. Evidently

$$t + m_1 + 2m_2 + 3m_3 = 8. \tag{6.1}$$

On the other hand,

$$|B \cap Bf| = t + m_2 + 3m_3 \leq 4,$$

whence

$$m_1 + m_2 \geq 4.$$

In particular, there are at least 4 point orbits of length 3. □

Corollary 6.4. *An automorphism of order 3 of a 2-(22, 8, 4) design fixes at most 10 points.*

As we have already mentioned, the nonexistence of a 2-(22, 8, 4) design with an automorphism of order 3 fixed exactly 1 point has been proved by Kapralov [9]. Thus we have to consider automorphisms fixing 4, 7 or 10 points.

Lemma 6.5. *If an automorphism of order 3 of a 2-(22, 8, 4) design fixes more than 1 point then each fixed point is contained in at least 3 fixed blocks.*

Proof. Since $r = 12 \equiv 0 \pmod 3$, the number of fixed blocks through a fixed point is a multiple of 3. Any pair of fixed points is contained in $4 \equiv 1 \pmod 3$ blocks, hence one or all of these 4 blocks must be fixed. Thus each fixed point occurs in a fixed block, and consequently, in at least 3 fixed blocks. □

Suppose that D is a 2-(22, 8, 4) design with an automorphism f of order 3. The orbit matrix M with respect to the cyclic group generated by f can be presented in the following form

$$M = \begin{vmatrix} T & U \\ V & W \end{vmatrix}, \tag{6.3}$$

where $T = (t_{ij})$ has rows and columns indexed by the fixed points and blocks; $U = (u_{ij})$ has rows indexed by fixed points and columns indexed by nontrivial block orbits; $V = (v_{ij})$ has rows indexed by nontrivial point orbits and columns by fixed blocks; and $W = (w_{ij})$ has rows and columns indexed by nontrivial point and block orbits.

7. Automorphisms of order 3 fixing 10 points

In this case there are exactly 4 point orbits of length 3, i.e. the matrix (V, W) from (6.3) has exactly 4 rows. By Lemma 6.3 each entry of W is either 1 or 2.

Suppose that there are x fixed blocks, and hence $y = (33 - x)/3$ blocks orbits of length 3. Let $(v_{i1}, \ldots, v_{ix}, w_{i1}, \ldots, w_{iy})$ be a row of (V, W), and denote by q_j (resp. p_j) the number of entries among $v_{i1}, \ldots, v_{ix}$ (resp. $w_{i1}, \ldots, w_{iy}$) equal to j $(0 \leq j \leq 3)$. Clearly

$$\begin{aligned} q_3 + 2p_2 + p_1 &= 12, \\ q_3 + \ \ p_2 \qquad &= 4, \\ p_2 + p_1 &= y, \end{aligned}$$

whence $y = 8$, and $x = 9$, i.e. there are exactly 9 fixed blocks.

Equations (2.4)–(2.7) now give the following possibilities for the rows of (V, W) (Table 2):

Table 2. Rows of (V, W).

Type	V									W							
i	0	0	0	0	0	0	0	0	0	2	2	2	2	1	1	1	1
ii	3	0	0	0	0	0	0	0	0	2	2	2	1	1	1	1	1
iii	3	3	0	0	0	0	0	0	0	2	2	1	1	1	1	1	1
iv	3	3	3	0	0	0	0	0	0	2	1	1	1	1	1	1	1
v	3	3	3	3	0	0	0	0	0	1	1	1	1	1	1	1	1

By equation (2.6) and Lemma 2.4 the scalar product of pair of rows of W must be either 9 or 12. This is possible only for pairs of rows of the following types: (i, v), (ii, iv), (iii, iii), (iii, iv), (iv, v). This excludes rows of type i or v. Furthermore, there is at most one row of type iv, and such a row can be combined with at most 2 rows of type iii; hence a row of type iv is also excluded. Eventually, up to permutation of rows and columns, (V, W) looks as follows:

$$(V, W) = \begin{vmatrix} 3 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 3 & 3 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 3 & 3 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 2 & 2 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 3 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 \end{vmatrix}.$$

Hence there are 8 fixed blocks each containing 5 fixed points, one fixed block (say B) consisting entirely of fixed points, and each nonfixed block contains 3 fixed points. Let P be a fixed point belonging to B. Denote by R_1 the number of fixed blocks other than B and containing P, and let R_2 be the number of nonfixed blocks containing P. Counting in two ways the number of blocks containing P and another fixed point, one gets:

$$7 + 4R_1 + 2R_2 = 9 \cdot 4,$$

a contradiction.

Therefore, there is no design with an automorphism of order 3 fixing 10 points.

8. Automorphisms of order 3 fixing 7 points

The number of point orbits is now 12, hence by Lemma 2.3 and Corollary 6.2 there are 3, 6 or 9 fixed blocks.

Each fixed block contains 2 or 5 fixed points. By Lemma 6.5 each fixed point is contained in at least 3 fixed blocks. If there are only 3 fixed blocks then each of the 7 fixed points must belong to each of the 3 fixed blocks, which contradicts to Lemma 2.4. Hence there are 6 or 9 fixed blocks.

Assume that there are exactly 6 fixed blocks. Denote by n_2 (resp. n_5) the number of blocks containing exactly 2 (resp. 5) fixed points. Evidently

$$n_2 + n_5 = 6,$$

and since each fixed point is contained in at least 3 fixed blocks (Lemma 6.5), we have also

$$2n_2 + 5n_5 \geqslant 7 \cdot 3,$$

whence $n_5 \geqslant 3$.

Two fixed blocks, each containing 5 fixed points, must intersect in at least 3 fixed points. Each pair of such a triple of points is contained in at least 2, and hence in exactly 4 fixed blocks. Therefore, each point of such a triple occurs in at least 4 fixed blocks, hence by the proof of Lemma 6.5 in at least 6 fixed blocks, i.e. in all fixed blocks, which leads to a contradiction with $\lambda = 4$.

Therefore, there must be exactly 9 fixed blocks.

Proceeding as in the case of 10 fixed points (Section 7), it can be seen that the matrix (V, W) must consist of 5 rows of type iii (cf. Table 2). However, it is readily seen that the matrix (7.1) cannot be extended with a 5th row of type iii so that the scalar product of each pair of rows to be either 9 or 12.

9. Automorphisms of order 3 fixing 4 points

In this case a fixed block must consist of 2 fixed points and 2 point orbits of length 3. Each pair of fixed points is contained in 4 blocks, either one or all of them being fixed. However, if there is a pair of fixed points contained in 4 fixed blocks then some pair of these 4 blocks must have at least 5 common points, in conflict with Lemma 2.4. Thus each pair of fixed points is contained in precisely one fixed block, and hence there are exactly 6 fixed blocks.

In the notation of (6.3), the matrix T now is an incidence matrix of the trivial 2-(4, 2, 1) design, e.g.

$$T=\begin{vmatrix}1&1&1&0&0&0\\1&0&0&1&1&0\\0&1&0&1&0&1\\0&0&1&0&1&1\end{vmatrix}. \tag{9.1}$$

Up to permutation of rows and columns there are 3 possibilities for the matrix U:

$$U=\begin{vmatrix}1&1&1&0&0&0&0&0&0\\1&0&0&1&1&0&0&0&0\\1&0&0&0&0&1&1&0&0\\1&0&0&0&0&0&0&1&1\end{vmatrix}. \tag{9.2}$$

$$U=\begin{vmatrix}1&1&1&0&0&0&0&0&0\\1&0&0&1&1&0&0&0&0\\1&0&0&0&0&1&1&0&0\\0&1&0&1&0&1&0&0&0\end{vmatrix}. \tag{9.3}$$

$$U=\begin{vmatrix}1&1&1&0&0&0&0&0&0\\1&0&0&1&1&0&0&0&0\\0&1&0&1&0&1&0&0&0\\0&0&1&0&1&1&0&0&0\end{vmatrix}. \tag{9.4}$$

Equations (2.4)–(2.7) give the following possibilities for rows of (V, W) (Table 3):

Lemma 9.1. *There is no design with a matrix U of the form* (9.2).

Proof. Assume that U has the form (9.2). Then by Lemma 6.3 each block from the only block orbit of length 3 containing 4 fixed points must contain at most one point from a point orbit of length 3. Thus the orbit matrix M has the following

Table 3. Rows of (V, W).

Type	V						W								
i	0	0	0	0	0	0	2	2	2	2	1	1	1	1	0
ii	3	0	0	0	0	0	2	2	2	1	1	1	1	1	0
iii	3	3	0	0	0	0	2	2	1	1	1	1	1	1	0
iv	0	0	0	0	0	0	2	1	1	1	1	1	1	1	3
v	3	3	3	0	0	0	2	1	1	1	1	1	1	1	0
vi	3	0	0	0	0	0	1	1	1	1	1	1	1	1	3
vii	3	3	3	3	0	0	1	1	1	1	1	1	1	1	0

form:

$$M=\left|\begin{array}{cccccccccccccccc}
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
 & & & & & & 0 & & & & & & & & \\
 & & & & & & 0 & & & & & & & & \\
 & & & * & & & 1 & & & & * & & & & \\
 & & & & & & 1 & & & & & & & & \\
 & & & & & & 1 & & & & & & & & \\
 & & & & & & 1 & & & & & & & &
\end{array}\right|. \tag{9.5}$$

Hence the first two rows of the submatrix W of (9.5) contain a common zero coordinate, and therefore, such a row cannot be of type iv or vi. Since the scalar product of two rows of W must be either 9 or 12, the first two rows can be of the following types; (i, vii), (ii, v), (iii, iii), (iii, v), (v, vii). The scalar product of a row of (V, W) after replacing each entry 3 in V by 1 with each row of (T, U) must be equal to 4. This is not possible if one of the first two rows of W is of type i, ii, iii, iv, or v. This completes the proof. □

In general, if $(t_{i1}, \ldots, t_{i6}, u_{i1}, \ldots, u_{i9})$, $1 \leq i \leq 4$ are the rows of (T, U), then any row $(v_1, \ldots, v_6, w_1, \ldots, w_9)$ of (V, W) must satisfy the following equations (cf. (2.6)):

$$\sum_{j=1}^{6} v_j t_{ij} + 3 \sum_{j=1}^{9} w_j u_{ij} = 12, \quad i = 1, 2, 3, 4.$$

Any solution of (9.6) must be of type i–vii (Table 3).

Lemma 9.2. *If U is of the form* (9.3) *or* (9.4), *then there is no row of (V, W) of type* iv, vi, *or* vii.

Proof. Assume that U has the form (9.3). Then the system of Equations (9.6) looks as follows:

$$\begin{array}{l}
v_1 + v_2 + v_3 + 3w_1 + 3w_2 + 3w_3 = 12, \\
v_1 + v_4 + v_5 + 3w_1 + 3w_4 + 3w_5 = 12, \\
v_2 + v_4 + v_6 + 3w_1 + 3w_6 + 3w_7 = 12, \\
v_3 + v_5 + v_6 + 3w_2 + 3w_4 + 3w_6 = 12.
\end{array}$$

If some $w_i = 3$ then there should be some $w_j = 0$. Hence a solution of type iv or vi is not possible.

Assume now that there is a solution of type vii. Up to permutation, there are only two possibilities: $v_1 = \cdots = v_4 = 3$, $v_5 = v_6 = 0$; or $v_1 = v_6 = 0$, $v_2 = \cdots = v_5 = 3$ (cf. (9.1)). In the first case two of w_1, w_2, w_3 must be zero, a contradiction (see Table 3). In the second case, if $w_1 = 1$ then one of w_2 or w_3, as well as one of w_4 or w_5 must be zero, a contradiction; if $w_1 = 0$, then the first 3 equations imply $w_2 = \cdots = w_7 = 1$, whence the 4th equation is violated.

The case when U has the form (9.4) is treated similarly; the system of Equations (9.6) again does not admit any solution of type iv, vi or vii. □

Using the fact that the matrix V contains 12 entries equal to 3 and 24 zeros, Lemmas 9.1, 9.2 and Eq. (2.4–2.7) imply the following

Lemma 9.3. *There are* 6 *possibilities for the types of the rows of the matrix* (V, W):

$$1(\mathrm{i}) + 1(\mathrm{ii}) + 1(\mathrm{iii}) + 3(\mathrm{v}), \tag{9.7}$$

$$3(\mathrm{ii}) + 3(\mathrm{v}), \tag{9.8}$$

$$1(\mathrm{i}) + 3(\mathrm{iii}) + 2(\mathrm{v}), \tag{9.9}$$

$$2(\mathrm{ii}) + 2(\mathrm{iii}) + 2(\mathrm{v}), \tag{9.10}$$

$$1(\mathrm{ii}) + 4(\mathrm{iii}) + 1(\mathrm{v}), \tag{9.11}$$

$$6(\mathrm{iii}). \tag{9.12}$$

Here $a(b)$ means a rows of type b.

Let us now consider the incidence structure F with "points" the 6 nontrivial point orbits and "blocks" the 6 fixed blocks. Each block of F consists of a pair of points and (by Lemma 2.4) there are no repeated blocks. Hence F is a collection of 6 distinct 2-subsets of a given 6-set, or equivalently, F is a 6-subset of the set of all 15 2-subsets of the point set. The set of all such $\binom{15}{6}$ 6-subsets is divided into 21 orbits under the action of the symmetric group of degree 6 on the point set (cf. e.g. Kramer and Mesner [10]). Thus there are at most 21 possible configurations for F. By Lemmas 9.1 and 9.2 each point of F occurs in at most 3 blocks, which reduces the possibilities from 21 to 14.

Let us define a graph G with vertices the points of F and edges the blocks of F. By definition G has 6 vertices and 6 edges. Using Equations (2.4)–(2.7), the possible types of rows of (V, W) (Table 3), and Lemmas 6.3, 9.1, 9.2, 9.3, it can be seen that the graph G must possess the following properties:

9.4. Each vertex is of degree at most 3.

9.5. A vertex of degree 0, 1, 2 or 3 corresponds to a row of (V, W) of type i, ii, iii, or v respectively.

9.6. Two vertices of degree 3 are necessarily adjacent.

9.7. Any vertex of degree 1 is adjacent to a vertex of degree 3.

9.8. A vertex of degree 3 is adjacent to at most one vertex of degree 1.

9.9. A triple of vertices of degree 2 cannot form a complete graph of size 3.

9.10. Given a vertex P of degree 3, there is at most one vertex of degree 2 nonadjacent to P.

9.11. If G contains a pair of adjacent vertices of degree 1 and 3 respectively, then there is no vertex of degree 0 in G.

9.12. The scalar product of two rows of W corresponding to a pair of adjacent (resp. nonadjacent) vertices of G is 9 (resp. 12).

The properties 9.4–9.12 reduce the possible configurations for F to the following 4 ones:

$$F_1 = \{12, 13, 14, 23, 25, 45\},$$

$$F_2 = \{12, 16, 23, 34, 45, 56\},$$

$$F_3 = \{12, 14, 15, 23, 26, 34\},$$

$$F_4 = \{12, 13, 14, 23, 25, 36\}.$$

Using 9.12, it is straightforward to check that (up to permutation of rows and columns) a triple of rows of (V, W) of type iii corresponding to 3 vertices of G of degree 2, two adjacent and the third nonadjacent to any of them, looks as follows:

$$\begin{array}{ccccccccccccccc}
3 & 3 & 0 & 0 & 0 & 0 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
3 & 0 & 3 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 2 \\
0 & 0 & 0 & 3 & 3 & 0 & 1 & 2 & 0 & 1 & 1 & 1 & 1 & 2 & 1.
\end{array} \tag{9.13}$$

The matrix (9.13) cannot be extended by a row of type i. This eliminates F_1.

Similarly, the matrix (9.13) cannot be extended by a row of type iii, having scalar product 12 with the first two rows and 9 with the third row. Thus F_2 is also impossible.

Up to permutation, there is only one possibility for a triple of rows of (V, W) of type v, iii, ii respectively, corresponding to a triple of pairwise nonadjacent vertices of G:

$$\begin{array}{ccccccccccccccc}
3 & 3 & 3 & 0 & 0 & 0 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 3 & 3 & 0 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 3 & 2 & 0 & 2 & 2 & 1 & 1 & 1 & 1 & 1.
\end{array} \tag{9.14}$$

The matrix (9.14) cannot be extended by a row of type ii having scalar product 9 with the first row, and 12 with each of the remaining two rows of (9.14). This eliminates F_3.

Finally, there is exactly one (up to permutation) matrix (V, W) corresponding to F_4:

$$\begin{matrix} 3&3&3&0&0&0&2&1&1&1&1&1&1&1&0\\ 3&0&0&3&3&0&1&2&1&1&1&1&1&0&1\\ 0&3&0&3&0&3&1&1&2&1&1&1&0&1&1\\ 0&0&3&0&0&0&0&2&2&1&1&1&1&1&2\\ 0&0&0&0&3&0&2&0&2&1&1&1&1&2&1\\ 0&0&0&0&0&3&2&2&0&1&1&1&2&1&1. \end{matrix} \tag{9.15}$$

The corresponding matrix U has to be of the form (9.4). However, the system (9.6) has only two solutions for a row of (T, U): 110100000000111 and 001011000111000. Hence, the matrix (9.15) is not extendable to an orbit matrix.

Consequently, there is no 2-(22, 8, 4) design with an automorphism of order 3 fixing exactly 4 points.

Combined with the Kapralov result [9], the above results can be summarized in the following.

Theorem 9.13. *The full automorphism group of a* 2-(22, 8, 4) *design must be either a* 2-*group, or trivial.*

Acknowledgements

The second author wishes to thank the Eindhoven University of Technology for the hospitality during the preparation of this paper. Special thanks are due to A. Blokhuis, A.E. Brouwer, and E.W. Lambeck, as well as to the referees for their useful remarks. The research is partially supported by the NCSCMB contract 37/1987.

Final remark

The authors have been informed by one of the referees that an investigation of 2-(22, 8, 4) designs has been recently carried out by Hall, Roth, van Rees and Vanstone [12]. Since the last paper had not yet been published by the time of submission of our paper, we were unable to make any comparison with its results.

References

[1] M. Aschbacher, On collineation groups of symmetric block designs, J. Combin. Theory A 11 (1971) 272–281.

[2] A. Baartmans and K.J. Danhof, Block designs admitting regular automorphism groups, Discrete Math. 10 (1974) 1–8.

[3] Th. Beth, D. Jungnickel and H. Lenz, Design Theory (Bibliographisches Institut, Mannheim-Wien-Zurich, 1985).
[4] P.J. Cameron and J.H. van Lint, Graphs, Codes and Designs (Cambridge Univ. Press, Cambridge, 1980).
[5] M. Hall, Jr., Combinatorial Theory, Second Ed. (Wiley-Interscience, New York, 1986).
[6] N. Hamada and Y. Kobayashi, On the block structure of BIB designs with parameters $v = 22$, $b = 33$, $r = 12$, $k = 8$, and $\lambda = 4$, J. Combin. Theory A 24 (1978) 75–83.
[7] H. Hanani, Balanced incomplete block designs and related designs, Discrete Math. 11 (1975) 255–369.
[8] D.R. Hughes and F.C. Piper, Design Theory (Cambridge Univ. Press, Cambridge, 1985).
[9] St. Kapralov, Combinatorial 2-(22, 8, 4) designs with automorphisms of order 3 fixing one point, Mathematics and Education in Math., Proc. of the XVI Spring Conference of the Union of Bulgarian Mathematicians, Sunny Beach, April 6–10, 1987, Sofia, BAN, 453–458.
[10] E.S. Kramer and D.M. Mesner, T-designs on hypergraphs, Discrete Math. 15 (1976) 263–296.
[11] R. Mathon and A. Rosa, Table of parameters of BIBDs with $r \leqslant 41$ including existence, enumeration, and resolvability results, Annals Discrete Math. 26 (1985) 275–308.
[12] M. Hall, Jr., R. Roth, J. van Rees and S.A. Vanstone, On designs (22, 33, 12, 8, 4), J. Combin. Theory A (to appear).
[13] V.D. Tonchev, Combinatorical Configurations (Longman Scientific & Technical, John Wiley, New York, 1988).

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 191-203
North-Holland

NESTING OF CYCLE SYSTEMS OF ODD LENGTH

C.C. LINDNER[1,2] C.A. RODGER[2] and D.R. STINSON[3]

Department of Algebra, Combinatorics and Analysis, Division of Mathematics, Auburn University, Auburn, Alabama 36849, U.S.A.

Department of Computer Science, University of Manitoba, Winnipeg, Manitoba R3T 2N2, Canada

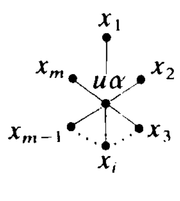
1. Introduction

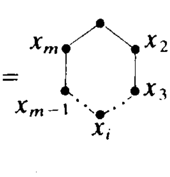
Denote by K_n the complete undirected graph on n vertices. An *m-cycle* of K_n is a collection of m edges $\{x_1, x_2\}, \{x_2, x_3\}, \ldots, \{x_{m-1}, x_m\}, \{x_m, x_1\}$ such that the vertices $x_1, x_2, \ldots, x_m$ are *distinct.* In what follows we will denote the m-cycle $\{x_1, x_2\}, \{x_2, x_3\}, \ldots, \{x_{m-1}, x_m\}, \{x_m, x_1\}$ by any cyclic shift of $(x_1, x_2, \ldots, x_m)$. An *m-cycle system* is a pair (K_n, C), where C is a collection of edge disjoint m-cycles which partition K_n. The number n is called the *order* of the m-cycle system (K_n, C) and, of course, the number of m-cycles $|C|$ is $n(n-1)/2m$. A 3-cycle system is, of course, a *Steiner triple system* (everybody's favorite) and a 5-cycle system is a *pentagon system* (well liked by those who know what a pentagon system is).

A *nesting* of the m-cycle system (K_n, C) is a mapping

$$\alpha\colon C \to \{1, 2, 3, \ldots, n\}$$

such that $C(\alpha)$ is an edge disjoint decomposition of K_n where

$C(\alpha) = \{$ 

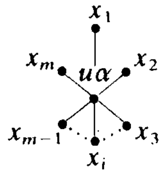
$\mid\ u =$ 

$\in C \}$.

[1] Research supported by NSF grant DMS-8401263.
[2] Research supported by NSA grant MDA-904-88-H-2005.
[3] Research supported by NSERC grant A 9287.

In what follows we will denote the

star



by $(x_1, x_2, \ldots, x_m; u\alpha)$.

A simple counting argument shows that a necessary condition for an m-cycle system (K_n, C) to be nested is $n \equiv 1 \pmod{2m}$. Whether or not an arbitrary m-cycle system can be nested is undoubtedly an extremely difficult problem. A much more reasonable problem is the following: For a given cycle length m, determine the *spectrum* of m-cycle systems which can be nested (= the set of all $n \equiv 1 \pmod{2m}$ for which there exists an m-cycle system of order n which can be nested). This problem has been completely settled for $m = 3$ [2, 6, 9] (the spectrum for Steiner triple systems which can be nested is precisely the set of all $n \equiv 1 \pmod 6$) *and* with 11 possible exceptions for $m = 5$ [5] (the spectrum for pentagon systems which can be nested is the set of all $n \equiv 1 \pmod{10}$, except possibly 111, 201, 221, 231, 261, 301, 381, 511, 581, 591, and 621).

The purpose of this paper is to prove that for any *odd* cycle length m the spectrum of m-cycle systems which can be nested is the set of all $n \equiv 1 \pmod{2m}$ with *at most* 13 possible exceptions for each m. In addition we remove some of these 13 possible exceptions for small values of m. In particular we remove the possible exceptions for pentagon systems, showing that the spectrum for pentagons systems which can be nested is *precisely* the set of all $n \equiv 1 \pmod{10}$.

Finally, we remark that the nesting of an m-cycle system (K_n, C) is equivalent to an edge disjoint decomposition of $2K_n$ into *wheels*, each with m spokes with the property that for each pair of vertices x and y, one of the edges $\{x, y\}$ occurs on the rim of wheel and one of the edges $\{x, y\}$ is the spoke of a wheel.

In the following, m will always denote a positive ODD integer. Also, when we write $d = i \pmod m$ we assume that $d \in Z_m$.

2. Preliminaries

The main ingredients in our construction of m-cycle systems which can be nested are a *skew Room frame* and an *m-nesting sequence*. We begin with the definition of a skew Room frame.

Let $X = \{1, 2, 3, \ldots, 2s\}$ and let $H = \{h_1, h_2, \ldots, h_t\}$ be a partition of X with the property that each h_i has size 2 or 4. The sets $h \in H$ are called *holes*. Using this jargon, we can say that H is a partition of X into holes of size 2 or 4. Denote by $T(X)$ the set of all 2-element subsets of X and by $T(H)$ the set of all

2-elements subsets belonging to a hole of H. Let F be a $2s \times 2s$ array and fill in (a subset of) the cells of F as follows:

(1) For each hole $h_i \in H$, fill in the cells of $h_i \times h_i$ with

x_1x_2	
	x_1x_2

if $h_i = \{x_1, x_2\}$

x_1x_2	x_3x_4		
	x_1x_2	x_3x_4	
		x_1x_2	x_3x_4
x_3x_4			x_1x_2

if $h_i = \{x_1, x_2, x_3, x_4\}$

(in what follows the cells $h_i \times h_i$, $h_i \in H$, will be called a *square* hole);

(2) distribute the 2-element subsets in $T(X)\setminus T(H)$ among the cells not belonging to a square hole (each 2-element subset used exactly once) so that each row and column of F is a 1-factor of K_{2s}; and

(3) if $\{a, b\} \in T(X)\setminus T(H)$, exactly one of the cells (a, b) and (b, a) of F is occupied.

The resulting array is called a skew Room frame of order $2s$ with holes of size 2 or 4.

Example 2.1

1 2			6 9		8 10		3 5	4 7	
	1 2	6 10		7 9		4 5			3 8
5 10		3 4			2 7		1 9	6 8	
	5 9		3 4	1 8		2 10			6 7
8 9		1 7		5 6			4 10	2 3	
	7 10		2 8		5 6	3 9			1 4
4 6		2 9		3 10		7 8		1 5	
	3 6		1 10		4 9		7 8		2 5
	4 8		5 7		1 3		2 6	9 10	
3 7		5 8		2 4		1 6			9 10

Previous page: Skew Room frame of order 10 with holes of size 2 or 4. (In this example all holes happen to be of size 2.)

We state the following existence theorem for skew Room frames with holes and *delay* the proof until Section 5.

Theorem 2.2. *There exists a skew Room frame in which all holes have size* 2 *for every even order* $n \notin \{2, 4, 6, 8, 12, 44, 46, 48, 52, 54, 56, 60, 68, 76\}$. *There exists a skew Room frame with holes of size* 2 *or* 4 *for every even* $n \notin \{2, 4, 6, 8, 12\}$.

Let $[x]$ denote the greatest integer less than or equal to x and define $D(i, j) = \min\{i - j \pmod m,\ j - i \pmod m\}$. An *m-nesting sequence* is a sequence $(d_0, d_1, d_2, \ldots, d_{[m/2]})$, $i \in Z_m$, such that

(1) $\{D(d_i, d_{i-1}) \mid i = 1, 2, \ldots, [m/2]\} = \{1, 2, \ldots, [m/2]\}$, and

(2) $\{D(d_{[m/2]}, d_i) \mid i = 0, 1, \ldots, [m/2] - 1\} = \{1, 2, \ldots, [m/2]\}$.

Example 2.3

$$\begin{cases} (0, 1) \text{ is a 3-nesting sequence,} \\ (0, 1, 4) \text{ is a 5-nesting sequence,} \\ (0, 1, 6, 2) \text{ is a 7-nesting sequence, and} \\ (0, 1, 8, 2, 7) \text{ is a 9-nesting sequence.} \end{cases}$$

Lemma 2.4. *There exists an m-nesting sequence for every odd* $m \geqslant 3$.

Proof. Define $d_i = (-1)^{i+1}[(i + 1)/2] \pmod m$. Then $(d_0, d_1, d_2, \ldots, d_{[m/2]})$ is an m-nesting sequence. □

We close this section with a construction of an m-cycle system of order $2m + 1$ which, as we shall see in Section 3, is a principal ingredient in the skew Room frame construction.

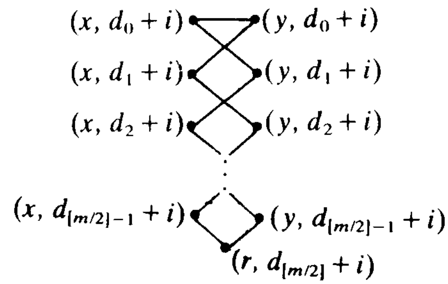
Lemma 2.5. *There exists an m-cycle system of order* $2m + 1$ *which can be nested for every odd* $m \geqslant 3$.

Proof. Let $m = 2n + 1$ and define $c = ((-1)^1 1, (-1)^2 \cdot 2, \ldots, (-1)^n \cdot n, (-1)^n \cdot (n + 1), (-1)^{n+1} \cdot (n + 2), \ldots, (-1)^{2n} \cdot (2n + 1))$, where each coordinate is reduced modulo $2m + 1$. Let $c + i$, $i = 0, 1, 2, \ldots, 2m$, be formed by replacing each coordinate x of c by $x + i \pmod{2m + 1}$. Let K_{2m+1} be based on Z_{2m+1} and define $C = \{c + i \mid i = 0, 1, 2, \ldots, 2m\}$. Then (K_{2m+1}, C) is an m-cycle system of order $2m + 1$ and the mapping α defined by $(c + i)\alpha = i$ is a nesting. □

Example 2.6. For $m = 3$, $c = (6, 5, 3)$, and $C = \{(6 + i, 5 + i, 3 + i) \mid i \in Z_7\}$. For $m = 5$, $c = (10, 2, 3, 7, 5)$ and $C = \{(10 + i, 2 + i, 3 + i, 7 + i, 5 + i) \mid i \in Z_{11}\}$.

3. The skew Room frame construction

We begin with some notation. Let $(d_0, d_1, d_2, \ldots, d_{[m/2]})$ be an m-nesting sequence and $X = \{1, 2, 3, \ldots, 2k\}$. Further let x, y, and r be any 3 distinct elements belonging to X and i any element belonging to Z_m. In what follows we will denote the cycle



by $(x, y, r; d_0+i, d_1+i, \ldots, d_{[m+2]}+i)$, where d_j+i is reduced modulo m.

The skew Room frame construction. Let $m \geq 3$ be *odd*, $X = \{1, 2, 3, \ldots, 2k\}$, and let K_{2km+1} be based on $\{\infty\} \cup (X \times Z_m)$. Further, let S be a skew Room frame (based on X) with holes H of size 2 or 4 and let $(d_0, d_1, d_2, \ldots, d_{[m/2]})$ be an m-nesting sequence. Now define a collection of m-cycles C of K_{2km+1} as follows:

(1) For each hole $h \in H$, define an m-cycle system (which can be nested) on $\{\infty\} \cup (h \times Z_m)$ and place these cycles in C. (*Important*: If the hole $h \in H$ has size 2, then Lemma 2.5 guarantees the existence of an m-cycle system of order $2m+1$ which can be nested. It goes without saying that if $h \in H$ has size 4, this construction is used only if it is *known* that an m-cycle system of order $4m+1$ which can be nested *exists*!); and

(2) for each x and y belonging to *different* holes and *each* $i \in Z_m$, place the m-cycle $(x, y, r; d_0+i, d_1+i, \ldots, d_{[m/2]}+i)$ in C, where r is the *row* of S containing the pair $\{x, y\}$.

It is straightforward to see that (K_{2km+1}, C) is an m-cycle system, and so it remains to show that (K_{2km+1}, C) can be nested.

Theorem 3.1. *The m-cycle system (K_{2km+1}, C) constructed using the skew Room frame construction can be nested.*

Proof. For each hole $h \in H$ denote by $h\alpha$ a nesting of the m-cycle system defined on $\{\infty\} \cup (h \times Z_m)$ *and* define a mapping

$$g\alpha = \begin{cases} (1) & g(h\alpha), \text{ if } g \in \{\infty\} \cup (h \times Z_m) \text{ for some } h \in H; \text{ and} \\ (2) & (c, d_{[m/2]}+i), \text{ if } g = (x, y, r; d_0+i, d_1+i, \ldots, d_{[m/2]}+i), \\ & \text{where } c \text{ is the } \textit{column} \text{ of } S \text{ containing } \{x, y\}. \end{cases}$$

Claim: α is a nesting of (K_{2km+1}, C). We must show that the collection of stars $C(\alpha)$ obtained from C is an edge disjoint decomposition of K_{2km+1}. Trivially the m-cycle systems defined on $\{\infty\} \cup (h \times Z_m)$, $h \in H$, are partitioned by stars belonging to $C(\alpha)$ and so it suffices to show that each edge of the form $\{(x, i), (y, j)\}$, x and y in different holes, belongs to some star of $C(\alpha)$. There are two cases to consider: $i = j$ and $i \neq j$.

$i = j$. Let $d_{[m/2]} + t = i = j \pmod m$. Since S is a skew Room frame and x and y belong to different holes, exactly one of the cells (x, y) and (y, x) is occupied. If cell (x, y) is occupied by $\{a, b\}$, then the m-cycle $c = (a, b, x, d_0 + t, d_1 + t, \ldots, d_{[m/2]} + t = i = j) \in C$. Hence the star $((a, d_0 + t), (b, d_0 + t), (a, d_1 + t), (b, d_1 + t), \ldots, (x, d_{[m/2]} + t = i = j); (y, d_{[m/2]} + t = i = j)) \in C(\alpha)$. The same argument is valid if (y, x) is occupied.

$i \neq j$. Let $d = \min\{i - j \pmod m,\ j - i \pmod m\}$. Then $d \in \{1, 2, 3, \ldots, [m/2]\}$ and so there exists a t such that $D(d_{[m/2]}, d_t) = d$. We assume $d = j - i = d_{[m/2]} - d_t \pmod m$, the other three cases having similar proofs. Then there exists a q such that $j = d_{[m/2]} + q \pmod m$ and $i = d_t + q \pmod m$. Since x and y belong to different holes, column y contains a pair of the form $\{x, z\}$. Denote by (r, y) the cell containing $\{x, z\}$. Then the m-cycle $(x, z, r; d_0 + q, d_1 + q, \ldots, d_{[m/2]} + q) \in C$ and so the star $((x, d_0, +q), (z, d_0 + q), (x, d_1 + q), (z, d_1 + q), \ldots, (x, d_t + q = i), (z, d_t + q = i), \ldots, (r, d_{[m/2]} + q = j); (y, d_{[m/2]} + q = j)) \in C(\alpha)$.

Combining the above two cases shows that the collection of stars $C(\alpha)$ is an edge disjoint decomposition of K_{2km+1} which completes the proof. □

Theorem 3.2. *For any odd $m \geq 3$, the spectrum of m-cycle systems which can be nested is the set of all $n \equiv 1 \pmod{2m}$, with the 13 possible exceptions $n = km + 1$, $k \in \{4, 6, 8, 12, 44, 46, 48, 52, 54, 56, 60, 68, 76\}$.*

Proof. A skew Room frame in which all holes have size 2 exists for every even order $k \notin \{2, 4, 6, 8, 12, 44, 46, 48, 52, 54, 56, 60, 68, 76\}$ (Theorem 2.2). Since there exists an m-cycle system of order $2m + 1$ which can be nested for every odd $m \geq 3$ (Lemma 2.5), the statement of the theorem follows from the skew Room frame construction (Theorem 3.1). □

Corollary 3.3. *If m is odd and there exists an m-cycle system of order $4m + 1$ which can be nested, then the spectrum of m-cycle systems which can be nested is the set of all $n \equiv 1 \pmod{2m}$, with the 3 possible exceptions $6m + 1$, $8m + 1$, and $12m + 1$.*

Proof. In the proof of Theorem 3.2 replace skew Room frames with holes of size 2 with skew Room frames with holes of size 2 or 4. □

4. The spectrum for some small value of m

It should come as no surprise that for a given cycle length m we can improve on the results guaranteed by Theorem 3.2 and Corollary 3.3. We list improvements here for $m \leqslant 15$. There is, of course, nothing special about the number 15. We could just as well use 50 or 100. However, $m \leqslant 15$ is sufficient for illustration.

The principle tool used to improve on the results in Theorem 3.2 and Corollary 3.3 is the finite field construction.

The finite field construction. Let $n = 2km + 1$ be a prime power, x a *primitive* element in $F = \mathrm{GF}(2km + 1)$, and define: $B = \{(x^i, x^{i+2k}, x^{i+4k}, \ldots, x^{i+2(m-1)k}) \mid i = 0, 1, 2, \ldots, k-1\}$. If $b = (a_1, a_2, \ldots, a_m) \in B$ and $y \in F$ denote by $b + y$ the m-cycle $(a_1 + y, a_2 + y, \ldots, a_m + y)$, and set $C = \{b + y \mid b \in B$ and $y \in F\}$. If K_{2km+1} is based on F, then (K_{2km+1}, C) is an m-cycle system and the mapping α given by $(b + y)\alpha = y$ is a nesting.

Finally, we will need the following two m-cycle systems (which can be nested).

(1) Let K_{21} be based on Z_{21} and define $B = \{(1, 6, 19, 18, 7), (4, 16, 13, 9, 11)\}$. Let $C_{21} = \{b + i \mid b \in B$ and $i \in Z_{21}\}$, where $b + i$ is obtained from b by adding $i \pmod{21}$ to each coordinate of b. Then (K_{21}, C_{21}) is a pentagon system and $\alpha: C_{21} \to Z_{21}$ defined by $(b + i)\alpha = i$ is a nesting.

(2) Let K_{45} be based on Z_{45} and define $B = \{(1, 2, 4, 7, 3, 8, 14, 5, 12, 28, 20), (6, 23, 34, 16, 26, 13, 36, 21, 35, 15, 27)\}$. Set $C_{45} = \{b + i \mid b \in B$ and $i \in Z_{45}\}$, where $b + i$ is obtained from b by adding $i \pmod{45}$ to each coordinate of b. Then (K_{45}, C_{45}) is an 11-cycle system and $\alpha: C_{45} \to Z_{45}$ defined by $(b + i)\alpha = i$ is a nesting.

The finite field construction plus (K_{21}, C_{21}) and (K_{45}, C_{45}) guarantees the existence of an m-cycle system of order $4m + 1$ which can be nested for every $m \in \{3, 5, 7, 9, 11, 13, 15\}$. Hence Corollary 3.3 further guarantees for $m \in \{3, 5, 7, 9, 11, 13, 15\}$ that $6m + 1$, $8m + 1$, and $12m + 1$ are the only possible exceptions in the spectrum of m-cycle systems which can be nested. In the following table we have eliminated some of these possible exceptions using the finite field construction.

m	spectrum of m-cycle systems which can be nested
3	all $n \equiv 1 \pmod 6$ Steiner triple systems [9]
5	all $n \equiv 1 \pmod{10}$ pentagon systems [5]
7	all $n \equiv 1 \pmod{14}$ except possibly 57 and 85
9	all $n \equiv 1 \pmod{18}$ except possibly 55
11	all $n \equiv 1 \pmod{22}$ except possibly 133
13	all $n \equiv 1 \pmod{26}$ except possibly 105
15	all $n \equiv 1 \pmod{30}$ except possibly 91

Comments. The spectrum for Steiner triple systems which can be nested was *first* determined by Stinson [9]. The spectrum for pentagon systems was determined with the 11 possible exceptions 111, 210, 221, 231, 261, 301, 381, 511, 581, 591, and 621 by Lindner and Rodger [5]. Denote by $S(m)$ the spectrum of m-cycle systems which can be nested. If $4m+1 \in S(m)$, then $S(m)$ consists of all $n \equiv 1 \pmod{2m}$ with the three possible exceptions $6m+1$, $8m+1$, and $12m+1$ (Corollary 3.3). If $6m+1$, $8m+1$, and $12m+1 \in S(m)$ as well, then $S(m) = \{n \mid n \equiv 1 \pmod{2m}\}$. The important problem of finding a general construction to show that $\{4m+1,\ 6m+1,\ 8m+1,\ 12m+1\} \in S(m)$ remains open. Since it is "surely true" that $\{4m+1,\ 6m+1,\ 8m+1,\ 12m+1\} \in S(m)$ for every odd m, we do not hestitate to make the following *conjecture*: $S(m) = \{n \mid n \equiv 1 \pmod{2m}\}$ *for every odd m.*

5. Proof of Theorem 2.2

We begin with some notation. If S is a skew Room frame with holes H, the *type* of S is defined to be the *multiset* $T(S) = \{|h| \mid h \in H\}$, where $|h|$ is the size of the hole $h \in H$. In what follows we will abbreviate the type $T(S)$ by $1^{t(1)} \cdot 2^{t(2)} \cdot \ldots \cdot k^{t(k)}$, where $t(i)$ denotes the number of holes $h \in H$ of size i, with the proviso that $i^{t(i)}$ occurs in this product if and only if $t(i) \neq 0$. So, for example, a skew Room frame of order 54 with 5 holes of size 2 and 11 holes of size 4 is of type $2^5 \cdot 4^{11}$.

The following result was proved in [10].

Theorem 5.1. *There exists a skew Room frame of type* 2^n *for all* $n \geq 5$, *except possibly for* $n \in \{6, 11, 15, 19, 20, 22, 23, 24, 26, 27, 28, 30, 31, 34, 36, 38, 43, 46, 51, 58, 59, 62, 67\}$.

We prove here the following two results.

Theorem 5.2. *There exists a skew Room frame of type* 2^n *for all* $n \geq 5$, *except possibly for* $n \in \{6, 22, 23, 24, 26, 27, 28, 30, 34, 38\}$.

Theorem 5.3. *For all* $n \geq 5$, $n \neq 6$, *there exists a skew Room frame of order* $2n$, *having holes of size* 2 *and* 4.

In what follows we will *shorten* skew Room frame *to* skew frame. Now, let us recall several constructions from [10]. Let G be an abelian group, written additively, and let H be a subgroup of G. Denote $g = |G|$, $h = |H|$ and suppose that $g - h$ is even. A *frame starter* in $G \backslash H$ is a set of unordered pairs

$S = \{\{s_i, t_i\} \mid 1 \leq i \leq (g-h)/2\}$ satisfying (1) $\{s_i\} \cup \{t_i\} = G \setminus H$, and (2) $\{\pm(s_i - t_i)\} = G \setminus H$. An *adder* for S is an injection $A: S \to G \setminus H$, such that

$$\{s_i + a_i\} \cup \{t_i + a_i\} = G \setminus H, \quad \text{where } a_i = A(s_i, t_i), \quad 1 \leq i \leq (g-h)/2.$$

A is *skew* if, in addition, $\{a_i\} \cup \{-a_i\} = G \setminus H$.

Construction 1. Suppose there exists a frame starter S in $G \setminus H$, and a skew adder A for S. Then there is a skew frame of type $h^{g/h}$, where $g = |G|$ and $h = |H|$.

We also use a modified starter-adder construction, which we now describe. As before, let G be an abelian group and let H be a subgroup of G, where $g = |G|$, $h = |H|$, and suppose that $g - h$ is even. A *2k-intransitive starter* in $G \setminus H$ is defined to be a triple (S, R, C), where

$$\begin{cases} S = \{\{s_i, t_i\} \mid 1 \leq i \leq (g-h-2k)/2\} \cup \{\{u_i\} \mid 1 \leq i \leq 2k\}, \\ C = \{\{p_i, q_i\} \mid 1 \leq i \leq k\}, \quad \text{and} \\ R = \{\{p_i', q_i'\} \mid 1 \leq i \leq k\}, \end{cases}$$

satisfying

$$\begin{cases} (1) \quad \{s_i\} \cup \{t_i\} \cup \{u_i\} \cup \{p_i\} \cup \{q_i\} = G \setminus H, \\ (2) \quad \{\pm(s_i - t_i)\} \cup \{\pm(p_i - q_i)\} \cup \{\pm(p_i' - q_i')\} = G \setminus H, \text{ and} \\ (3) \quad \text{all } p_i - q_i \text{ and } p_i' - q_i' \text{ have even order in } G. \end{cases}$$

An *adder* for (S, R, C) is an injection $A: S \to G \setminus H$, such that $\{s_i + a_i\} \cup \{t_i + a_i\} \cup \{u_i + A(u_i)\} \cup \{p_i', q_i'\} = G \setminus H$, where $a_i = A(s_i, t_i)$, $1 \leq i \leq (g - h - 2k)/2$. A is *skew* if, further,

(1) $\{a_i\} \cup \{-a_i\} \cup \{A(u_i), -A(u_i)\} = G \setminus H$, and
(2) for each i, $1 \leq i \leq k$, there exists a $j \geq 1$ such that $p_i - q_i$ has order $2^j m_1$ and $p_i' - q_i'$ has order $2^j m_2$, where m_1 and m_2 are odd.

Construction 2. If there is a $2k$-intransitive frame starter and a skew adder in $G \setminus H$, where $g = |G|$ and $h = |H|$, then there is a skew frame of type $h^{g/h}(2k)^1$.

We next describe recursive constructions for skew frames. All required design theoretic terminology can be found in [1].

Construction 3. Let (X, G, B) be a group divisible design (GDD), and let $w: X \to Z^+ \cup \{0\}$ (we say that w is a *weighting*). For every $b \in B$ suppose there is a skew frame of type $\{w(x) \mid x \in b\}$. Then there is a skew frame of type $\{\sum_{x \in g} w(x) \mid g \in G\}$.

Construction 4. Suppose (X, B) is a pairwise balanced design (PBD), and there exists a skew frame of type $2^{|b|}$, for every $b \in B$. Then there is a skew frame of type $2^{|X|}$.

Construction 5. Suppose $m \geq 4$, $m \neq 6$ or 10, and suppose $0 \leq t \leq 3m$. Suppose also that there exist skew frames of types 2^{2m} and 2^t. Then there exists a skew frame of type 2^{8m+t}.

Construction 6. Suppose $s = u(v-1)+1$, and let t be a rational number such that $2t$ and $(v-1)/t$ are both integers. Suppose there exist skew frames of type $(2t)^u$ and 2^v, and suppose that $(v-1)/t \neq 2$ or 6. Then there exists a skew Room frame of type 2^s.

Construction 7. Suppose there is a skew Room frame of type $t_1^{u_1}t_2^{u_2}\cdots t_j^{u_j}$, and suppose also that $t \neq 2$ or 6. Then there exists a skew Room frame of type $(t\cdot t_1)^{u_1}(t\cdot t_2)^{u_2}\cdots(t\cdot t_j)^{u_j}$.

Lemma 5.4. *There is a skew frame of type* 2^{59}.

Proof. This is a special application of Construction 3. We start with a group divisible design (GDD) of type 3^8 having blocks of size 4, in which the blocks can be partitioned into 7 parallel classes (see [4] for a construction of this design). Adding a new infinite point to each of 5 of the parallel classes, we obtain a GDD of group-type $3^8 5^1$ having blocks of size 4 and 5. Give every point weight 4, and apply Construction 3, using input frames of type 4^4 and 4^5 (these are constructed in [7]). A skew Room frame of type $12^8 20^1$ is produced. Now, add on two new rows and columns, and fill in the holes with skew frames of types 2^7 and 2^{11}. A skew frame of type 2^{59} results. □

Lemma 5.5. *There exist skew frames of type* $4^{11}2^1$, 4^{12}, *and* $4^{11}2^5$.

Proof. The constructions are obtained by the methods of "projecting sets" as described in [8]. The frames are all constructed by means of intransitive starters and skew adders, by altering slightly the following starter and skew adder in $G\backslash H$, where $G = Z_{11}\times Z_2\times Z_2$ and $H = \{0\}\times Z_2\times Z_2$. Suppose $S = \{\{(x,0,0), (2x,0,0)\}, \{(x,0,1), (2x,1,0)\}, \{(x,1,0), (2x,1,1)\}, \{(x,1,1), (2x,0,1)\} \mid x = 1,3,4,5,9\}$, and $A((x,i,j),(2x,k,l)) = (x, i+k, j+l)$. Then S and A generate a skew frame of type 4^{11}. Now consider the two pairs (in S) $\{(1,0,1),(2,1,0)\}$ and $\{(3,0,1),(6,1,0)\}$. Suppose we delete these two pairs from S, and adjoin the two singletons $\{(1,0,1)\}$ and $\{(6,1,0)\}$, obtaining S'. Then, define $C = \{(2,1,0),(3,0,1)\}$, and $R = \{(3,0,1),(6,1,0)\}$. This produces a 2-intransitive starter and skew adder (S', R, C), and hence there is a skew frame of type $4^{11}2^1$. Now, repeat the above procedure, starting with S', using the pairs $\{(1,1,0),(2,1,1)\}$ and $\{(3,1,0),(6,1,1)\}$. This gives a 4-intransitive starter and skew adder, producing a skew frame of type $4^{11}4^1 = 4^{12}$. We can do this trick three times more, using pairs $\{(1,1,1),(2,0,1)\}$ and $\{(3,1,1),(6,0,1)\}$; $\{(9,0,1),(7,1,0)\}$ and $\{(5,0,1),(10,1,0)\}$; and $\{(9,1,0),(7,1,1)\}$

and $\{(5,1,0),\ (10,1,1)\}$. Thus we obtain a 10-intransitive starter skew adder, and a skew frame of type $4^{11}10^1$. Filling in the hole of size 10 with a skew frame of type 2^5, we obtain the skew frame of type $4^{11}2^5$. This completes the constructions. □

In a similar fashion, we can prove the following lemma.

Lemma 5.6. *There is a skew frame of type* 4^{14}.

Proof. The procedure is similar to that used in Lemma 5.5. We begin with the following starter and skew adder in $G\backslash H$, where $G = Z_{13} \times Z_2 \times Z_2$ and

Table 1. Constructions for skew frames of type 2^n.

n	Construction	Remark
11	2	Table 3
15	2	Table 3
19	2	Table 3
20	1	Table 3
$31 = 5(7-1) + 1(t = 3/2)$	6	A skew frame of type 3^5 is constructed in [3]
$36 = 5(8-1) + 1(t = 1)$	6	
$43 = 8\cdot 4 + 11$	5	
$46 = 5(10-1) + 1(t = 1)$	6	
$51 = 5(11-1) + 1(t = 1)$	6	
$58 = 7\cdot 8 + 1 + 1$	4	There is a PBD on 58 points having blocks of size 7, 8, and 9, constructed by deleting points from a TD(9, 8)
59	Lemma 5.4	
$62 = 7\cdot 8 + 5 + 1$	4	There is a PBD on 62 points having blocks of size 5, 7, 8, and 9, constructed by deleting points from a TD(9, 8)
$67 = 8\cdot 7 + 11$	5	

Table 2. Constructions for skew frames with holes of size 2 and 4.

n	Frame	Construction	Remark
44	4^{11}	7 $(t = 4)$	a skew frame of type 1^{11} exists [7]
46	$4^{11}2^1$	Lemma 5.5	
48	4^{12}	Lemma 5.5	
52	4^{13}	7 $(t = 4)$	a skew frame of type 1^{13} exists [7]
54	$4^{11}2^5$	Lemma 5.5	
56	4^{14}	Lemma 5.6	
60	4^{15}	7 $(t = 4)$	a skew frame of type 1^{15} exists [7]
68	4^{17}	7 $(t = 4)$	a skew frame of type 1^{17} exists [7]
76	4^{19}	7 $(t = 4)$	a skew frame of type 1^{19} exists [7]

Table 3. Starter-adder constructions for skew frames of type 2^n.

$n=8$	5	6	12	1	2
	10	12	3	13	15
	14	1	6	4	7
	15	3	7	6	10
	4	9	5	9	14
	7	13	14	5	11
	11	2	1	12	3
$n=11$	1	2	17	18	19
	7	9	5	12	14
	14	17	9	3	6
	11	15	14	5	9
	18	3	13	11	16
	6	12	16	2	8
	8	16	19	7	15
	5		8	13	
	19		2	1	
$C=$	4	13			
$R=$				4	17
$n=15$	1	27	5	6	4
	2	26	19	21	27
	3	25	2	5	27
	4	24	20	24	16
	5	23	15	20	10
	6	22	25	3	19
	13	16	27	12	15
	12	17	6	18	23
	11	18	11	22	1
	10	19	16	26	7
	9	20	21	2	13
	7		4	11	
	15		10	25	
$C=$	8	21			
$R=$				8	9
$n=19$	19	20	31	14	15
	15	22	25	4	11
$n=19$	14	23	19	33	6
	13	24	15	28	3
	12	25	13	25	2
	11	26	9	20	35
	10	27	35	9	26
	1	35	6	7	5
	2	34	14	16	12
	3	33	26	29	23
	4	32	28	32	24
	5	31	3	8	34
	6	30	16	22	10
	7	29	24	31	17
	9		4	13	
	17		2	19	
$C=$	16	21			
$R=$				27	30
$n=20$	14	15	39	13	14
	11	13	33	4	6
	5	8	23	28	31
	33	37	12	5	9
	31	36	27	18	23
	10	16	11	21	27
	27	34	38	25	32
	21	29	18	39	7
	23	32	10	33	2
	12	22	4	16	26
	38	9	21	19	30
	35	7	3	38	10
	17	30	5	22	35
	28	2	6	34	8
	4	19	32	36	11
	25	1	16	1	17
	26	3	26	12	29
	6	24	31	37	15
	39	18	25	24	3

$H=\{0\}\times Z_2\times Z_2$. Suppose $S=\{\{(x,0,0),\ (4x,0,0)\},\ \{(x,0,1),\ (4x,1,0)\},\ \{(x,1,0),\ (4x,1,1)\},\ \{(x,1,1),\ (4x,0,1)\}\mid x=1,2,3,5,6,9\}$,

$$\begin{cases} A((x,i,j),(4x,k,l))=(3x,i+k,j+l), & \text{if } x=1,3, \text{ or } 9, \text{ and}\\ A((x,i,j),(4x,k,l))=(10x,i+k,j+l), & \text{if } x=2,6, \text{ or } 5.\end{cases}$$

Then S and A generate a skew frame of type 4^{13}. Now, consider the pairs (in S) $\{(5,0,1),(7,1,0)\}$ and $\{(1,0,1),(4,1,0)\}$. Delete these two pairs from S, and adjoin the two singletons $\{(5,0,1\}$ and $\{(4,1,0)\}$, obtaining S'. Then, define $C=\{(1,1,0),(7,0,1)\}$, and $R=\{(4,0,1),(5,1,0)\}$. Then, repeat this process, using instead $\{(5,1,0),\ (7,1,1)\}$ and $\{(1,1,0),\ (4,1,1)\}$. This gives a 4-intransitive starter and skew adder, giving rise to a skew frame of type 4^{14}. □

We present in Table 1 a list of skew frames of type 2^n obtained using the above constructions. As an immediate consequence of Theorem 5.1 and Table 1, we obtain Theorem 5.2. As well, we present in Table 2 a list of skew frames with holes of size 2 and 4. As an immediate consequence of Theorem 5.2 and Table 2, we obtain Theorem 5.3. Theorem 2.2 is, of course, the combination of Theorems 5.2 and 5.3.

References

[1] Th. Beth, D. Jungnickel and H. Lenz, Design Theory, (Bibliographisches Institut, Zurich, 1985).
[2] C.J. Colbourn and M.J. Colbourn, Nested triple systems, Ars Combinatoria 16 (1983) 27–34.
[3] J.H. Dinitz and D.R. Stinson, The construction and uses of frames, Ars Combinatoria 10 (1980) 31–54
[4] E.R. Lamken and S.A. Vanstone, *Elliptic semiplanes and group divisible designs with orthogonal resolutions*, Aequationes Math. (to appear).
[5] C.C. Lindner and C.A. Rodger, *Nesting and almost resolvability of pentagon systems*, Europ. J. Combinatorics 9 (1988) 483–493.
[6] C.C. Lindner and D.R. Stinson, *The spectrum for the conjugate invariant subgroups of perpendicular arrays*, Ars Combinatoria 18 (1983) 51–60.
[7] D.R. Stinson, *The spectrum of skew Room squares*, J. Australian Math. Soc. A 31 (1981) 475–480.
[8] D.R. Stinson, *Some constructions for frames, Room squares, and subsquares*, Ars Combinatoria 12 (1981) 229–267.
[9] D.R. Stinson, *The spectrum of nested Steiner triple systems*, Graphs and Combinatorics 1 (1985) 189–191.
[10] D.R. Stinson, *On the existence of skew frames of type* 2^n, Ars Combinatoria 24 (1987) 115–128.

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 205–216
North-Holland

ON THE (15, 5, λ)-FAMILY OF BIBDs

R. MATHON
Department of Computer Science, University of Toronto, Toronto, Canada

A. ROSA
Department of Mathematics & Statistics, McMaster University, Hamilton, Ontario, L8S 4K1 Canada

Dedicated to Haim Hanani on his 75th birthday.

1. Introduction

Haim Hanani was the first to determine necessary and sufficient conditions for the existence of BIBDs with $k = 3$, 4, and 5 [5, 6, 7]. With a single exception, these designs exist whenever obvious arithmetic conditions are satisfied. The single exception occurs when $v = 15$, $k = 5$, $\lambda = 2$: the (15, 5, 2)-design does not exist as it would be a residual of a nonexistent symmetric (22, 7, 2)-design. Thus in order to show that a $(15, 5, \lambda)$-BIBD exists for all even $\lambda \geq 4$ (λ even is necessary), Hanani had to construct a (15, 5, 4)- and a (15, 5, 6)-BIBD.

Not many (15, 5, 4)-BIBDs are known. In our tables [10], where this design is listed under No. 102, a lower bound of 1 is given. In Hall's book [4], a 1-rotational solution is given. Hanani gives a solution in [5], and another one in [6, 7] (see also [1]). Another highly symmetric solution is given in [2, 9, 12], and as shown in [12], this solution, Hall's solution and the second of Hanani's solutions are mutually nonisomorphic. Another 1-rotational (15, 5, 4)-design is obtained from the twofold pentagon system of order 15 given in [8].

As for (15, 5, 6)-BIBDs (No. 280 in [10]), the only ones known appear to be that given by Hanani in [6] (and again in [7]) and by Dinitz and Stinson in [3]. No resolvable (15, 5, 4)- or (15, 5, 6)-design appears to be known.

In this paper, we take a somewhat closer look at the $(15, 5, \lambda)$-family. In particular, we investigate the existence of cyclic and 1-rotational, as well as the existence of resolvable $(15, 5, \lambda)$-designs. We enumerate completely the 1-rotational (15, 5, 4)-BIBDs (there exists no cyclic (15, 5, 4)-BIBD), and two subclasses of cyclic, and 1-rotational (15, 5, 6)-designs, respectively. In the process, we substantially improve the lower bounds for the number of nonisomorphic designs. We also obtain what we believe are first examples of resolvable (15, 5, 6)-BIBDs, and enumerate completely the resolvable (15, 5, 6)-BIBDs with an automorphism of order 5.

2. 1-rotational (15, 5, 4)-BIBDs

A design with v elements is 1-rotational if it has an automorphism consisting of one fixed point and a single $(v-1)$-cycle. We performed a complete enumeration of 1-rotational (15, 5, 4)-designs. These designs were generated and analyzed by a computer (they were generated by an IBM PC, and analyzed on a Mac II). Applying multipliers resulted in a reduced set of 85 distinct designs which ultimately proved pairwise nonisomorphic. Our first attempt to distinguish nonisomorphic designs involved employing intersection numbers: for each base block, the number of blocks in each orbit intersecting the given base block in i elements, $i = 0, 1, \ldots, 5$, was calculated. In spite of its simplicity, this invariant is fairly sensitive. It partitioned the set of 85 distinct designs into 50 nonisomorphic classes, 19 of which still contained more than one design (13 consisted of two designs each but one of the classes still contained 8 nondistiguished designs). Another invariant, the element counts in blocks containing a particular pair of elements, proved even more sensitive. Here, one counts in the 4 blocks, containing a given pair of elements x, y, the number of occurrences of the remaining 13 elements. For each such pair x, y, one obtains an ordered triple (a_1, a_2, a_3) where a_i is the number of elements occurring i times in the 4 blocks in question. Because the designs are 1-rotational, it clearly suffices to consider pairs $(0, i)$ for $i = 1, 2, \ldots, 13$, and $(0, \infty)$. A sorted list of obtained triples is an invariant of the design.

This invariant partitioned the set of first 82 designs into 60 nonisomorphic classes (the last three designs with 2 short orbits each were already distinguished as nonisomorphic by the previous invariant), 16 of which still contained more than one design (10 contained two, 6 contained three). The two invariants combined failed to distinguish only 7 pairs of designs.

In the end, for each design D its element versus block incidence graph $G(D)$ was formed. As there are 15 elements and 42 blocks, $G(D)$ has 57 vertices. Canonical ordering of vertices of this graph is a complete invariant. All 85 distinct designs are nonisomorphic, thus there exist exactly 85 nonisomorphic 1-rotational (15, 5, 4)-BIBDs. These designs are listed in Table 1. First 82 designs have three full-length-orbits, while the last 3 have two full-length orbits and two half-length orbits (the last 3 designs have also a common half-orbit 0178e not shown in Table 1; all designs have an automorphism (0123456789$abcd$)(e)). The 1-rotational design occurring in [4], p. 410 (under No. 82) is isomorphic to our No. 40 in Table 1, while the design obtained from [8] is isomorphic to our No. 76.

The order of the automorphism group of each design is 14. None of the designs contains a single parallel class.

The two Hanani's (15, 5, 4)-designs appearing in [5], and in [6, 7], respectively, contain an automorphism of order 5. The automorphism group of the design in [2, 9, 12] has order 2520. These designs are mutually nonisomorphic, and also not isomorphic to any of the 85 1-rotational designs. Thus, in the notation of [10], $Nd(15, 42, 14, 5, 4) \geq 88$.

Table 1. 1-rotational 2-(15, 5, 4)-designs

No	Base blocks			No	Base blocks		
1	01256	0247a	0138e	44	01257	0348a	0356e
2	01256	0247a	0578e	45	01457	01357	0169e
3	01256	0368a	0138e	46	01457	02467	0169e
4	01256	0368a	0578e	47	01457	01359	0138e
5	01237	0148a	0358e	48	01457	01359	0578e
6	01237	0348a	0358e	49	01457	04689	0138e
7	01237	0247a	0149e	50	01457	04689	0578e
8	01237	0247a	0349e	51	01457	01579	0136e
9	01237	0368a	0149e	52	01457	01579	0356e
10	01237	0368a	0349e	53	01457	02489	0136e
11	01246	01479	0158e	54	01457	02489	0356e
12	01246	02589	0158e	55	02347	01468	0169e
13	01246	01479	0378e	56	02347	02478	0169e
14	01246	02589	0378e	57	02347	01379	0149e
15	01246	0137a	0169e	58	02347	01379	0349e
16	01246	0237a	0169e	59	02347	02689	0149e
17	01356	01468	0158e	60	02347	02689	0349e
18	01356	01468	0378e	61	01248	01358	0149e
19	01356	01579	0147e	62	01248	01358	0349e
20	01356	01579	0367e	63	01248	03578	0149e
21	01356	0148a	0138e	64	01248	03578	0349e
22	01356	0148a	0578e	65	01568	02458	0237e
23	01247	01468	0149e	66	01568	02458	0457e
24	01247	01468	0349e	67	01568	03468	0237e
25	01247	02478	0149e	68	01568	03468	0457e
26	01247	02478	0349e	69	01568	0148a	0235e
27	01247	01359	0158e	70	01568	0348a	0235e
28	01247	01359	0378e	71	02348	01258	0259e
29	01247	04689	0158e	72	02348	01258	0479e
30	01247	04689	0378e	73	02348	03678	0259e
31	01247	0247a	0156e	74	02348	03678	0479e
32	01247	0368a	0156e	75	02348	0136a	0138e
33	01257	02458	0158e	76	02348	0136a	0578e
34	01257	02458	0378e	77	02348	0356a	0138e
35	01257	03468	0158e	78	02348	0356a	0578e
36	01257	03468	0378e	79	01249	0148a	0136e
37	01257	01359	0147e	80	01249	0148a	0356e
38	01257	01359	0367e	81	01249	0348a	0136e
39	01257	04689	0147e	82	01249	0348a	0356e
40	01257	04689	0367e				
41	01257	0148a	0136e	83	03458	02458	0279e
42	01257	0148a	0356e	84	01246	01469	037ae
43	01257	0348a	0136e	85	01246	03589	037ae

The number of 2-rotational (15, 5, 4)-designs (those with an automorphism consisting of a fixed element and two cycles of length 7) is apparently very large—huge amounts of these were generated on Mac II.

On the other hand, an exhaustive search has shown that there exists no resolvable (15, 5, 4)-design with an automorphism of order 7 or one of order 5, or one of order 3. For more on this, see beginning of Section 5.

3. 1-rotational (15, 5, 6)-BIBDs

Since the number of blocks in a (15, 5, 6)-BIBD is 63, a 1-rotational (15, 5, 6)-design could a priori have 4 full-length orbits and one half-length orbit of blocks, or 3 full-length orbits and 3 half-length orbits. We expected the number of 1-rotational (15, 5, 6)-designs to be quite large—an expectation that eventually proved to be true—and since the latter possibility seemed to be more restrictive, we expected a smaller, more manageable subclass to emerge. To our surprise, this class turned out to be empty. In other words, there exists no 1-rotational (15, 5, 6)-design containing three half-length orbits of blocks, whether repeated or not.

As for the former class, since the shorter orbits are multiplier-isomorphic, one may assume one arbitrary (but fixed) half-length orbit to be present in the design. With this assumption, we generated a set of 5268 distinct such designs, conceivably all pairwise nonisomorphic. Since this is too large a number of designs to analyze, we decide to focus on certain "reasonable" subclasses. One such subclass contains 1-rotational (15, 5, 6)-designs with repeated blocks (and therefore necessarily repeated block orbits). The number of such distinct designs is 29. The "intersection numbers" invariant partitioned these into 22 pairwise nonisomorphic classes, and the "canonical ordering of the incidence graph" invariant proved all 29 designs to be pairwise nonisomorphic. These are listed in Table 2.

The second subclass of 1-rotational (15, 5, 6)-designs that we investigated was the class of designs having at least three S-orbits of blocks. Here, an orbit is called an S-orbit if it is invariant under the mapping $i \to -i (i \in Z_{14})$. This class contained 79 distinct designs, of which 78 have exactly 3 S-orbits and 1 has exactly 4 S-orbits (there is no design having all 5 orbits S-orbits). Again, the intersection numbers partitioned the 79 distinct designs into 64 pairwise nonisomorphic classes, and the "canonical ordering of the incidence graph" invariant proved all 79 designs to be pairwise nonisomorphic. These are listed in Table 3 (all designs in Tables 2 and 3 have also common half-orbit 0178*e* not shown, and an automorphism (0123456789*abcd*)(*e*)).

None of the designs is resolvable, but some of them contain several parallel classes. Of the 79 designs with at least 3 S-orbits, 20 have no parallel class, 52 have 7 parallel classes, 4 have 14 parallel classes and one (No. 37 in Table 3) has 35 parallel classes. The automorphism group of each design given in Tables 2 and 3 has order 14.

Table 2. 1-rotational 2-(15, 5, 6)-designs with repeated orbits

No	Base blocks				No	Base blocks			
1	01246	02569	02569	0238e	16	02348	01358	01358	0348e
2	01246	02569	02569	0568e	17	02348	01358	01358	0458e
3	02456	02569	02569	0238e	18	04568	01358	01358	0348e
4	02456	02569	02569	0568e	19	04568	01358	01358	0458e
5	01246	0136a	0136a	0238e	20	02348	02359	02359	0348e
6	01246	0136a	0136a	0568e	21	02348	02359	02359	0458e
7	02456	0136a	0136a	0238e	22	04568	02359	02359	0348e
8	02456	0136a	0136a	0568e	23	04568	02359	02359	0458e
9	01356	01356	01579	036ae	24	03458	03458	01379	0247e
10	01356	01356	0148a	0269e	25	03458	03458	01379	0357e
11	01356	01356	0148a	0379e	26	01358	01358	0126a	0236e
12	01247	01247	0146a	0359e	27	01358	01358	0126a	0346e
13	01247	01247	0146a	0469e	28	02359	02359	0126a	0236e
14	01247	01247	0256a	0359e	29	02359	02359	0126a	0346e
15	01247	01247	0256a	0469e					

Table 3. 1-rotational 2-(15, 5, 6)-designs with 3 or 4 S-orbits

No	Base blocks				No	Base blocks			
1	01236	01458	0258a	0249e	41	01347	01349	01359	0249e
2	01236	03478	0258a	0249e	42	01347	01349	04689	0249e
3	01236	0126a	0357a	0258e	43	01347	0126a	02358	0249e
4	01236	0126a	0357a	0368e	44	01347	0126a	03568	0249e
5	01256	01347	0258a	0249e	45	01457	01349	02458	0249e
6	01256	03467	0258a	0249e	46	01457	01349	03468	0249e
7	01246	01349	0147a	0249e	47	01457	03458	02368	0249e
8	01246	01349	0369a	0249e	48	01457	03458	02568	0249e
9	01346	01349	0148a	0249e	49	01367	03458	02458	0249e
10	01346	01349	0269a	0249e	50	01367	03458	03468	0249e
11	01346	0126a	02369	0249e	51	02347	03458	0258a	0157e
12	01346	0126a	03679	0249e	52	02347	03458	0258a	0267e
13	01346	0126a	0357a	0238e	53	01248	03458	03469	0249e
14	01346	0126a	0357a	0568e	54	01248	03458	03569	0249e
15	01356	01257	01359	036ae	55	01348	01349	02458	0249e
16	01356	01257	04689	036ae	56	01348	01349	03468	0249e
17	01356	02348	0147a	0249e	57	01348	03458	02368	0249e
18	01356	02348	0369a	0249e	58	01348	03458	02568	0249e
19	01356	01249	01359	036ae	59	02348	01349	0357a	0146e
20	01356	01249	04689	036ae	60	02348	01349	0357a	0256e
21	01356	01349	0148a	0247e	61	02348	03458	02369	0249e
22	01356	01349	0148a	0357e	62	02348	03458	03679	0249e
23	01356	01349	02469	0148e	63	02348	03458	0357a	0238e
24	01356	01349	02469	0478e	64	02348	03458	0357a	0568e
25	01356	01458	02368	0249e	65	01349	03458	01357	0269e
26	01356	01458	02568	0249e	66	01349	03458	01357	0379e
27	01356	03458	01468	0269e	67	01349	03458	01468	0247e
28	01356	03458	01468	0379e	68	01349	03458	01468	0357e
29	01356	03458	0247a	0157e	69	01349	03458	02469	0137e
30	01356	03458	0247a	0267e	70	01349	03458	02469	0467e
31	01356	0126a	02369	0247e	71	01349	02458	0357a	0126e
32	01356	0126a	02369	0357e	72	01349	02458	0357a	0456e
33	02346	01349	0259a	0269e	73	01258	03458	02458	0249e
34	02346	01349	0259a	0379e	74	01258	03458	03468	0249e
35	02346	01569	02369	0249e	75	03458	02368	0357a	0126e
36	02346	01569	03679	0249e	76	03458	02368	0357a	0456e
37	02346	01569	0357a	0238e	77	01369	0126a	0357a	0124e
38	02346	01569	0357a	0568e	78	01369	0126a	0357a	0234e
39	02346	01489	03469	0249e	79	01356	01349	0236a	0249e
40	02346	01489	03569	0249e					

If the results concerning these two subclasses are any indication, most, if not all, of the 5268 distinct 1-rotational designs are likely to be nonisomorphic.

As a consequence of our computational results of this and the preceding section, we have the following.

Theorem 1. *A* 1*-rotational* (15, 5, λ)-BIBD *exists if and only if* $\lambda \equiv 0 \pmod 2$, $\lambda \geqslant 4$.

Proof. Necessity is obvious. There exists a 1-rotational $(15, 5, 4)$- and a 1-rotational $(15, 5, 6)$-design. Noting that every even number $\lambda \geqslant 4$ can be written as $\lambda = 4m + 6n$, where m, n are nonnegative integers, completes the proof. $\square$

4. Cyclic $(15, 5, 6)$-BIBDs

In a sense, this section parallels the previous one. A design with v elements is cyclic if it has an automorphism consisting of a single cycle of length v. Any cyclic

Table 4. Cyclic 2-(15, 5, 6)-designs with repeated orbits

No	Base blocks				No	Base blocks			
1	01235	0148a	0148a	0158a	20	01346	01268	0267a	0267a
2	01235	0148a	0148a	0259a	21	01346	02678	0267a	0267a
3	02345	0148a	0148a	0158a	22	02356	01268	0267a	0267a
4	02345	0148a	0148a	0259a	23	02356	02678	0267a	0267a
5	01245	0249a	0249a	0347a	24	01247	02349	0267a	0267a
6	01245	0249a	0249a	0367a	25	01247	05679	0267a	0267a
7	01236	02379	0267a	0267a	26	03567	02349	0267a	0267a
8	01236	02679	0267a	0267a	27	03567	05679	0267a	0267a
9	03456	02379	0267a	0267a	28	01347	03458	0249a	0249a
10	03456	02679	0267a	0267a	29	01367	0125a	01468	01468
11	01237	02368	0267a	0267a	30	01367	0345a	01468	01468
12	01237	02568	0267a	0267a	31	01467	0125a	01468	01468
13	04567	02368	0267a	0267a	32	01467	0345a	01468	01468
14	04567	02568	0267a	0267a	33	01248	01248	0145a	0258a
15	01237	02359	0267a	0267a	34	01248	01248	0157a	0356a
16	01237	04679	0267a	0267a	35	02348	02348	01479	0158a
17	04567	02359	0267a	0267a	36	02348	02348	01479	0259a
18	04567	04679	0267a	0267a	37	02348	02348	02589	0158a
19	01239	02459	02459	036ab	38	02348	02348	02589	0259a

$(15,5,6)$-design must have 4 full-length block orbits and one short orbit. After generating all distinct cyclic designs and applying all possible multiplier isomorphisms, we arrived at a reduced set of 1953 distinct cyclic $(15,5,6)$-designs, which are multiplier nonisomorphic, and therefore, according to [11], all pairwise nonisomorphic. Although this number is somewhat smaller than the corresponding number for 1-rotational $(15,5,6)$-designs, it is still too large for a complete analysis. We have again restricted ourselves to the same subclasses as in the case of 1-rotational designs: the cyclic $(15,5,6)$-designs with repeated blocks, and the cyclic $(15,5,6)$-designs with at least three S-orbits of blocks. The number of distinct designs in these 2 classes are 38, and 57, respectively. Of the 57 designs in the latter class, 55 have exactly 3 S-orbits, and 2 have exactly 4 S-orbits (there is no cyclic design with all 5 orbits S-orbits). The "canonical ordering of the incidence graph" invariant shows that all of the 38 cyclic $(15,5,6)$-designs with repeated blocks are pairwise nonisomorphic (these designs are listed in Table 4) as are the 57 cyclic $(15,5,6)$-designs with at least 3 S-orbits (these designs are listed in Table 5; all designs in Tables 4 and 5 contain also the short orbit with base block $(0369c)$, and have an automorphism $(01 \cdots 0abcde)$). This follows also from [11]: note that $(15, \varphi(15)) = 1$.

All designs in Table 4 have automorphism group of order 15, except for No. 26 (order 30) and No. 33 (order 60). All designs in Table 5 have automorphism group of order 15, except for Nos. 39, 48, 52, 53, 57 (order 30) and No. 51 (order 120). We have the following analogue of Theorem 1.

Theorem 2. *A cyclic* $(15, 5, \lambda)$-BIBD *exists if and only if* $\lambda \equiv 0 \pmod 2$, $\lambda \geq 6$.

Proof. It is easy to see that there exists no cyclic $(15,5,4)$-BIBD (such a design would necessarily contain the short orbit repeated 4 times, therefore any full-length orbit of blocks in the design cannot contain pairs of elements covered

Table 5. Cyclic 2-(15, 5, 6)-designs with 3 or 4 S-orbits

No	Base blocks				No	Base blocks			
1	01235	0249a	0148a	036ab	30	01238	04568	0257b	036ab
2	02345	0249a	0148a	036ab	31	01238	03458	0148a	0257b
3	01245	01279	0257b	036ab	32	01238	03458	0269a	0257b
4	01245	02789	0257b	036ab	33	01238	03458	0157a	0248b
5	01245	0127a	0158a	0248b	34	01238	03458	0359a	0248b
6	01245	0127a	0259a	0248b	35	01238	0145a	01358	0248b
7	01245	02379	0249a	036ab	36	01238	0145a	03578	0248b
8	01245	02679	0249a	036ab	37	01239	01348	0256a	0257b
9	01236	01468	0249a	036ab	38	01239	01348	0458a	0257b
10	01236	02478	0249a	036ab	39	01239	02459	04579	036ab
11	01256	01269	0235a	0248b	40	01356	01268	01468	036ab
12	01256	03789	0235a	0248b	41	01356	01268	02478	036ab
13	01256	0127a	01358	0248b	42	01356	01348	0249a	0148a
14	01256	0127a	03578	0248b	43	01356	01348	0249a	0269a
15	01237	01249	0257b	036ab	44	01356	01259	0249a	0236a
16	01237	05789	0257b	036ab	45	01356	01259	0249a	0478a
17	01237	01478	0257b	0135a	46	01247	03458	0148a	0249a
18	01237	01478	0257b	0245a	47	01247	03458	0269a	0249a
19	01237	01569	0235a	0248b	48	01457	03458	02379	0249a
20	01237	03489	0235a	0248b	49	01367	03458	01468	0249a
21	01237	02458	0249a	036ab	50	01367	03458	02478	0249a
22	01237	03468	0249a	036ab	51	01248	04678	0145a	0258a
23	01267	01356	0237a	0248b	52	01248	03458	0249a	01469
24	01267	01356	0378a	0248b	53	01248	03458	0249a	03589
25	01267	01457	0235a	0248b	54	02348	03458	0249a	01479
26	01267	02367	0235a	0248b	55	02348	03458	0249a	02589
27	01267	03458	01368	0248b	56	01239	03458	0267a	0257b
28	01267	03458	02578	0248b	57	01356	01248	0249a	036ab
29	01238	02348	0257b	036ab					

by short orbits; but all possible full-length orbits do), hence necessity. For sufficiency, we note that every even integer $\lambda \geqslant 6$ can be written as $\lambda = 6m + 8n + 10p$. Thus, in addition to the cyclic (15, 5, 6)-designs of this section, we need to provide a cyclic (15, 5, 8)- and a cyclic (15, 5, 10)-design. These are given below:

(a) base blocks of a cyclic (15, 5, 8)-design:

$$01256,\ 01257,\ 01268,\ 0237a,\ 0247b,\ 0369c,\ 0369c,\ 0369c.$$

(b) base blocks of a cyclic (15, 5, 10)-design:

$$01256,\ 01268,\ 01269,\ 02458,\ 02368,\ 0267a,\ 0358b. \quad \square$$

5. Resolvable (15, 5 6)-BIBDs

A resolvable (15, 5, 6)-design will contain 21 disjoint parallel classes of 3 blocks each. It appears natural to investigate the existence of resolvable (15, 5, 6)-designs with an automorphism of order 7, and of order 5, respectively. In the former case, the set of elements is taken to be $Z_7 \times \{1, 2\} \cup \{\infty\}$, and there would be three base parallel classes (i.e. three orbits of 7 parallel classes each). In the latter case, the set of elements is taken to be $Z_5 \times \{1, 2, 3\}$, and there would be five base parallel classes (i.e. 4 orbits of 5 parallel classes each, and one parallel class fixed under Z_5).

In the case of an automorphism of order 7, there are following two tactical decompositions:

Base resolutions

	1st	2nd	3rd		1st	2nd	3rd
1)	133	322	214	2)	142	313	223
	322	133	241		313	142	232
	100	100	100		100	100	100

Table 6. Resolvable 2-(15, 5, 6) designs with automorphism of order 5

Tactical decomposition:	3 1 1	3 1 1	1 2 2	1 2 2
	1 3 1	1 3 1	2 1 2	2 1 2
	1 1 3	1 1 3	2 2 1	2 2 1

1	21	0125a	3689d	47bce	0135e	4689a	27bcd	056cd	239ae	1478b	069ce	235bd	1478a
2	21	0125a	3689e	47bcd	0135a	2789d	46bce	068ae	125cd	3479b	067ad	135ce	2489b
3	21	0125a	3689e	47bcd	0135b	2789e	46acd	068ae	125cd	3479b	067be	135ad	2489c
4	21	0125a	3689e	47bcd	0135c	2789a	46bde	068ae	125cd	3479b	067ac	135be	2489d
5	21	0125a	3689e	47bcd	0135d	2789b	46ace	068ae	125cd	3479b	067bd	135ac	2489e
6	21	0125a	3689e	47bcd	0135e	2789c	46abd	068ae	125cd	3479b	067ce	135bd	2489a
7	21	0125a	3689b	47cde	0125d	3789e	46abc	078ab	239ce	1456d	057be	139ad	2468c
8	21	0125a	3689b	47cde	0135c	4689e	27abd	056ac	239de	1478b	069cd	235be	1478a
9	21	0125a	3689e	47bcd	0135a	2678d	49bce	068ae	129cd	3457b	067ad	135ce	2489b
10	21	0125a	3689c	47bde	0125d	3789b	46ace	078ac	239de	1456b	068de	249ab	1357c
11	21	0125a	3689c	47bde	0135a	2678e	49bcd	068bd	129ac	3457e	067bc	135de	2489a
12	21	0125a	3689e	47bcd	0135c	4789b	26ade	058ae	239bd	1467c	067ad	239ce	1458b
13	21	0125a	3689d	47bce	0126c	3589b	47ade	057bd	239ce	1468a	089cd	137ae	2456b
14	21	0125a	3689c	47bde	0135b	4679c	28ade	069cd	345ae	1278b	089bd	135ac	2467e
15	21	0125a	3689e	47bcd	0126c	3589d	47abe	057be	239ac	1468d	089bd	137ae	2456c
16	21	0125a	3689b	47cde	0126c	3589e	47abd	079bc	236ad	1458e	067ce	138ab	2459d
17	21	0125a	3689c	47bde	0126c	3589d	47abe	079cd	236be	1458a	067bd	138ae	2459c
18	21	0125a	3689d	47bce	0135c	2679a	48bde	079ab	128de	3456c	056be	139cd	2478a
19	21	0125a	3689b	47cde	0137d	4568b	29ace	058ce	239bd	1467a	089bc	237de	1456a
20	21	0125a	3689c	47bde	0137a	4568b	29cde	058ae	239bd	1467c	089bd	237ae	1456c
21	21	0125a	3689e	47bcd	0135d	4789a	26bce	068cd	345ae	1279b	067ad	135ce	2489b
22	21	0125a	3689c	47bde	0126c	4789d	35abe	078ab	239ce	1456d	057cd	139be	2468a
23	21	0125a	3689d	47bce	0126e	4789a	35bcd	078be	239ad	1456c	068bc	249de	1357a
24	21	0125a	3689b	47cde	0137e	2568c	49abd	067ac	235de	1489b	079cd	238be	1456a
25	31	0125a	3689e	47bcd	0135d	4678a	29bce	068cd	349ae	1257b	067ad	135ce	2489b
26	21	0125a	3689c	47bde	0135a	4678e	29bcd	068bd	349ac	1257e	067bc	135de	2489a
27	21	0125a	3689e	47bcd	0127e	4589c	36abd	057bd	239ce	1468a	089ab	137cd	2456e
28	21	0125a	3689d	47bce	0127b	3568e	49acd	056cd	239ae	1478b	089be	246cd	1357a
29	21	0125a	3689c	47bde	0127c	4568d	39abe	069ab	235ce	1478d	059cd	138be	2467a
30	21	0125a	3689c	47bde	0136b	4589c	27ade	079ce	346ad	1258b	067bc	135de	2489a
31	21	0125a	3689e	47bcd	0136a	2589d	47bce	079ae	126cd	3458b	067ad	135ce	2489b
32	21	0125a	3789b	46cde	0135b	4689d	27ace	068bc	239de	1457a	089ac	235be	1467d
33	31	0125a	3689c	47bde	0137c	4569d	28abe	058ad	347be	1269c	067bc	135de	2489a
34	31	0125a	3689c	47bde	0137c	4569d	28abe	067bc	348ae	1259d	058ad	137be	2469c
35	21	0125a	3789e	46bcd	0125d	4789b	36ace	068ae	239bd	1457c	067ac	249de	1358b
36	21	0125a	3689e	47bcd	0137d	2689b	45ace	059bd	128ce	3467a	057ae	136cd	2489b
37	21	0125a	3789d	46bce	0127e	3689c	45abd	079bc	235de	1468a	089ad	245bc	1367e
38	21	0125a	3789e	46bcd	0127a	3689c	45bde	079be	235ad	1468c	089bc	245ae	1367d
39	21	0125a	3689c	47bde	0138d	4569c	27abe	069be	347ad	1258c	067bc	135de	2489a
40	21	0125a	3789c	46bde	0128d	4679a	35bce	057ab	236ce	1489d	056cd	248ae	1379b
41	21	0125a	3789b	46cde	0135a	2689c	47bde	068bd	125ce	3479a	067bc	138ae	2459d
42	31	0125a	3789b	46cde	0137c	4689a	25bde	067bc	349ad	1258e	058ad	139bc	2467e
43	21	0125a	3789b	46cde	0138d	4679a	25bce	067bc	349ad	1258e	069be	135cd	2478a

Tactical decomposition:	3 2 0	2 2 1	2 2 1	2 2 1
	1 2 2	2 2 1	1 1 3	1 1 3
	1 1 3	1 1 3	2 2 1	2 2 1

1	21	0125a	3489d	67bce	0168d	2359c	47abe	026de	139ac	4578b	027cd	135be	4689a
2	21	0125a	3489e	67bcd	0157d	2468a	39bce	018ad	247be	3569c	028bc	135de	4679a
3	21	0125a	3468e	79bcd	0256e	1478d	39abc	016bd	247ac	3589e	018ac	246de	3579b
4	21	0125a	3489b	67cde	0269d	1478a	35bce	017bc	235ad	4689e	025ae	147bd	3689c
5	21	0125a	3478e	69bcd	0157e	2489c	36abd	017ac	245bd	3689e	027de	148bc	3569a
6	21	0125a	3478b	69cde	0157b	2489e	36acd	017ac	245de	3689b	027de	148ac	3569b
7	21	0125a	3478e	69bcd	0257e	1369a	48bcd	017bc	248ad	3569e	017ad	246ce	3589b

Table 6 (*Continued*)

8	21	0125a	3478e	69bcd	0267e	1359a	48bcd	017bc	249ad	3568e	017ad	245ce	3689b
9	21	0125a	3469c	78bde	0257c	1389b	46ade	016ac	248bd	3579e	019cd	248ae	3567b
10	21	0125a	3469d	78bce	0267c	1458a	39bde	017ad	249bc	3568e	019cd	245ab	3678e
11	21	0125a	3469d	78bce	0267d	1458e	39abc	017bc	249ae	3568d	019ce	245bd	3678a
12	21	0125a	3469e	78bcd	0168c	2459a	37bde	015ce	248ab	3679d	027ae	148bd	3569c
13	26	0125a	3469d	78bce	0267a	1359c	48bde	016cd	249ab	3578e	018bd	245ae	3679c
14	21	0125a	3469d	78bce	0269a	1357c	48bde	016cd	247ab	3589e	018bd	247ae	3569c
15	21	0125a	3478d	69bce	0256d	1478e	39abc	017bc	239ad	4568e	025de	138ac	4679b
16	21	0125a	3478e	69bcd	0256d	1478b	39ace	017bd	345ac	2689e	025ae	138bc	4679d
17	21	0125a	3468e	79bcd	0156c	2379a	48bde	027be	148cd	3569a	028ab	147ce	3569d
18	21	0125a	3469d	78bce	0267a	1389e	45bcd	015bd	347ae	2689c	028de	135ac	4679b
19	21	0125a	3469d	78bce	0268b	1357c	49ade	016cd	235ae	4789b	027ad	148be	3569c
20	21	0125a	3478e	69bcd	0157a	2369e	48bcd	027bd	138ae	4569c	028ac	147bd	3569e
21	21	0125a	3478e	69bcd	0167a	2359e	48bcd	026bd	138ae	4579c	028ce	135bd	4679a
22	21	0125a	3469d	78bce	0158d	3479a	26bce	026ad	147bc	3589e	027de	148ab	3569c
23	26	0125a	3469d	78bce	0167c	2359a	48bde	025cd	137be	4689a	025de	148ab	3679c

Tactical decomposition:	3 2 0	1 2 2	1 2 2	1 2 2
	0 3 2	2 1 2	2 1 2	2 1 2
	2 0 3	2 2 1	2 2 1	2 2 1

1	21	012ab	34589	67cde	056ce	129ad	3478b	068ab	139de	2457c	079ac	246bd	1358e
2	21	012ac	34589	67bde	057bc	348de	1269a	078ac	139be	2456d	079cd	136ae	2458b
3	21	012ac	34589	67bde	057ae	129cd	3468b	078de	245ab	1369c	059ce	137bd	2468a
4	21	012ac	34589	67bde	058bc	346ad	1279e	058de	137ab	2469c	089be	137cd	2456a
5	21	012ab	34589	67cde	058cd	129be	3467a	058be	137ad	2469c	069bd	245ae	1378c
6	21	012ac	34589	67bde	058ad	347be	1269c	067de	248bc	1359a	068bc	135ae	2479d
7	21	012ac	34589	67bde	058ab	347cd	1269e	079bd	245ae	1368c	067ce	248ab	1359d
8	21	012ac	34589	67bde	067bd	348ce	1259a	068ab	135cd	2479e	079cd	136ae	2458b
9	21	012ac	34589	67bde	067ce	348bd	1259a	068bc	135ae	2479d	079ab	136de	2458c
10	21	012ab	34589	67cde	068ae	129cd	3457b	058bd	246ac	1379e	059ce	138ad	2467b
11	21	012ac	34589	67bde	069ae	128bd	3457c	068cd	135be	2479a	089bc	247de	1356a
12	21	012ab	34589	67cde	078ac	125de	3469b	069ac	138be	2457d	079be	248cd	1356a
13	21	012ac	34589	67bde	057ce	239ad	1468b	058de	236bc	1479a	089bc	137de	2456a

Tactical decomposition:	3 0 2	1 2 2	1 2 2	1 2 2
	0 3 2	2 2 1	1 2 2	1 2 2
	2 2 1	2 1 2	3 1 1	3 1 1

1	21	012ab	567cd	3489e	078bd	1469a	235ce	05cde	2369a	1478b	05acd	1379e	2468b
2	21	012ab	567ce	3489d	078bc	1469e	235ad	05bcd	2369a	1478e	05bce	1379a	2468d
3	21	012ab	679de	3458c	059ac	1478d	236be	06ace	2358d	1479b	07bcd	1356e	2489a
4	21	012ac	679bd	3458e	059bc	1478d	236ae	06ade	2358b	1479c	07ace	1356b	2489d
5	21	012ab	679ce	3458d	058cd	3469a	127be	08abc	2467d	1359e	09acd	1378e	2456b
6	21	012ac	679de	3458b	058ab	3469d	127ce	08bce	2467d	1359a	09cde	1378b	2456a
7	21	012ab	679ce	3458d	057be	2368a	149cd	06bcd	2359e	1478a	09acd	2478e	1356b
8	21	012ac	679de	3458b	057ae	2368c	149bd	06bde	2359a	1478c	09abc	2478d	1356e
9	21	012ab	567cd	3489e	068ad	2479c	135be	05bce	1289d	3467a	05cde	1379a	2468b
10	21	012ab	567ce	3489d	068ab	2479d	135ce	05acd	1289e	3467b	05bcd	1379a	2468e
11	21	012ac	567bd	3489e	068ab	2479c	135de	05cde	1289a	3467b	05bce	1379a	2468d
12	21	012ac	567bd	3489e	068cd	2479e	135ab	05cde	1289b	3467a	05bde	1379c	2468a
13	21	012ac	567bd	3489e	068ab	2479c	135de	05bce	2369a	1478d	05cde	2369b	1478a
14	21	012ab	679de	3458c	056ce	2478a	139bd	08bde	1269c	3457a	07bcd	1356a	2489e
15	26	012ac	679be	3458d	056cd	2478b	139ae	08bcd	1269a	3457e	07abd	1356c	2489e
16	21	012ab	679ce	3458d	059bc	2467a	138de	08ace	1279d	3456b	09bde	1367a	2458c

Tactical decomposition:	3 1 1	3 1 1	1 2 2	1 2 2
	0 3 2	2 1 2	2 1 2	2 1 2
	2 1 2	0 3 2	2 2 1	2 2 1

1	21	012ac	4569b	378de	01257	46ade	389bc	068ad	235be	1479c	089ce	246ab	1357d
2	21	012ac	4569b	378de	01257	46bde	389ac	068ae	235bd	1479c	089cd	246ab	1357e

Table 6 (*Continued*)

3	21	012ac	4569b	378de	01257	46ade	389bc	079cd	236be	1458a	078bd	245ce	1369a
4	21	012ac	4569e	378bd	01259	38abc	467de	068cd	239ae	1457b	069be	247ad	1358c
5	21	012ac	4569e	378bd	01259	47abc	368de	067ce	239bd	1458a	069cd	138ae	2457b
6	21	012ac	4569d	378be	01259	47bcd	368ae	067be	239ac	1458d	069ab	138de	2457c
7	21	012ac	4569d	378be	01268	49bcd	357ae	089be	235ad	1467c	058ae	246bc	1379d
8	21	012ac	4569d	378be	01269	38abd	457ce	067bc	235de	1489a	058de	246bc	1379a
9	21	012ac	4569d	378be	01279	45cde	368ab	078ce	236bd	1459a	068bc	249ae	1357d
10	21	012ab	3589c	467de	01268	37acd	459be	057bc	236ae	1489d	058bd	246ac	1379e
11	21	012ac	3589d	467be	01279	36bcd	458ae	056bd	237ae	1489c	079de	136ac	2458b
12	21	012ab	4579c	368de	01267	39acd	458be	078be	236ad	1459c	078cd	135ae	2469b
13	21	012ac	4579d	368be	01268	47bcd	359ae	079be	238ac	1456d	089ab	135de	2467c
14	21	012ac	4579e	368bd	01269	37abc	458de	056cd	239ae	1478b	078be	249ad	1356c
15	21	012ac	4579e	368bd	01279	48abc	356de	068ce	237bd	1459a	067cd	135ae	2489b
16	21	012ac	3689b	457de	01257	39ade	468bc	089be	235ac	1467d	059bd	246ae	1378c
17	21	012ab	3689c	457de	01257	36bde	489ac	079cd	238ae	1456b	078ac	246bd	1359e
18	21	012ac	3689b	457de	01257	48abc	369de	067cd	235be	1489a	059ad	246be	1378c
19	21	012ac	3689b	457de	01259	46ace	378bd	067cd	239be	1458a	058bc	249de	1367a
20	21	012ac	3689b	457de	01267	35abe	489cd	079ce	236ad	1458b	078be	136cd	2459a
21	21	012ab	3689c	457de	01269	35bde	478ac	058cd	239ae	1467b	059ac	246bd	1378e
22	21	012ac	4569e	378bd	01359	47abc	268de	057be	129ac	3468d	068cd	137ae	2459b
23	21	012ac	4569d	378be	01359	47abe	268cd	068be	129ad	3457c	057cd	136ab	2489e
24	21	012ac	4569b	378de	01368	29bce	457ad	078bc	125ae	3469d	059bd	137ae	2468c
25	21	012ac	4569d	378be	01369	28ade	457bc	057ad	348ce	1269b	078bc	246de	1359a
26	21	012ac	4569b	378de	01379	46ade	258bc	056ce	129ad	3478b	068bd	135ae	2479c
27	21	012ac	4569b	378de	01379	46bde	258ac	056de	129ac	3478b	068bc	135ae	2479d
28	21	012ac	4569d	378be	01379	46bcd	258ae	089ac	346be	1257d	057ae	136bc	2489d
29	21	012ac	4569e	378bd	01379	48abe	256cd	057be	128ad	3469c	058cd	139ae	2467b
30	21	012ac	4569b	378de	01379	48acd	256be	068bc	129ad	3457e	056de	138ab	2479c
31	21	012ac	4569b	378de	01379	48bcd	256ae	068bd	129ac	3457e	056ce	138ab	2479d
32	21	012ac	4569b	378de	01389	26ade	457bc	057ae	129bd	3468c	069ce	245ad	1378b
33	21	012ab	3589d	467ce	01368	45abc	279de	089be	126ad	3457c	069ac	135de	2478b
34	21	012ac	3589e	467bd	01378	45bcd	269ae	069bd	348ce	1257a	058ab	139cd	2467e
35	21	012ac	4579d	368be	01357	29cde	468ab	078ce	126ad	3459b	089ae	245cd	1367b
36	21	012ac	4579b	368de	01367	29abe	458cd	059bd	127ac	3468e	078ce	246ab	1359d
37	21	012ac	4579b	368de	01367	29abc	458de	078ce	125ad	3469b	059bd	246ae	1378c
38	21	012ab	4579c	368de	01378	49bcd	256ae	067ce	129bd	3458a	069ac	135be	2478d
39	21	012ac	4579e	368bd	01378	49bcd	256ae	069bc	127ad	3458e	078be	246cd	1359a
40	21	012ac	4579d	368be	01378	45cde	269ab	056bc	128ad	3479e	089ac	135de	2467b
41	21	012ab	4579c	368de	01378	25abe	469cd	056ac	347be	1289d	059bd	137ac	2468e
42	21	012ac	3689b	457de	01378	45bcd	269ae	056ab	348ce	1279d	089bd	135ac	2467e
43	21	012ac	3689b	457de	01378	26bcd	459ae	079bd	345ac	1268e	089ce	247ab	1356d
44	21	012ab	4569d	378ce	01368	29bde	457ac	069ac	237de	1458b	089cd	235ab	1467e
45	21	012ac	4569e	378bd	01357	49abc	268de	069de	147bc	2358a	078be	149ad	2356c
46	21	012ac	3589d	467be	01358	26cde	479ab	068de	239ab	1457c	089ce	237bd	1456a
47	21	012ac	3589b	467de	01368	45abe	279cd	069be	237ad	1458c	078ce	236ab	1459d
48	21	012ab	3589d	467ce	01379	26cde	458ab	057be	238ad	1469c	078ce	236ab	1459d
49	21	012ac	4569b	378de	01389	45bde	267ac	057de	148ac	2369b	058cd	147ab	2369e
50	21	012ac	4579d	368be	01357	48ade	269bc	067bd	238ac	1459e	089bc	235ae	1467d
51	21	012ac	4569b	378de	01389	26acd	457be	067ae	149cd	2358b	069be	148cd	2357a
52	21	012ab	4579e	368cd	01378	45abc	269de	078ac	236be	1459d	079ad	238be	1456c
53	21	012ac	4579b	368de	01378	45bce	269ad	078cd	236be	1459a	056de	148ab	2379c
54	21	012ab	3689e	457cd	01378	25cde	469ab	059ac	236be	1478d	079bd	238ac	1456e

Above, the first row corresponds to the (element) orbit $Z_7 \times \{1\}$, second row to the orbit $Z_7 \times \{2\}$, and the third row to the fixed element ∞. The columns correspond to blocks in a base parallel class. Thus in (a_{ij}), $i = 1, 2, 3$, $j = 1, 2, 3$, a_{ij} is the number of elements from ith orbit in the jth block of the base parallel class in question.

An exhaustive search has shown that no resolvable $(15, 5, 6)$-design with an automorphism of order 7 exists. This, together with a similar negative result for

$\lambda = 4$ (as a result of an exhaustive search, there exists no resolvable (15, 5, 4)-design with an automorphism of order 7, and there is not even an admissible tactical configuration for a resolvable (15, 5, 4)-design with an automorphism of order 5 or order 3) was quite disappointing.

However, the situation proved to be quite different in the case of resolvable (15, 5, 6)-BIBDs with an automorphism of order 5. In this case, there are 5 tactical decompositions. There exist resolvable (15, 5, 6)-designs corresponding to each one of them. These are listed in Table 6, together with their tactical decompositions. Only the base blocks for the 4 full-length orbits of the parallel classes are shown. The fixed parallel class 01234 56789 *abcde* is common to all designs; all designs have an automorphism (01234)(56789)(*abcde*).

The number of nonisomorphic resolvable (15, 5, 6)-designs obtained is $43 + 23 + 13 + 16 + 54 = 149$. Each of these 149 designs has an automorphism group of order 5. The underlying designs are also pairwise nonisomorphic as in each case the resolution is unique. The number of parallel classes, which each design admits, is not constant, however. While most designs admit exactly 21 parallel classes, i.e. exactly those that appear in the unique resolution, three designs admit 26 parallel classes, and four designs admit 31 parallel classes.

6. Conclusion

As a result of Section 2, we have in the notation of [10] for $\lambda = 4$: $Nd(15, 42, 14, 5, 4) \geqslant 88$.

For $\lambda = 6$, we see easily that the designs of Section 3, Section 4 and Section 5 are mutually nonisomorphic. The (15, 5, 6)-design given by Hanani in [6, 7] is isomorphic to our No. 51 in Table 5, but in Dinitz–Stinson design in [3] is not isomorphic to either of them, thus $Nd(15, 63, 21, 5, 6) \geqslant 108 + 1953 + 149 + 1 = 2211$. We also have $Nr(15, 63, 14, 5, 6) \geqslant 149$.

One question that remains open is that about the existence of a resolvable (15, 5, 4)-BIBD.

Acknowledgements

The authors would like to thank Doug Stinson for pointing out reference [3] and for several valuable comments.

Research of the authors is supported by NSERC Canada under grants number A8651 (RM) and A7268 (AR).

References

[1] T. Beth, D. Jungnickel and H. Lenz, Design Theory (Bibl. Inst., Mannheim, 1985).

[2] P.J. Cameron and J.H. van Lint, Graphs, Codes and Designs, London Math. Soc. Lecture Note 43 (Cambridge Univ. Press, 1980).

[3] J.H. Dinitz and D.R. Stinson, Boss block designs, Ars Combinatoria 9 (1980) 59–68.
[4] M. Hall, Jr., Combinatorial Theory, 2nd ed. (J. Wiley & Sons, New York, 1986).
[5] H. Hanani, The existence and construction of balanced incomplete block designs, Ann. Math. Stat. 32 (1961) 361–386.
[6] H. Hanani, On balanced incomplete block designs with blocks having five elements, J. Combin. Theory (A) 12 (1972) 184–201.
[7] H. Hanani, Balanced incomplete block designs and related designs, Discrete Math. 11 (1975) 255–369.
[8] C.C. Lindner and A. Rosa, Twofold pentagon systems, Caribbean J. Math. (to appear).
[9] R. Mathon, On linked arrays of pairs, Ann. Discrete Math. 15 (1982) 273–292.
[10] R. Mathon and A. Rosa, Tables of parameters of BIBDs with $r \leq 41$ including existence, enumeration and resolvability results, Ann. Discrete Math. 26 (1985) 275–308.
[11] P.P. Palfy, Isomorphism problem for relational structures with a cyclic automorphism, Europ. J. Combin. 8 (1987) 35–43.
[12] S.S. Sane and S.S. Shrikhande, On generalized quasi-residual designs, J. Stat. Plan. Infer. 17 (1987) 269–276.

Discrete Mathematics 77 (1989) 217–236
North-Holland

FINITE BASES FOR SOME PBD-CLOSED SETS

R.C. MULLIN
Department of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, N2L 3G1 Canada

Let $H^a = \{v : v \geq a + 1, v \equiv 1 \pmod a\}$. It is well known that such sets are PBD-closed. Finite bases are found for these sets for $a = 5$, 6 and 7.

1. Introduction

The theory of PBD closure was developed by R.M. Wilson in a remarkable series of papers (see 9, 10 and 11]). Amongst other results, he proved that every PBD closed set contains a finite basis, and illustrated this fact by presenting finite bases for certain instances. The following definitions allow these concepts to be made more precise.

A *pairwise balanced design* (PBD) of index unity is a pair (V, A) where V is a finite set (of points) and A is a class of subsets of V (called blocks) such that any pair of distinct points of V occurs in exactly one of the blocks of A.

A PBD$[K, v]$ is defined to be a PBD(V, A) where $|V| = v$ and $|B| \in K$ for every $B \in A$. Here K is a (finite or infinite) set of positive integers.

If K consists of a single positive integer k, the resulting configuration is called a $(v, k, 1)$ balanced incomplete block design (BIBD).

If K is a (finite or infinite) set of positive integers, let $B(K)$ denote the set of positive integers v for which there exists a PBD$[K, v]$. A set K is PBD-closed (or simply closed) if $B(K) = K$. Wilson has shown that every closed set K contains all sufficiently large integers v with $v \equiv 1 \pmod{\alpha(K)}$ and $v(v-1) \equiv 0 \pmod{\beta(K)}$, where $\alpha(K)$ is the greatest common divisor of the integers $\{k - 1 : k \in K\}$ and $\beta(K)$ is the greatest common divisor of the integers $\{k(k-1) : k \in K\}$. As a consequence of this, as Wilson has pointed out, if K is a closed set, then there exists a finite subset $J \subseteq K$ such that $K = B(J)$. Such a set J is called a *finite basis* for the closed set K. Using the notation of Wilson [11], let a be a positive integer. Then $H^a = \{v : v > a, v \equiv 1 \pmod a\}$ is closed. In fact, Wilson points out the following results.

$$H^2 = B(\{3, 5\}),$$
$$H^3 = B(\{4, 7, 10, 19\}),$$
$$H^4 = B(\{5, 9, 13, 17, 29, 33, 49, 57, 89, 93, 129, 137\}).$$

It is clear that each closed set K has a unique minimal finite basis. An element $x \in K$ is said to be essential in K iff $x \notin B(K \setminus \{x\})$, or equivalently $x \notin B(\{y \in K : y < x\})$. Thus in the unique minimal basis, every element is essential. In the basis for H^4 above, not all listed elements are essential. Indeed, it was later shown that 89, 129, and 137 are not essential. Therefore it is also true that

$$H^4 = B(\{5, 9, 13, 17, 29, 33, 49, 57, 93\}).$$

It is improbable that this is minimal. It is the purpose here to provide the following bases:

$H^5 = B(\{6, 11, 16, 21, 26, 36, 41, 46, 51, 56, 61, 71, 86, 101, 116, 131, 141, 146, 161, 166, 191, 196, 201, 206, 221, 226, 231, 236, 251, 261, 266, 281, 286, 291, 296, 311, 316, 321, 326, 351, 356, 376, 386, 401, 416, 436, 441, 446, 476, 491, 591, 596\})$.

$H^6 = B(\{7, 13, 19, 25, 31, 37, 43, 55, 61, 67, 73, 79, 97, 103, 109, 115, 121, 127, 139, 145, 157, 163, 181, 193, 199, 205, 211, 223, 229, 235, 241, 253, 265, 271, 277, 283, 289, 295, 307, 313, 319, 331, 349, 355, 361, 367, 373, 379, 391, 397, 409, 415, 421, 439, 445, 451, 457, 487, 493, 499, 643, 649, 655, 661, 667, 685, 691, 697, 709, 727, 733, 739, 745, 751, 781, 787, 811, 1063, 1069, 1231, 1237, 1243, 1249, 1255, 1315, 1321, 1327, 1543, 1549, 1567, 1579, 1585, 1783, 1789, 1795, 1801, 1819, 1831\})$.

$H^7 = B(\{8, 15, 22, 29, 36, 43, 50, 71, 78, 85, 92, 99, 106, 113, 127, 134, 141, 148, 155, 162, 169, 176, 183, 190, 197, 204, 211, 218, 225, 239, 246, 253, 260, 267, 274, 281, 295, 302, 309, 316, 323, 330, 337, 351, 358, 365, 372, 379, 386, 414, 421, 428, 442, 575, 582, 589, 596, 603, 610, 701, 708, 715, 722, 827, 834, 1205, 1212, 1219, 1226, 1261, 1268, 1275, 1282, 2031, 2038, 2045, 2066\})$.

2. Constructions for pairwise balanced designs

For the definition of group divisible design (GDD), transversal design (TD), resolvable balanced incomplete block design (RBIBD), and for a discussion of Wilson's fundamental construction for group divisible designs, and relevant notation, see section 3 of [11]. For the definition of incomplete transversal design, incomplete pairwise balanced design (IPBD), and a discussion of the singular indirect product, and relevant notation, see section 2 of [6].

Let P be a finite set of positive prime integers. Define $U(P)$ to be the smallest integer δ such that, for any positive n, there exists an integer s such that $n \leq s \leq n + \delta$ and $(s, p) = 1$ for every $p \in P$, where as usual, (s, p) denotes the greatest common divisor of s and p. The function $U(P)$ is investigated in [8], with particular reference to $U(P_k)$ where $P_k = \{q \leq k,\ q \text{ prime}\}$. The main result of interest here is the following lemma, taken from [8].

Lemma 2.1. *Let k be a positive integer. Then given any positive integer n, there exists an integer s such that $n \leq s < n + U(P_k)$ and there exists a $TD(k+2, s)$.*

The following lemmas are useful in establishing finite bases for the sets H^a.

Lemma 2.2. *Let a be a positive integer. Suppose that there exists a positive integer u such that $u \equiv 1 \pmod a$ and that there exist both a $\mathrm{TD}(a+1, u-1)$ and a $\mathrm{TD}(a+1, u)$. If there exists a $\mathrm{TD}(u+1, m)$, then $m(u-1)(a+1)+at+1$ is inessential in H^a for $0 \leq t \leq m$.*

Proof. By adjoining an ideal point ∞ to a $\mathrm{TD}(a+1, u-1)$, and deleting any other point a $\mathrm{GDD}[\{a+1, u\}]$ of type $a^{u-1}(u-1)^1$ is formed. Similarly by deleting a point from a $\mathrm{TD}(a+1, u)$, a $\mathrm{GDD}[\{a+1, u\}]$ of type $a^u(u-1)^1$ is formed.

Let $G_1, G_2, \ldots, G_{u+1}$ denote the groups of a $\mathrm{TD}(u+1, m)$. Truncate G_1 to obtain a group G_1' of size t, and assign a weight a to each point of $G_1', G_2, \ldots, G_u$, and assign weight $(u-1)$ to each point of G_{u+1}. Apply Wilson's fundamental theorem [11] to obtain a $\mathrm{GDD}[\{a+1, u\}]$ with group type $(am)^{u-1}(at)^1((u-1)m)^1$. Adjoin a point to each group to obtain a $\mathrm{PBD}[\{at+1, (u-1)m+1, am+1, a+1, u\}, m(u-1)(a+1)+at+1]$. Since $\{at+1, (u-1)m+1, am+1\} \subset H^a$, the result follows. □

Let $V(a, b) = \{v : v \equiv 1 \pmod a,\ a+1 \leq v \leq b\}$.

Theorem 2.3. *Let a be a positive integer, and u be an integer such that $u \equiv 1 \pmod a$ and there exists a $TD(a+1, u-1)$ and a $TD(a+1, u)$. Let $\delta = U(P_{u-1})$ and let w be an integer such that*

(*i*) *there exists a $TD(u+1, w)$ and*

(ii) *$w \geq \delta(u-1)(a+1)/a$.*

Then the set $V(a, w(u-1)(a+1)-a+1)$ is a finite basis for H^a.

Proof. For any integer $s \geq \delta(u-1)(a+1)/a$, the inequality

$$(s+\delta)(u-1)(a+1)+1 \leq s(u-1)(a+1)+as+1$$

holds. By the definition of w, all of the values congruent to $1 \pmod a$ in the interval $[w(u-1)(a+1)+1, w(u-1)(a+1)+aw+1]$ are (by Lemma 2.2) inessential in H^a. By the definition of δ, there exists an integer w_1, satisfying $w+1 \leq w_1 \leq w+\delta$ such that there exists a $\mathrm{TD}(u+1, w_1)$ and trivially $w_1 \geq \delta(u-1)(a+1)/a$. Hence, since $w_1(u-1)(a+1)-a+1 \leq w(u-1)(a+1)+wa+1$, all values congruent to $1 \pmod a$ in the interval $[w(u-1(a+1)+1, w_1(u-1)(a+1)-a+1]$ are inessential in H^a. A simple induction completes the proof. □

The following values of $U(P_k)$ are required here and are cited from [8].

k	$U(P_k)$
5	6
7	10
11	14
13	22

(Note that this function increases only when k is prime.)

The following well known result is included for the sake of completeness.

Lemma 2.4. *Let D be a pairwise balanced design on v points, whose smallest blocks contain s elements and which contains a block L of length l. Then $v \geqslant l(s-1)+1$, with equality only if there is a resolvable balanced complete block design $(l(s-1)+1, s-1, 1)$.*

Proof. Let ∞ denote any point not on L in D. Since ∞ is contained in a block with each of the points on L, there are at least l blocks containing ∞, each containing $(s-1)$ points other than ∞. Therefore $v \geqslant l(s-1)+1$.

In the case of equality, all blocks other than L must contain precisely s points, and the configuration determined by removing the points of l is a RBIBD$(l(s-1)+1, s-1, 1)$. Clearly any RBIBD$(l(a-1)+1, s-1, 1)$ can be extended to such a pairwise balanced design. □

3. A basis for H^5.

In Section 1, bases for H^2, H^3, and H^4 were given. Unfortunately, the size of bases for H^a which can be formed tends to increase rapidly with a, so that the basis given for H^5 is considerably larger. We begin by pointing out that $\{6, 11, 16, 21, 26, 36, 41\}$ is a set of essential elements in any basis for H^5. Indeed, by Lemma 2.4, any PBD with block sizes from the above list which contains blocks of more than one size must contain at least 46 points, so any inessential elements in the above set must correspond to PBDs which contain blocks of only one size. If any of these are non-trivial (that is, do not consist of a single block) then there must be balanced incomplete block designs. But any balanced incomplete block design of index one with a block size 11 or more must contain at least 111 blocks, which reduces the problem to considering BIBDs of block size 6. By a Lemma 2.4 in the case $l = s$, such a design must contain at least 31 points, and the number v of such points must satisfy $v \equiv 1$ or $v \equiv 6 \pmod{15}$. The projective plane of order 5 provides an example for $v = 31$, and it is well known that there is no affine plane of order 6, so that the integer 36 is essential. Since $41 \equiv 11 \pmod{15}$, 41 is also essential.

Since there exist both a TD(6, 15) and TD(6, 16), by Lemma 2.3, taking

$w = 397$, the set $V(5, 35726)$ is a finite basis for H^5. This result can be greatly improved after the following lemmas.

Lemma 3.1. *Let m be an integer such that there exists a* TD$(14, m)$. *Then $65m + 15t + 1$ is inessential in H^5 for $0 \leq t \leq m$. See* Zhu [14].

Lemma 3.2. *Let v be an integer such that $v \equiv 1$ or $v \equiv 6$ (mod 15) and $v \geq 6$. Then $v \in B(6)$ with the possible exception of $v \in S$, where S is the set of* 99 *values listed in Table* 1 *below.*

Table 1.

16	21	36	46	51	61	81	141	166	171
196	201	226	231	246	256	261	276	286	291
316	321	336	346	351	376	406	411	436	441
466	471	486	496	501	526	561	591	616	621
646	651	676	706	711	736	741	766	771	796
801	831	886	891	916	946	1011[a]	1066	1071	1096
1101	1131	1141	1156	1161	1176	1186	1191	1221	1246
1251	1276	1396	1401	1456	1461	1486	1491	1516	1521
1546	1611	1641	1671	1816	1821	1851	1881	1971	2031
2241	2601	3201	3471	3501	4191	4221	5391	5901	

[a] See Corollary 3.13.1.

Proof see [14]. The values 1551, 1636, 3621, 3771, 4346, 4251 have been obtained by W.H. Mills (private communcation). □

Lemma 3.3. *Let m be an integer such that there exists a* TD$(16, m)$. *Then $75m + 5t + 1$ is inessential in H^5 for $0 \leq t \leq m$.*

Proof. Since $76 \in B(6)$, there exists a GDD[{6}] with group type 5^{15}. By extending the resolvable BIBD(65, 5, 1) to a PBD[{6, 16}, 81] and deleting a point not on the block of size 16, a GDD [{6, 16}] with group type 5^{16} is created. Applying Wilson's fundamental theorem establishes the result. □

Lemma 3.4. *If there exists a* TD$(19, m)$, *then $90m + 5t + 1$ is inessential in H^5 for t satisfying $0 \leq t \leq m$.*

Proof. Apply Lemma 2.2 with $a = 5$, $u = 16$. □

Lemma 3.5. *Let v be an integer such that $v \equiv 1$* (mod 5) *and v satisfies $1876 \leq v \leq 35721$. If v does not lie in the interval $2571 \leq v \leq 2606$, then v is inessential in H^5.*

Proof. First consider the interval $2666 \leqslant v \leqslant 35721$. By Lemma 3.2, it is sufficient to establish the result in this range for $v \equiv 11 \pmod{15}$ together with $v \in X = \{3201, 3471, 3501, 4191, 4221, 5391, 5901\}$. We first take care of values such that $v \equiv 11 \pmod{15}$ using Lemma 3.1 in conjunction with appropriate m which satisfy $m \equiv 2 \pmod 3$. The results are given below.

m	$65m+1$	$80m+1$
41	2666	3281
47	3056	3761
53	3446	4241
59	3836	4721
71	4616	5681
83	5396	6641
89	5786	7121
101	6566	8081
113	7346	9041
131	8516	10481
149	9686	11921
167	10856	13361
197	12866	15761
227	14756	18161
269	17486	21521
323	20996	25841
383	24896	30641
443	28796	35441
449	29186	35921

Now if $m \equiv 1 \pmod 3$ in Lemma 3.1, then $65m + 15t + 1 \equiv 6$ $(mod\ 15)$, so that the values of v in X are treated as follows.

m	$65m+1$	$80m+1$
49	3186	3921
61	3966	4880
79	5136	6321

The remaining values, apart from v satisfying $2006 \leqslant v \leqslant 2021$, are dealt with by Lemmas 3.3 and 3.4 as below.

Lemma 3.3			Lemma 3.4		
m	$75m+1$	$80m+1$	m	$90m+1$	$95m+1$
25	1876	2001	23	2071	2186
27	2026	2161	27	2431	2566
29	2176	2321	29	2611	2756
31	2326	2481			

In the interval $2006 \leqslant v \leqslant 2021$, we need only consider 2006 and 2021 in view of Lemma 3.2. but $2006 = 29.65 + 8.15 + 1$ and $2021 = 29.65 + 9.15 + 1$. This completes the lemma. □

Lemma 3.6. *Suppose that there exists a* $\mathrm{PBD}[H^5, v]$ *which contains a flat of order* f *and a* $\mathrm{TD}(6, v - f + a) - \mathrm{TD}(6, a)$, *where* $0 \leqslant a \leqslant f$. *Then* $w = 6v - 5f + 5a$ *is inessential in* H^5, *and there exists a* $\mathrm{PBD}[H^5, w]$ *which contains a flat of order* $f + 5a$.

Proof. The proof is analogous to that of construction 4.1 in [5]. □

For convenience, we record the well-known observation below.

Lemma 3.7. *If there is a resolvable* BIBD *with block size* 5 *and* r *resolution classes, then there exists a* $\mathrm{PBD}[\{6, r\}, 5r + 1]$.

Lemma 3.8. *Suppose that* a, t, *and* m *are integers satisfying* $0 \leqslant t \leqslant m$ *and* $0 \leqslant a \leqslant m$. *If there exist a* $\mathrm{TD}(8, m)$ *and a* $\mathrm{TD}(6, t)$, *then there exists a* $\mathrm{TD}(6, 7m + t + a) - \mathrm{TD}(6, a)$.

Proof. See Wilson [12]. □

For the existence of $\mathrm{RBIBD}(v, 5, 1)$, see [4]. As authority for the existence of a $\mathrm{TD}(k, m)$, we use [2] unless otherwise indicated.

Lemma 3.9. *If* v *is any integer such that* $v \equiv 1 \pmod 5$ *and* v *satisfies* $2571 \leqslant v \leqslant 2606$, *then* v *is inessential in* H^5.

Proof. Since there exists a $\mathrm{TD}(6, 76)$, then there exists a $\mathrm{PBD}[\{6, 76\}, 456]$ with a flat of order 76. Also, since $380 + a = 7.53 + 9 + a$, there exists a $\mathrm{TD}(6, 380 + a) - \mathrm{TD}(6, a)$ for $0 \leqslant a \leqslant 53$. Hence the values of v such that $v \equiv 1 \pmod 5$ which satisfy $2356 \leqslant v \leqslant 2621$ are inessential in H^5 by Lemma 3.6. □

As the result of the above lemmas, note that if $v \geqslant 1876$, then v is inessential in H^5.

Lemma 3.10. *Suppose that there exists a* $\mathrm{TD}(26, m)$.

(i) *If* $m \equiv 0 \pmod 5$, *then* $26m + 5t + 1$ *is inessential in* H^5, *for* $0 \leqslant t \leqslant m$.

(ii) *If* $m \equiv 1 \pmod 5$, *then* $26m + 5t$ *is inessential in* H^5 *for* $0 \leqslant t \leqslant m$.

Proof. There exists a trivial $\mathrm{GDD}[\{26\}]$ with group type 1^{26}. Also, since $31 \in B(6)$, there exists a $\mathrm{GDD}[\{6\}]$, with group type $25^1 6^1$. If there exists a $\mathrm{TD}(26, m)$, then by Wilson's fundamental construction [11], there exists a $\mathrm{GDD}[\{6, 26\}]$ with group type $m^{25}(m + 5t)^1$. To obtain the result, if $m \equiv 1$

(mod 5), use the GDD as a PBD. If $v \equiv 0 \pmod 5$, then adjoin a new point to each group to obtain the required PBD. $\square$

Lemma 3.11. *Let v be any integer such that $v \equiv 1 \pmod 5$ and v satisfies $v \geqslant 1001$. Then v is inessential in H^5.*

Proof. First use Lemma 3.6 to cover the following intervals.

PBD with flat	flat	incomplete TD	max a	interval
$176(=11 \times 17)$	11	$165 + a = 11.15 + a$	11	1001–1056
$181(\in B(6))$	6	$175 + a = 7.25 + a$	6	1056–1086

Now apply Lemma 3.10

m	$26m$	$31m$
41	1066	1271

Again apply Lemma 3.6

PBD with flat	flat	incomplete TD	max a	interval
$241(=6.40+1)$	41	$200 + a = 7.27 + 11 + a$	27	1241–1376
$246(=6.41)$	41	$205 + a = 7.27 + 16 + a$	27	1271–1406
$271(=6.45+1)$	46	$225 + a = 7.32 + 1 + a$	32	1396–1556
$276(=6.46)$	46	$230 + a = 7.31 + 13 + a$	31	1426–1581

Now apply Lemma 3.10 again.

m	$26m$	$31m$
61	1586	1891

These cover all required values in the interval $1001 \leqslant v \leqslant 1891$. This, together with the fact that the result is true for $v \geqslant 1876$, establishes the lemma. $\square$

Lemma 3.12. *Let v be any integer such that $v \equiv 1 \pmod 5$ and v satisfies $516 \leqslant v \leqslant 996$ and v does not lie in the intervals $591 \leqslant v \leqslant 596$ or $966 \leqslant v \leqslant 996$. Then v is inessential in H^6.*

Proof. Note that there exists a BIBD(601, 6, 1). Now apply Lemma 3.6 as below.

PBD with flat	flat	incomplete TD	max a	interval
$91\ (\in B(6))$	6	$85 + a = 7.11 + 8 + a$	6	516–546
106 (RBIBD(85, 5, 1))	21	$85 + a = 7.11 + 8 + a$	11	531–586
$106\ (\in B(6))$	6	$100 + a = 7.13 + 9 + a$	6	606–636
$111\ (\in B(6))$	6	$105 + a = 7.15 + a$	6	636–666

Now use Lemma 3.10

m	$26m+1$	$31m+1$
25	651	776

Now again use Lemma 3.6.

PBD with flat	flat	incomplete TD	max a	interval
156(RBIBD(125, 5, 1))	31	$125+a=7.16+13+a$	16	781–861

Now again apply Lemma 3.10.

m	$26m$	$31m$
31	806	961

This completes the Lemma. □

Lemma 3.13. *There exists a* TD(6, 28) − TD(6, 3) *and a* TD(6, 29) − TD(6, 4).

Proof. These are constructed by the matrix-minus diagonal method of Wilson [13]. The following arrays lie in GF(25) as generated by $x^2+3=0$. □

TD(6, 28) − TD(6, 3)

—	0	1	2	$3x+2$	$4x+4$
0	—	1	$x+3$	$3x+4$	$2x+4$
0	1	—	2	$x+3$	$4x+1$
0	2	4	—	$4x+3$	$x+4$
0	3	2	$3x+3$	—	4
0	4	x	3	$3x+2$	—
0	x	$3x+1$	$2x$	2	$4x+3$
0	$x+2$	$4x+1$	$3x+2$	$2x+1$	$2x+2$
0	$2x$	$x+2$	$3x+1$	4	$x+3$
0	$3x+1$	$4x+3$	$2x+1$	$4x+1$	$3x+4$

TD(6, 29) − TD(6, 4)

—	0	1	2	3	4
0	—	1	3	$x+1$	$2x+1$
0	1	—	$x+3$	$3x+4$	$2x$
0	2	x	—	$2x+3$	$x+1$
0	x	$x+2$	$3x+2$	—	$2x+2$
0	$x+2$	2	$3x+1$	$2x$	—

Corollary 3.13.1. *There exists a* PBD[{6, 21}, 171] *and a* PBD[{6, 26}, 176] *which contains a unique block of size* 26. *Therefore* 171 *and* 176 *are inessential in* H^5. *Further there exists a* BIBD(1011, 5, 1).

Proof. To obtain the pairwise balanced designs in the enunication, apply Lemma 3.6 to the BIBD(31, 6, 1) using a block of size 6 used as a flat.

Note that one can apply Lemma 3.6 to the PBD[{6, 26}, 176] above, using the block of size 26 as a flat. Using the value $a = 17$, noting that $167 = 7.19 + 17 + 17$, yields a PBD [{6, 111}, 1011] which contains a unique block of size 111, which can be "replaced" by a BIBD(111, 6, 1) to yield a BIBD(1011, 6, 1). □

Lemma 3.14. *Suppose that v is any integer such that $v \equiv 1 \pmod 5$ and v satisfies $v \geqslant 516$. If $v \notin \{591, 596\}$, then v is inessential in H^5.*

Proof. In view of Lemmas 3.11 and 3.12, it is sufficient to treat the interval $966 \leqslant v \leqslant 996$. This is dealt with using Lemma 3.6 and Corollary 3.13.1 and the following table.

PBD with flat	flat	incomplete TD	max a	interval
176	26	$150 + a = 17.19 + 17 + a$	19	926–1021

This establishes the result. □

We are now in a position to prove the main result of this section.

Table 2. A basis for H^5.

6	11	16	21	26	36	41	46	51	56
61	71	86	101	116	131	141	146	161	166
191	196	201	206	221	226	231	236	251	261
266	281	286	291	296	311	316	321	326	351
356	376	386	401	416	436	441	446	476	491
591	596								

Theorem 3.15. *The* 52 *values in Table* 2 *above are a basis for* H^5.

Proof. In view of the above, we need only consider $v \leqslant 511$. After eliminating those values in $B(6)$, the set of values {81, 171, 176, 246, 256, 276, 336, 341, 346, 371, 406, 411, 431, 461, 466, 471, 486, 496, 501, 506} remain. These are treated below. (In all applications of Lemma 3.6, the existence of the required Incomplete Transversal Design is immediate.)

$81 = 65 + 16$	RBIBD(65, 51)	
171	Corollary 3.13.1	
176	Corollary 3.13.1	
$246 = 6.41$		
$256 = 16^2$		
$276 = 11.25 + 1$		
$336 = 6.56$		
$341 = 6.55 + 11$	(Lemma 3.6, $f = 11$)	$(66 = 6.11)$
$346 = 6.55 + 16$	(Lemma 3.6, $f = 11$)	$(66 = 6.11)$
$371 = 6.60 + 11$	(Lemma 3.6, $f = 6$)	$66 \in B(6)$
$406 = 325 + 81$		$\exists$ RBIBD(325, 5, 1)
$411 = 6.65 + 21$	(Lemma 3.6, $f = 16$)	$81 = 65 + 16$(RBIBD)
$431 = 6.70 + 11$	(Lemma 3.6, $f = 6$)	
$461 = 6.75 + 11$	(Lemma 3.6, $f = 6$)	$81 = 65 + 16$(RBIBD)
$466 = 6.75 + 16$	(Lemma 3.6, $f = 16$)	$91 = 6.15 + 1$
$471 = 6.75 + 21$	(Lemma 3.6, $f = 16$)	$91 = 6.15 + 1$
$486 = 6.81$		
$496 = 16.31$		
$501 = 6.80 + 21$	(Lemma 3.6, $f = 16$)	$96 = 6.16$
$506 = 405 + 101$		$\exists$ RBIBD(405, 5, 1)

Thus all required cases are covered. □

4. A basis for H^6

Since there exist both a TD(7, 12) and TD(7, 13), and since $U(P_{12}) = 14$, the following lemma is immediate from Lemma 2.3 (using $w = 197$).

Lemma 4.1. *The set* $V(7, 16543)$ *is a basis for* H^6.

To improve upon this result, we note the following.

Lemma 4.2. *If* m *satisfies*
(i) $m \equiv 1 \pmod 6$, *and*
(ii) *there exists a* TD$(43, m)$,
then $43m + 6t$ *is inessential in* H^6 *for* $0 \leq t \leq m$.

Proof. There exists a BIBD (49, 7, 1). Considering this, the proof is analogous to that of Lemma 3.10. □

Lemma 4.3. *Suppose that there exists a* $\mathrm{PBD}[H^6, v]$ *which contains a flat of order* f, *and there exists a* $\mathrm{TD}(6, v-f+a)-\mathrm{TD}(6, a)$, *where* $0 \leqslant a \leqslant f$. *Then* $w = 7v - 6f + 6a$ *is inessential in* H^6.

Proof. The proof is that of Theorem 3.6, mutatis mutandis. □

The following theorems are direct analogues of Lemmas 3.7 and 3.8 respectively.

Lemma 4.4. *If there exists a resolvable* BIBD *with block size* 6 *and* r *resolution classes, then there exists a* $\mathrm{PBD}[\{7, r\}, 6r+1]$ *which contains a unique flat of order* r.

Lemma 4.5. *Suppose that* a, t, *and* m *are integers satisfying* $0 \leqslant t \leqslant m$ *and* $0 \leqslant a \leqslant m$. *If there exists a* $\mathrm{TD}(8, m)$ *and a* $\mathrm{TD}(7, t)$, *then there exists a* $\mathrm{TD}(7, 7m+t+a)-\mathrm{TD}(7, a)$.

Lemma 4.6. *Suppose there exists a* $\mathrm{TD}(k, s)$, *a* $\mathrm{TD}(k, s+1)$, *a* $\mathrm{TD}(k, s+2)$, *a* $\mathrm{TD}(k+t+1, m)$ *and a* $\mathrm{TD}(k, s+t+u)$ *where* $u \in \{0, 1\}$. *Then there exists a* $\mathrm{TD}(k, ms+t+a)-\mathrm{TD}(k, a)$ *for* $0 \leqslant a \leqslant m-1+u$. (cf. Zhu [14]).

Proof. This follows from Wilson's constructions [12]. □

Corollary 4.6.1. *If there exists a* $\mathrm{TD}(8+t, m)$ *and a* $\mathrm{TD}(7, 7+t+u)$ *where* $u \in \{0, 1\}$, *then there exists a* $\mathrm{TD}(7, 7m+t+a)-\mathrm{TD}(7, a)$, *for* $0 \leqslant a \leqslant m-1+u$.

Lemma 4.7. *Let* m *be an integer such that there exists a* $\mathrm{TD}(14, m)$. *Then* $84m+6t+1$ *is inessential in* H^6.

Proof. Take $a = 6$ and $u = 13$ in Lemma 2.2. □

Lemma 4.8. *If* v *satisfies* $v \equiv 1 \pmod 6$ *and* $v \geqslant 1849$, *then* v *is inessential in* H^6.

Proof. Consider the following intervals.

m	$43m$	$49m$	Lemma 4.2
43	1849	2107	
49	2107	2401	
m	$84m+1$	$90m+1$	Lemma 4.7
27	2269	2431	
29	2437	2611	
31	2605	2791	

m	$43m$	$49m$	Lemma 4.2
61	2623	2989	
67	2881	3283	
73	3139	3577	
79	3397	3871	

Now apply Lemma 4.3.

PBD with flat	flat	incomplete TD	max a	interval
$595 = 7.85$	85	$510 = 7.71 + 13 + a$	71	3655–4081

Now return to Lemmas 4.2 and 4.7.

m	$84 + 1$	$90m + 1$	Lemma 4.7
47	3949	4231	

m	$43m$	$49m$	Lemma 4.2
97	4171	4753	
109	4687	5341	
121	5203	5929	
127	5461	6223	
139	5977	6811	
151	6493	7399	
163	7009	7987	
181	7783	8869	
199	8557	9751	
223	9589	10927	
241	10363	11809	
271	11653	13279	
307	13201	15043	
343	14749	16807	

This establishes the lemma. □

Lemma 4.9. *If there exists a* TD(8, m), *then* $48m + 1 \in B[\{7, 6m + 1\}]$.

Proof. Since $49 \in B(7)$, there exists a GDD[{7}] of group type 6^8. Apply Wilson's fundamental theorem [11].

Lemma 4.10. *Suppose that* v *satisfies* $v \equiv 1 \pmod 6$ *and* $v \geq 1075$. *Then* v *is inessential in* H^6 *with the possible exception of* $v \in \{1231, 1237, 1243, 1249, 1255, 1315, 1321, 1327, 1543, 1549, 1567, 1579, 1585, 1783, 1789, 1795, 1801, 1819, 1831\}$.

Proof. We begin with Lemma 4.3.

PBD with flat	flat	incomplete TD	max a	interval
$175 = 7.25$	25	$150 + a = 7.19 + 17 + a$	19	1075–1189
$175 = 7.25$	7	$168 + a = 7.23 + 7 + a$	7	1183–1225
187(RBIBD(156, 6, 1))	7	$180 + a = 7.25 + 5 + a$ (Corollary 4.6.1, $u = 1$)	7	1267–1309
$217 = 7.31$	31	$186 + a = 7.25 + 11 + a$	25	1333–1483

Use Lemma 4.7.

m	$84m + 1$	$90m + 1$
17	1429	1531

Again, use Lemma 4.3.

PBD with flat	flat	incomplete TD	max a	interval
$259 = 7.37$	37	$222 + a = 7.31 + 5 + a$ (Corollary 4.6.1, $u = 1$)	31	1591–1777

The above intervals cover all cases except for the appropriate v in the intervals listed below.

$1231 \leqslant v \leqslant 1261$
$1315 \leqslant v \leqslant 1327$
$1537 \leqslant v \leqslant 1585$
$1783 \leqslant v \leqslant 1843$

All but one of the remaining cases, namely 1837, are covered in the following.

List of equations

$1261 = 13.97$
$1537 = 48.32 + 1$ (Lemma 4.9)
$1555 = 7.222 + 1$
$1561 = 7.223$
$1573 = 13.121$
$1807 = 13.139$
$1813 = 7.259$
$1825 = 25.73$
$1843 = 19.97$

The remaining case, $v = 1837$, can be disposed of as follows. We apply a more general form of the indirect product (see [5]). Note that since there exists a TD(7, 12), there exists a PBD[{7, 13}, 85] with a flat of order 13. Also there exists a TD(25, 73) − TD(25, 1). Since $1837 = 25(85 - 12) + 12$, it is inessential in H^6. □

Lemma 4.11. *Let v be any integer such that $v \equiv 1 \pmod 6$ which satisfies $505 \leqslant v \leqslant 1069$. Then v is inessential in H^6 with the possible exception of v in the intervals $643 \leqslant v \leqslant 667$, $727 \leqslant v \leqslant 751$, or $v \in \{685, 691, 697, 709, 781, 787, 811, 1063, 1069\}$.*

Proof. We begin by using Lemma 4.3.

PBD with flat	flat	incomplete TD	max a	interval
$85 = 7.12 + 1$	13	$72 + a = 7.9 + 9 + a$	9	517–571
$91 = 7.13$	13	$78 + a = 7.11 + 1 + a$	11	559–625
$91 = 7.13$	7	$84 + a = 7.11 + 11 + a$	7	595–637
$133 = 7.19$	19	$114 + a = 7.16 + 2 + a$ (Corollary 4.6.1, $u = 0$)	15	817–907
$151 = 126 + 25$(RBIBD)	25	$126 + a = 7.17 + 7 + a$	17	907–1009
$151 = 126 + 25$(RBIBD)	7	$144 + a = 7.19 + 11 + a$	17	1015–1057

This covers all possibilities except those in the intervals listed below.

$$505 \leqslant v \leqslant 511$$
$$643 \leqslant v \leqslant 811$$
$$1063 \leqslant v \leqslant 1069$$

The remaining cases are treated below.

$505 = 7.72 + 1$	$757 = 7.108 + 1$	
$511 = 7.73$	$763 = 7.109$	
$673 = 7.96 + 1$	$769 = 48.16 + 1$	(Lemma 4.9)
$679 = 7.97$	$775 = 25.31$	
$703 = 19.37$	$793 = 13.61$	
$715 = 7.102 + 1$	$799 = 7.114 + 1$	
$721 = 7.103$	$805 = 7.115$	

These equations establish the lemma. □

Lemma 4.12. *The values of $v \in \{49, 85, 91, 133, 151, 169, 175, 187, 217, 247, 259, 301, 325, 337, 343, 385, 403, 427, 433, 463, 469, 475, 481\}$ are inessential in H^6.*

Proof. Consider the following.

$49 \in B(7)$	(AG(2, 7))	$325 = 13.25$	
$85 = 7.12 + 1$		$337 = 48.7 + 1$	(Lemma 4.9)
$91 = 7.13$		$343 = 7.49$	
$133 = 7.19$		$385 = 48.8 + 1$	(Lemma 4.9)
$151 = 126 + 25$	(RBIBD)	$403 = 13.31$	
$169 = 13^2$		$427 = 7.61$	
$175 = 7.25$		$433 = 48.9 + 1$	(Lemma 4.9)
$187 = 156 + 31$	(RBIBD)	$463 = 7.66 + 1$	
$217 = 7.31$		$469 = 7.67$	
$247 = 13.19$		$475 = 19.25$	
$259 = 7.37$		$481 = 13.37$	
$301 = 7.43$			

These conditions establish the lemma. □

The foregoing can be summarized as follows.

Theorem 4.13. *The* 98 *values given in Table* 3 *are a basis* H^6.

Table 3.

7	13	19	25	31	37	43	55	61	67
73	79	97	103	109	115	121	127	139	145
157	163	181	193	199	205	211	223	229	235
241	253	265	271	277	283	289	295	307	313
319	331	349	355	361	367	373	379	391	397
409	415	421	439	445	451	457	487	493	499
643	649	655	661	667	685	691	697	709	727
733	739	745	751	781	787	811	1063	1069	1231
1237	1243	1249	1255	1315	1321	1327	1543	1549	1567
1579	1585	1783	1789	1795	1801	1819	1831		

5. A basis for $\mathbf{H}^7$

In this section, we find a basis for H^7 which has fewer elements than that found for H^6. This is because both 7 and 8 are prime powers. The importance of this fact becomes apparent in Lemma 5.1.

Lemma 5.1. *The set* $V(7, 4530)$ *is a basis for* H^7.

Proof. Apply Lemma 2.3 with $a = 7$, $u = 8$, $w = 81$. □

The following lemmas are useful in improving this result.

Lemma 5.2. *Suppose that there exists a* PBD$[H^7, v]$ *which contains a flat of size* f. *If there exists a* TD$(8, v-f+a)$ *where* $a \in \{0, 1\}$, *then* $8v - 7f + 7a$ *is inessential in* H^7.

Proof. Again this is a special case of the indirect product (see [5]).

Lemma 5.3. *If there exists a* TD$(8, m)$ *where* $m \equiv 0$ *or* $1 \pmod 7$, $m > 1$, *then* $8m + 1$ *or* $8m$ *respectively is inessential in* H^7.

Proof. Immediate. □

Lemma 5.4. *If there exists a resolvable* BIBD$(v, 8, 1)$ *with* r *resolution classes, then* $7v + 7t + 1$ *is inessential in* H^7 *for* $0 \leqslant t \leqslant r$.

Proof. Since $\{57, 64\} \subset B(8)$, there exist group divisible designs GDD$[\{8\}]$ of group types 7^8 and 7^9 respectively.

Adjoin t new points to obtain a PBD$[\{8, 9, t\}, v+t]$, and form a group divisible design GDD$[\{8, 9\}]$ of type $1^v t^1$ by taking as groups the block of size t and the remaining points as groups of size 1. Apply Wilson's fundamental construction [11]. □

Lemma 5.5. *If there exists a* TD$(9, m)$, *then* $56m + 7t + 1$ *is inessential in* H^7 *for* $0 \leqslant t \leqslant m$.

Prrof. Apply Lemma 2.2 with $a = 7$ and $u = 8$.

Lemma 5.6. *Let* m *be an integer satisfying* $1 \leqslant m \leqslant 43$, *where* $m \equiv 1 \pmod 7$. *Then* $57m$ *is inessential in* H^7.

Proof. See [3], Theorem 3.8. □

Lemma 5.7. *Suppose that* v *is any integer satisfying* $v \equiv 1 \pmod 7$ *and* $v \geqslant 449$. *Then* v *is inessential in* H^7 *with the possible exception of* v *in the intervals* $575 \leqslant v \leqslant 610$, $701 \leqslant v \leqslant 722$, $827 \leqslant v \leqslant 834$, $1205 \leqslant v \leqslant 1226$, $1261 \leqslant v \leqslant 1282$, $2031 \leqslant v \leqslant 2045$ *or* $v = 2066$.

Proof. Begin by applying Lemma 5.5

m	$56m+1$	$63m+1$
8	449	505
9	505	568
11	617	694
13	729	820

Now use Lemma 5.4 and the fact that there exists an RBIBD(120, 8, 1) to cover the following interval.

$$841 \leq v \leq 960.$$

Continue with Lemma 5.5.

m	$56m+1$	$63m+1$
17	953	1072
19	1065	1198
23	1289	1450
25	1401	1576
27	1513	1702
29	1625	1828
32	1793	2017
37	2073	2332
41	2297	2584
43	2409	2710
47	2633	2962
53	2969	3340
59	3305	3718
61	3417	3844
67	3753	4222
73	4089	4600

These cover all required v except for v in the intervals below.

$$575 \leq v \leq 610$$
$$701 \leq v \leq 722$$
$$827 \leq v \leq 834$$
$$1205 \leq v \leq 1282$$
$$2024 \leq v \leq 2066$$

For the remaining cases, note the following equations.

$$1233 = 8.154 + 1$$
$$1240 = 8.155$$
$$1247 = 29.43$$
$$1254 = 22.57 \qquad \text{(Lemma 5.6)}$$
$$2024 = 8.253$$
$$2052 = 36.57 \qquad \text{(Lemma 5.6)}$$
$$2059 = 29.71$$

This completes the proof. □

Lemma 5.8. *The elements* {57, 64, 120, 232, 288, 344, 393, 400, 407, 435, 449} *are inessential in* H^7.

Proof. Consider the following.

$57 \in B(8)$	PG(2, 7)
$64 \in B(8)$	AG(2, 8)
$120 \in B(8)$	
$232 = 8.29$	
$288 \in B(8)$	(See [1])
$344 \in B(8)$	$7^3 + 1$ (See [7])
$393 = 8.49 + 1$	
$400 \in B(8)$	Lines in PG(3, 7)
$407 = 8.50 + 7$	(Lemma 5.2)
$435 = 15.29$	
$449 = 8.56 + 1$	

This completes the lemma. □

As a result of the above, we have the following.

Theorem 5.9. *The* 77 *values given in Table* 4 *are a basis for* H^7.

Table 4. A basis for H^7.

8	15	22	29	36	43	50	71	78	85
92	99	106	113	127	134	141	148	155	162
169	176	183	190	197	204	211	218	225	239
246	253	260	267	274	281	295	302	309	316
323	330	337	351	358	365	372	379	386	414
421	428	442	575	582	589	596	603	610	701
708	715	722	827	834	1205	1212	1219	1226	1261
1268	1275	1282	2031	2038	2045	2066			

Acknowledgement

The author wishes to thank the referees for their enormous assistance with this paper.

References

[1] L. Bagchi, Private communication.
[2] A.E. Brouwer, The number of mutually orthogonal latin squares – a table of up to order 10000, Mathematisch Centrum, report ZW 123/79, Amsterdam, June 1979.
[3] A.E. Brouwer and G.H.J. van Rees, More mutually orthogonal latin squres, Discrete Math. 39 (1982) 263–281.
[4] R. Mathon and A. Rosa, Tables for parameters of BIBDs with $r \geq 41$ including existence, enumeration, and resolvability results, Annals Discrete Math. 26 (1985) 275–308.

[5] R.C. Mullin, On the extension of the Moore–Sade construction for combinatorial configurations, Congressus Numerantium 23 (1979) 87–102.
[6] R.C. Mullin and D.R. Stinson, Pairwise balanced designs with block sizes $6t+1$, Graphs and Combinatorics 3 (1987) 365–377.
[7] E. Seiden, A method of construction of resolvable BIBD, Sankhya 25A (1963) 393–394.
[8] D.R. Stinson, The distance between units in rings – an algorithmic approach, Utilitas Math. 15 (1979) 281–292.
[9] R.M. Wilson, An existence theory for pairwise balanced designs I: Composition theorems and morphisms, J. Combin. Theory (A) 13 (1972) 220–245.
[10] R.M. Wilson, An existence theory for pairwise balanced designs III: Proof of the existence conjecture, J. Combin. Theory (A) 18 (1975) 71–79.
[11] R.M. Wilson, Constructions and uses of pairwise balanced designs, Math. Centre Tracts 55 (Amsterdam 1975) 18–41.
[12] R.M. Wilson, Concerning the number of mutually orthogonal latin squares, Discrete Math. 9 (1974) 181–198.
[13] R.M. Wilson, A few more squares, Congressus Numerantium X (1974) 675–680.
[14] L. Zhu, B. Du and J. Yin, Some new balanced incomplete block designs with $k=6$ and $\lambda=1$, Ars Combinatoria 24 (1987) 185–192.

Discrete Mathematics 77 (1989) 237–254
North-Holland

ON THE CONSTRUCTIVE ENUMERATION OF PACKINGS AND COVERINGS OF INDEX ONE

A.J. PETRENJUK
Department of Higher Mathematics, Kirovograd College of Civil Aviation, Kirovograd, U.S.S.R.

0. Introduction

We discuss two methods of constructive enumeration of packings. Their common feature is that they both use certain systems of linear equations and inequalities whose integer solutions are interpreted as packings. The paper also describes results obtained by applying these methods.

Denote by Z^+ the set of nonnegative integers. Put $I(n) = \{1, 2, \dots, n\}$.

1. Main definitions and the formulation of the problem

Let E be a finite set, $|E| = v$, and let λ, l, k be integers, $1 < l < k < v$. A collection $\mathscr{B}$ of k-subsets (k-blocks) of E is called a *(λ, l, k, v)-packing* [1, 3] if every l-subset of E is contained in at most λ blocks of $\mathscr{B}$. The number of nonisomorphic (λ, l, k, v)-packings consisting of t blocks is denoted by $N_t(\lambda, l, k, v)$. When $\lambda = 1$, we have a *packing of index one.*

Denote by $P_t(\lambda, l, k, v)$ the set of all (λ, l, k, v)-packings consisting of t blocks, by $\bar{P}_t(\lambda, l, k, v)$ the set of representatives of isomorphism classes in $P_t(\lambda, l, k, v)$, one representative from each class. Clearly, $N_t(\lambda, l, k, v) = |\bar{P}_t(\lambda, l, k, v)|$.

A (λ, l, k, v)-packing consisting of m blocks is *maximum* if there exists no (λ, l, k, v)-packing consisting of $m + 1$ blocks. In such a case, we define $D(\lambda, l, k, v) = m$.

We are interested in the following: (1) values of $D(\lambda, l, k, v)$, (2) values of $N_t(\lambda, l, k, v)$, and (3) construction of the lists $\bar{P}_t(\lambda, l, k, v)$.

It was shown in [3] that

$$D(1, l, k, v) \leqslant \left[\frac{v}{k}\left[\frac{v-1}{k-1}\left[\cdots\left[\frac{v-l+2}{k-l+2}\left[\frac{v-l+1}{k-l+1}\right]\right]\cdots\right]\right]\right]$$

and

$$D(1, 2, 3, v) = \begin{cases} \left[\dfrac{v}{3}\left[\dfrac{v-1}{2}\right]\right] & \text{if } v \not\equiv 5 \pmod 6 \\ \left[\dfrac{v}{3}\left[\dfrac{v-1}{2}\right]\right] - 1 & \text{if } v \equiv 5 \pmod 6 \end{cases}$$

where $[x]$ denotes the greatest integer not exceeding x.

In [5] (see also [12]) the following formula was obtained:

$$D(\lambda, 2, 3, v) = \left[\frac{v}{3}\left[\frac{v-1}{2}\right]\right] - \varepsilon$$

where

$$\varepsilon = \begin{cases} 1 & \text{if } v \equiv \lambda + 1 \equiv 2 \pmod 3 \text{ and } \lambda(v-1) \equiv 0 \pmod 2 \\ 0 & \text{otherwise.} \end{cases}$$

A (λ, l, k, v)-packing $\mathscr{B} = \{B_1, \ldots, B_m\}$ is called *maximal* if for every B, $B \subseteq E$, $|B| = k$, the collection $\{B, B_1, \ldots, B_m\}$ is not a (λ, l, k, v)-packing. In particular, maximum packings are all maximal. Define $N_{\max}(\lambda, l, k, v) = N_D(\lambda, l, k, v)$ where $D = D(\lambda, l, k, v)$.

The table below contains information taken from [12].

v	4	5	6	7	8	9
$N_{\max}(2, 2, 3, v)$	1	1	1	4	22	36

In what follows we describe a method of constructing and analyzing $(1, l, k, v)$-packings, as well as the results obtained by applying this method. These are summarized in the following table:

t	1	2	3	4	5	6	7	8	9	10	11	12
$N_t(1, 3, 5, 11)$	1	3	7	15	29	32	15	3	1	1	1	0

2. Adding a block

Consider a $(1, l, k, v)$-packing $\mathscr{B} = \{B_1, \ldots, B_m\}$. Define an equivalence $\sim$ on E as follows: $x \sim y$ $(x, y \in E)$ if and only if for every block B_i, $i \in I(m)$, either $\{x, y\} \subseteq B_i$, or both $x \notin B_i$, $y \notin B_i$. This equivalence is called *inseparability*, and its classes are *components of inseparability*.

For example, it is easily seen that the $(1, 3, 5, 11)$-packing

12345 12678 34679

induces inseparability of elements with components $X_1 = \{1, 2\}$, $X_2 = \{3, 4\}$, $X_3 = \{5\}$, $X_4 = \{6, 7\}$, $X_5 = \{8\}$, $X_6 = \{9\}$, $X_7 = \{10, 11\}$.

For convenience, let X_n always denote that (possibly empty) component of inseparability whose elements are not used in the packing.

Further, let a $(1, l, k, v)$-packing $\mathscr{B}$ induce on E the inseparability of elements with components $X_1, X_2, \ldots, X_n$, and let a new block, B, contain exactly $t_j = t(X_j)$ elements of X_j, $j \in I(n)$.

Necessary and sufficient conditions for the collection $\mathscr{B} = \{B, B_1, \ldots, B_m\}$ to be a $(1, l, k, v)$-packing are

$$\sum_{j=1}^{n} t(X_j) = k \tag{2.1}$$

$$\sum_{\{j:j<n, X_j \subseteq B_i\}} t(X_j) < l \quad \text{for all } i \in I(m). \tag{2.2}$$

In what follows we assume $E = I(v)$.

A solution $(t_1^{(0)}, t_2^{(0)}, \ldots, t_n^{(0)})$ of the system (2.1), (2.2), for which $t_j^{(0)} \in Z^+$ for all $j \in I(n)$, will be called a Z^+-solution. To every Z^+-solution $(t_1^{(0)}, \ldots, t_n^{(0)})$ of (2.1), (2.2) assign a k-block B_0, $B_0 \subseteq E$, containing exactly $t_j^{(0)}$ elements of X_j for all $j \in I(n)$, and moreover, these elements are the smallest in the linear order on E. It is easy to see that a packing $\{B, B_1, \ldots, B_m\}$ constructed without this order condition is isomorphic to the packing $\{B_0, B_1, \ldots, B_m\}$. The latter will be called *canonical.*

Clearly, the system (2.1), (2.2) will have no Z^+-solution if and only if the initial packing $\mathscr{B}$ is maximal.

Consider the set $\bar{P}_m(1, l, k, v)$. For every packing in $\bar{P}_m(1, l, k, v)$, let us write down the system (2.1), (2.2), find all its Z^+-solutions, and construct, for every Z^+-solution, the canonical packing. As a result we obtain a list of packings of size $m+1$ in which clearly every isomorphism class of $P_{m+1}(1, l, k, v)$ is represented by at least one representative. Thus if we perform isomorph rejection and delete from this list all duplicates, we obtain the set $\bar{P}_{m+1}(1, l, k, v)$.

Starting with the trivially obtained list $\bar{P}_1(1, l, k, v)$, we can construct recursively all lists $\bar{P}_m(1, l, k, v)$ for every $m \subseteq (D)$, $D = D(1, l, k, v)$.

The advantage of this method is in that elimination of all packings corresponding to the Z^+-solution of the system (2.1), (2.2), except for the canonical one, makes it possible to obtain lists that are not too extensive, especially during initial stages, i.e. for small m. In subsequent stages, when the initial packing contains many blocks, the same effect is achieved due to "tightness". We believe that these circumstances justify calling our construction method economical.

Note that the system (2.1), (2.2) does not take into account at all the fact that $B_1, \ldots, B_n$ are k-blocks. Therefore out method is applicable to more general packings, when the block size is allowed to vary.

3. Description of invariants

Below we describe invariants which are used to distinguish and identify packings.

The element repetition (ER) *count* in the packing $\mathscr{B} = \{B_1, \ldots, B_m\}$ is the vector

$$\mathrm{ER}(\mathcal{B}) = (p_0, p_1, \ldots)$$

where p_i is the number of elements in E which belong to exactly i blocks of $\mathcal{B}$. Evidently, $\sum p_i = v$.

The *Π-index* of a block B_i in the packing $\mathcal{B}$ is the vector

$$\Pi(B_i) = (q_0, q_1, \ldots)$$

where q_α is the number of elements in B_i belonging to exactly α blocks of $\mathcal{B}$. Π is a local characteristic of a block, invariant under any isomorphism of packings. Clearly, $\sum q_\alpha = k$.

The *element repetition count* by blocks (ERB) in $\mathcal{B}$ is given by the table

$$\mathrm{ERB}(\mathcal{B}) = \begin{array}{|c|ccc|} \hline q_0^{(1)} & q_1^{(1)} & \ldots & n_1 \\ \ldots & & & \\ q_0^{(v)} & q_1^{(v)} & \ldots & n_v \\ \hline \end{array}$$

where $n_u(u \in I(v))$ is the number of those blocks B in $\mathcal{B}$ for which $\Pi(B) = (q_0^{(u)}, q_1^{(u)}, \ldots)$. Evidently, $\sum n_u = m$.

The *index of intersections* of a block B in $\mathcal{B}$ is the vector

$$\mathrm{II}(B) = (\pi_0, \pi_1, \ldots)$$

where π_s is the number of blocks in $\mathcal{B}$ which have exactly s common elements with B. The *table of block intersections* in $\mathcal{B}$ is of the form

$$\mathrm{TI}(\mathcal{B}) = \begin{array}{|c|ccc|} \hline \pi_0^{(1)} & \pi_0^{(1)} & \ldots & h_1 \\ \ldots & & & \\ \pi_0^{(\omega)} & \pi_1^{(\omega)} & \ldots & h_\omega \\ \hline \end{array}$$

where h_ε denotes the number of blocks B in $\mathcal{B}$ for which $\mathrm{II}(B) = (\pi_0^{(\varepsilon)}, \pi_1^{(\varepsilon)}, \ldots)$. It follows from the definition that $\sum h_\varepsilon = m$.

It is easy to see that ER, ERB and TI are isomorphism invariants not only of packings but of arbitrary block collections.

The *triple block intersection count* (TBI) of a packing $\mathcal{B}$ is the vector

$$\mathrm{TBI}(\mathcal{B}) = (g_0, g_1, \ldots)$$

where g_i is the number of those triples of blocks in $\mathcal{B}$ which have exactly i common elements. By analogy we may define quadruple, quintuple etc. block intersection counts.

For example, the $(1, 3, 5, 11)$-packing

$$12345 \quad 12678 \quad 34679 \quad 136AB \quad 279AB \tag{3.1}$$

has $\mathrm{ER} = (0, 2, 4, 5, 0, 0, 0)$,

$$\mathrm{ERB} = \boxed{\begin{array}{cccccc} 0 & 0 & 2 & 3 & 0 & 2 \\ 0 & 0 & 3 & 2 & 0 & 1 \\ 0 & 1 & 0 & 4 & 0 & 1 \\ 0 & 1 & 1 & 3 & 0 & 1 \end{array}}, \quad \mathrm{TI} = \boxed{\begin{array}{cccc} 0 & 0 & 4 & 3 \\ 0 & 1 & 3 & 2 \end{array}}, \quad \mathrm{TBI} = (5, 5, 0).$$

The described invariants are used mainly to distinguish nonisomorphic packings. But the information obtained in the process of their construction, namely the correspondences "blocks – Π-indices" and "blocks – indices of intersections" are used to construct some invariants for identification of isomorphic packings.

For identification we use Venn-like diagrams or their collections. For example, the packing (3.1) yields a diagram presented in Fig. 1. Represent the two blocks with Π-index $(0, 0, 2, 3, 0)$ in the form of a Greek letter Λ, then "hang on them" the block with Π-index $(0, 1, 1, 3, 0)$. Elements of the block with $\Pi = (0, 1, 0, 4, 0)$ are circled, the elements of the last block are printed in bold type.

The values of the invariants ER, ERB and TI for the $(1, 3, 5, 11)$-packing

$$12345 \quad 12678 \quad 34679 \quad 136AB \quad 478AB \tag{3.2}$$

coincide with the respective values for the packing (3.1). Are these two packings isomorphic?

Let us construct for the packing (3.2) a diagram (Fig. 2) similar to Fig. 1. It is easy to see that there exist only two permutations on $I(11)$, namely $\alpha_1 = (13)(24)(89)$ and $\alpha_2 = (13)(24)(89)(AB)$ which superimpose Fig. 1 on Fig. 2. A direct verification shows that they both realize an isomorphism between (3.1) and (3.2). This illustrates how we identify packings.

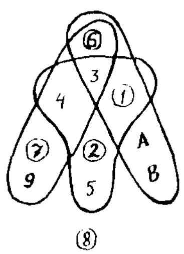


Fig. 1.

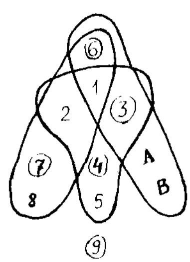


Fig. 2.

The diagrams described above are subinvariants, i.e. invariants which make sense for designs with equal values of other (basic) invariants, in this case of the invariant ERB. One often needs to use subinvariants which are collections of similar diagrams.

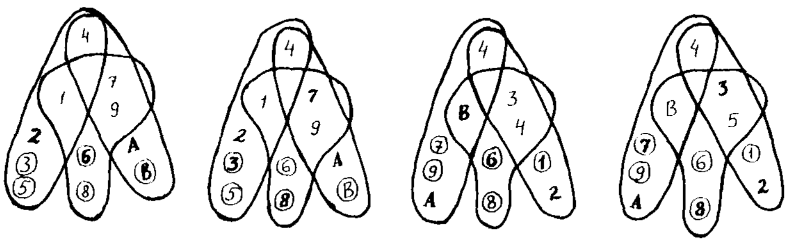


Fig. 3.

Note that similar invariants were used for distinguishing and identification of 1-factorizations [8, 9].

We give an example of finding automorphism groups (which, incidentally, were used with success to identify completions of packings) with the help of such diagrams. To the packing 6-5 (see the list below) corresponds the value

$$\mathrm{ERB} = \left|\begin{array}{cccccc|c} 0 & 0 & 0 & 5 & 0 & 0 & 2 \\ 0 & 0 & 1 & 4 & 0 & 0 & 2 \\ 0 & 0 & 2 & 3 & 0 & 0 & 2 \end{array}\right|$$

One of possible subinvariants for this packing has the value given in Fig. 3. Only two permutations, the identity and (1B)(2A)(37)(59) map this collection of diagrams into itself. It is verified directly that they constitute the automorphism group of the packing 6-5.

4. Results on the enumeration of (1, 3, 5, 11)-packings

A computer program implementation of the method presented in Section 2 enabled us to carry out a complete enumeration of the (1, 3, 5, 11)-packings. The results are presented below.

The list $\bar{P}_1$ (1, 3, 5, 11)

1-1. 12345

The list $\bar{P}_2$ (1, 3, 5, 11)

2-1. 12345 6789A
2-2. 12345 16789
2-3. 12345 12678

The list $\bar{P}_3$ (1, 3, 5, 11)

3-1. 12345 16789 1267B
3-2. 12345 16789 126AB
3-3. 12345 16789 2367A
3-4. 12345 16789 236AB
3-5. 12345 12678 1369A
3-6. 12345 12678 34679
3-7. 12345 12678 129AB

The list $\bar{P}_4\ (1,3,5,11)$

4-1.	12345	6789A	1267B	3489B
4-2.	12345	6789A	1267B	3468B
4-3.	12345	16789	126AB	378AB
4-4.	12345	12678	1369A	3467B
4-5.	12345	16789	2367A	468AB
4-6.	12345	16789	2367A	4568A
4-7.	12345	16789	2367A	4567B
4-8.	12345	16789	2367A	2468B
4-9.	12345	16789	126AB	3467A
4-10.	12345	16789	2367A	489AB
4-11.	12345	16789	236AB	457AB
4-12.	12345	16789	126AB	3478A
4-13.	12345	16789	2367A	4589A
4-14.	12345	12678	34679	1569A
4-15.	12345	12678	1369A	1479B

The list $\bar{P}_5\ (1,3,5,11)$

5-1.	12345	16789	126AB	347AB	589AB
5-2.	12345	16789	126AB	347AB	2589A
5-3.	12345	16789	2367A	248AB	569AB
5-4.	12345	6789A	1267B	3489B	356AB
5-5.	12345	16789	236AB	457AB	2489A
5-6.	12345	16789	2367A	2489A	4567B
5-7.	12345	16789	2367A	4567B	4589A
5-8.	12345	16789	126AB	3478A	3569A
5-9.	12345	16789	2367A	2489A	4568B
5-10.	12345	16789	2367A	4589A	146AB
5-11.	12345	16789	2367A	2468B	4589A
5-12.	12345	16789	2367A	248AB	4567B
5-13.	12345	16789	2367A	248AB	2569B
5-14.	12345	16789	126AB	347AB	2389A
5-15.	12345	16789	2367A	2489A	568AB
5-16.	12345	16789	126AB	347AB	3568A
5-17.	12345	16789	126AB	347AB	2578A
5-18.	12345	16789	2367A	2468B	156AB
5-19.	12345	16789	2367A	2489A	2568B
5-20.	12345	16789	2367A	2468B	4578A
5-21.	12345	16789	2367A	2489A	146AB
5-22.	12345	16789	2367A	2468B	147AB
5-23.	12345	6789A	1267B	1389B	4568B
5-24.	12345	12678	1369A	1479B	158AB
5-25.	12345	12678	34679	136AB	4568A
5-26.	12345	12678	34679	136AB	247AB

5-27.	12345	12678	34679	1389A	4568A		
5-27.	12345	12678	34679	1389A	4568A		
5-28.	12345	16789	126AB	3478A	3579B		
5-29.	12345	16789	126AB	347AB	3589A		

The list $\bar{P}_6$ (1, 3, 5, 11)

6-1.	12345	16789	2367A	148AB	259AB	4567B
6-2.	12345	16789	2367A	2489A	3468B	159AB
6-3.	12345	16789	126AB	3478A	2579B	3568B
6-4.	12345	16789	126AB	2378A	3479B	458AB
6-5.	12345	16789	126AB	2378A	479AB	3568B
6-6.	12345	16789	2367A	2489A	568AB	3479B
6-7.	12345	16789	2367A	248AB	4567B	359AB
6-8.	12345	16789	126AB	2378A	2479B	4569A
6-9.	12345	16789	126AB	3478A	2379B	3568B
6-10.	12345	16789	2367A	4589B	3578B	2468B
6-11.	12345	16789	2367A	2468B	147AB	3569B
6-12.	12345	16789	126AB	3478A	2379B	2589A
6-13.	12345	16789	2367A	2489A	2568B	457AB
6-14.	12345	16789	2367A	2468B	578AB	129AB
6-15.	12345	16789	2367A	2468B	147AB	569AB
6-16.	12345	16789	2367A	2489A	138AB	456AB
6-17.	12345	16789	126AB	347AB	2578A	3568B
6-18.	12345	16789	2367A	2468B	578AB	3489B
6-19.	12345	16789	2367A	2489A	2568B	146AB
6-20.	12345	16789	2367A	2489A	3468B	2578B
6-21.	12345	16789	2367A	2489A	138AB	3469B
6-22.	12345	6789A	1267B	1389B	346AB	4579B
6-23.	12345	12678	34679	1389A	236AB	3578B
6-24.	12345	12678	34679	1389A	236AB	1569B
6-25.	12345	12678	34679	1389A	236AB	4568A
6-26.	12345	12678	34679	1389A	4568B	2579A
6-27.	12345	16789	126AB	2378A	4567B	3489B
6-28.	12345	16789	2367A	2468B	4589A	157AB
6-29.	12345	16789	2367A	2468B	4589A	3579A
6-30.	12345	16789	126AB	3478A	2579A	3469B
6-31.	12345	16789	2367A	2489A	4567B	3589B
6-32.	12345	16789	2367A	4567B	4589A	2389B

The list $\bar{P}_7$ (1, 3, 5, 11)

7-1.	12345	16789	126AB	3478A	2379B	2589A	4567B
7-2.	12345	16789	126AB	2378A	2479B	4569A	3589B
7-3.	12345	16789	2367A	2468B	4589A	3579B	156AB
7-4.	12345	16789	2367A	2468B	147AB	3569B	2589A
7-5.	12345	16789	126AB	3478A	2379B	3568B	459AB
7-6.	12345	16789	2367A	2489A	2568B	146AB	4579B

7-7.	12345	16789	2367A	2489A	138AB	3469B	2578B
7-8.	12345	16789	2367A	2468A	578AB	129AB	4569A
7-9.	12345	16789	2367A	2469A	2568B	457AB	3469B
7-10.	12345	16789	2367A	2468B	147AB	569AB	3578B
7-11.	12345	16789	2367A	2489A	2568B	146AB	3478B
7-12.	12345	6789A	1267B	1389B	346AB	4579B	258AB
7-13.	12345	12678	34679	1389A	236AB	4568A	2579A
7-14.	12345	12678	34679	1389A	236AB	4568A	1569B
7-15.	12345	12678	34679	1389A	236AB	4568A	147AB

The list $\bar{P}_8\ (1,3,5,11)$

8-1.	12345	16789	2367A	2468B	578AB	129AB	4569A	3479B
8-2.	12345	12678	34679	1389A	236AB	4568A	147AB	1569B
8-3.	12345	12678	34679	1389A	236AB	4568A	3579A	3578B

The list $\bar{P}_9\ (1,3,5,11)$

9-1. 12345 12678 34679 1389A 236AB 4568A 147AB 1569B 2489B

The list $\bar{P}_{10}\ (1,3,5,11)$

10-1. (9-1) + 3578B

The list $\bar{P}_{11}\ (1,3,5,11)$

11-1. (9-1) + 3578B 2579A

The last packing is maximal, hence $D(1, 3, 5, 11) = 11$. From the lists given above one can obtain the values $D(1, 3, 5, v)$ for $v < 11$. These values are given in the following table.

v	7	8	9	10
$D(1, 3, 5, v)$	1	2	3	5
Maximum packing	1-1	2-3	3-6	5-27

Consider the case $k = 6$. The list $\bar{P}_1(1, 3, 6, 11)$ consists of a unique packing 123456, the list $\bar{P}_2(1, 3, 6, 11)$ consists of two packings

2-1. 123456 1789AB

2-2. 123456 12789A,

hence $N_1(1, 3, 6, 11) = 1$, $N_2(1, 3, 6, 11) = 2$. The packings from $\bar{P}_2(1, 3, 6, 11)$ are both maximal therefore $\bar{P}_t(1, 3, 6, 11) = \emptyset$ for $t \geqslant 3$. Thus $D(1, 3, 6, 11) = 2$.

An obvious reasoning yields $D(1, 3, k, 11) = 1$ for $6 < k < 11$.

5. Enumeration of minimal exact (1, 3, 11)-coverings

An interesting application of the above results is associated with the question about the minimal number $g(1, 3, 11)$ of blocks in an exact $(1, 3, 11)$-covering [6]. Just as was done in [6] for the case $v = 12$, one can show (see [10], Theorem 7.2) that if $g(1, 3, 11) < 46$ then a minimal $(1, 3, 11)$-covering contains only quintuples, quadruples and triples.

Denote by F the set of 5-blocks (*F-component*) of a covering, by Q the set of 4-blocks (*Q-component*), and by T the set of triples (*T-component*). Then, up to an isomorphism, it is either one of the $(1, 3, 5, 11)$-packings in Section 4, or the empty set of blocks, that can be the F-component.

Taking for the F-component one of these packings, F, examine all possible Q-components with a maximum number of blocks of an exact $(1, 3, 11)$-covering. Define an equivalence $\sim$ in the set of such Q-components by: $Q \sim Q_1$ if and only if there exists $\alpha \in \mathrm{Aut}(F)$ such that $Q_\alpha = Q_1$.

Construct a list $q(F)$ of representatives of equivalence classes under $\sim$. Every $Q \in q(F)$ uniquely determines the T-component. Call the exact $(1, 3, 11)$-coverings so obtained *F-minimal*. Construct, for every F from Section 4, a list of all F-minimal $(1, 3, 11)$-coverings. Evidently, the union of these lists contains all minimal $(1, 3, 11)$-coverings with maximum block size $k = 5$.

After completing the described procedure, we obtain a complete list of minimal exact $(1, 3, 11)$-coverings, and, consequently, we may determine $g(1, 3, 11)$.

The author has written a program that implements the above algorithm. The work is at present incomplete. We state below the results obtained up to the time this paper was written.

For the F-component 11-1 the maximal Q-component is empty. Consequently, there exists a unique exact $(1, 3, 11)$-covering with this F-component. Its size is 66.

For the F-component 10-1 there exists, up to an isomorphism, a unique F-maximal Q-component which consists of the unique block 2579. Hence for 10-1 there exists a unique F-minimal covering of size 72.

For the F-component 9-1 there exists a unique maximal Q-component

257B 259A 357A 358B 5789,

and the size of the corresponding F-minimal covering is 69.

For the F-component 8-1 the unique maximal Q-component consists of seven blocks

138B 147A 156B 2389 2579 348A 3568,

and the unique F-minimal $(1, 3, 11)$-covering consists of 72 blocks. For 8-2 two maximal Q-components exist:

2389 257A 258B 279B 348B 357B 5789,

2489 258B 259A 279B 348B 357A 5789.

The corresponding nonisomorphic coverings have 72 blocks each. Finally, for 8-3 there exist two maximal Q-components,

129B 146B 147A 1569 15AB 247B 2489 459B 689B

and

129B 146B 147A 1569 15AB 247B 2489 49AB 689B,

Table 1

F	Aut	$\lvert Q\rvert$	Nq	$\lvert q\rvert$	$\lvert\Pi\rvert$	Spg
7-1	3	10	1	1	72	3^1
7-2	2	12	2	2	66	2^2
7-3	12	17	1	1	51	12^1
7-4	2	11	1	1	69	2^1
7-5	1	11	1	1	69	1^1
7-6	1	11	16	16	69	1^{16}
7-7	2	12	34	17	66	1^{17}
7-8	1	12	1	1	66	1^1
7-9	1	12	3	3	66	1^3
7-10	2	11	9	5	66	$1^4 2^1$
7-11	1	12	33	33	66	1^{33}
7-12	20	15	1	1	57	20^1
7-13	12	16	1	1	54	12^1
7-14	4	12	16	6	66	$1^2 2^4$
7-15	6	11	588	100	69	$1^{99} 2^1$

and the corresponding two F-minimal $(1,3,11)$-coverings have size 65.

The results for the F-components having 7 blocks are presented in Table 1. Column F contains the numbers of the F-components, column Aut the order of the automorphism group of F, column $|Q|$ the size of the maximal Q-component, Nq the number of distinct maximal Q-components, $|q|$ the cardinality of $q(F)$, $|\Pi|$ the size of F-minimal $(1,3,11)$-covering, and Spg contains a specification of the set of F-minimal coverings by automorphism group orders.

Most of the above results are contained in [11].

Table 2 (next page) contains similar information about F-maximal Q-components of $(1,3,11)$-coverings with $|F|=6$. The additional column b contains, for every F, the cardinality of the set of those 4-blocks which have at most two common elements with every block of F.

The enumeration of minimal $(1,3,11)$-coverings for $|F|\leq 5$ is being continued.

6. List of coverings of size 51

The smallest known size (see [10]) of an exact $(1,3,11)$-covering with block cardinality $k\leq 5$ is 51. There exist exactly 11 nonisomorphic coverings with $|F|>5$. They are as follows:

1. 7-3 + 127B 128A 138B 139A 147A 149B 2389 2479 2569
   2578 29AB 3469 3478 34AB 3568 4567 78AB
2. 6-22 + 158A 137A 1468 149A 1569 1578 15AB 2368 2379 2469
   247A 248B 256A 2589 29AB 3478 3467 359A 458A 568B
3. 6-29 + 127B 128A 136B 139A 146A 157A 158B 2389 2479 2569 2578
   25AB 3469 3478 34AB 3568 4567 69AB 78AB 149B Aut = 48
4. 6-29 + (first fifteen 4-blocks from covering 3.) + 3568 38AB 4567
   47AB 69AB Aut = 8

Table 2

F	b	Aut	$\lvert Q\rvert$	Nq	$\lvert q\rvert$	$\lvert \Pi\rvert$	Spg
6-1	44	1	15	106	106	66	1^{106}
6-2	42	1	15	5	5	66	1^{5}
6-3	42	1	15	11	11	66	1^{11}
6-4	43	1	15	25	25	66	1^{25}
6-5	42	2	16	5	3	63	$1^{2}2^{1}$
6-6	40	4	15	2	1	66	1^{1}
6-7	42	24	18	2	1	57	12^{1}
6-8	49	1	18	12	12	57	1^{12}
6-9	48	1	14	207	207	69	1^{207}
6-10	47	4	15	576	172	66	$1^{116}2^{56}$
6-11	49	1	16	22	22	63	1^{22}
6-12	49	1	16	3	3	63	1^{3}
6-13	48	1	15	30	30	66	1^{30}
6-14	48	2	16	5	3	63	1^{3}
6-15	48	1	16	13	13	63	1^{13}
6-16	49	1	15	72	72	66	1^{72}
6-17	50	1	17	4	4	60	1^{4}
6-18	47	2	15	87	47	66	$1^{46}2^{1}$
6-19	55	1	16	24	24	63	1^{24}
6-20	54	2	16	24	23	63	1^{23}
6-21	56	1	16	60	60	63	1^{60}
6-22	56	4	20	1	1	51	1^{1}
6-23	60	1	16	5	1	63	1^{1}
6-24	61	12	15	51	7	66	$1^{2}2^{4}4^{1}$
6-25	62	2	18	66	3	57	1^{3}
6-26	65	60	17	395	7	60	$1^{5}3^{2}$
6-27	43	3	15	94	35	66	$1^{32}3^{3}$
6-28	42	4	16	138	45	63	$1^{25}2^{18}4^{2}$
6-29	40	48	20	10	3	51	$8^{1}16^{1}48^{1}$
6-30	45	3	16	12	4	63	1^{4}
6-31	46	16	16	120	98	63	$1^{58}2^{32}4^{8}$
6-32	48	384	20	128	6	51	$8^{2}48^{4}$

5. 6-29 + (first twelve 4-blocks from covering 3.) + 29AB 3469 3478 3568 38AB 4567 47AB 56AB Aut = 16
6. 6-32 + 126B 128A 137B 139A 146A 148B 157A 159B 2468 2479 24AB 2569 2578 3469 3478 3468 3579 35AB 68AB 79AB Aut = 48
7. 6-32 + (first 19 quadruples from the previous covering) + 78AB Aut = 8
8. 6-32 + (first 10 quadruples from covering 6.) + 2569 2578 25AB 3469 3478 3568 69AB 78AB Aut = 48
9. 6-32 + (first 13 quadruples from covering 6.) + 3468 3478 3569 3578 35AB 68AB 79AB Aut = 48
10. 6-32 + (first 8 quadruples from covering 6.) + 2469 2478 24AB 2568 2579 3479 3569 3578 35AB 69AB 78AB Aut = 8
11. 6-32 + (first 10 quadruples from the previous design) + 2568 2579 25AB 3468 3479 34AB 3569 3578 69AB 78AB Aut = 48

7. Bounds for possible values of $g(1, 3, 11)$

Let Π be a minimal exact $(1, 3, 11)$-covering with maximal block cardinality $k = 5$, $|\Pi| = g$. We are taking into account the fact that $g < 46$ is possibly only for coverings with blocks whose cardinalities do not exceed five. Denote by f, q, and t, respectively, the cardinalities of F-, Q-, and T-components of this covering. Then we have [6]

$$\begin{cases} f + q + t = g \\ 10f + 4q + t = 165, \end{cases}$$

whence

$$9f + 3q = 165 - g, \quad \text{or } q = (165 - g - 9f)/3.$$

It is not difficult to show [6] that $g \in \{30, 33, 36, 39, 42, 45, 46\}$. Taking into account the obvious inequality $q \leqslant g - f$ we get $(165 - g - 9f)/3 \leqslant g - f$ whence $f \geqslant (165 - 4g)/6$. Assuming $g = 30$ gives $f \geqslant 8$. But it was shown earlier that for $f \geqslant 8$ there exist no exact coverings with 30 blocks. Therefore $g(1, 3, 11) \neq 30$.

Assuming now $g = 33$, we get similarly that $f \geqslant 6$. But Table 2 excludes the existence of such a covering, thus $g(1, 3, 11) \neq 33$.

Theorem. $g(1, 3, 11) \in \{36, 39, 42, 45, 46\}$.

Note that in [4] a stronger inclusion $g(1, 3, 11) \in \{45, 46\}$ is proved.

8. Some properties of $N_t(\lambda, l, k, v)$

Let us note some general properties of the numbers $N_t(\lambda, l, k, v)$. Clearly for $k < v$ we have $N_1(1, l, k, v) = 1$. Also, it is not difficult to establish directly that

$$N_2(1, l, k, v) = \begin{cases} 0 & \text{for } v < 2k - l + 1 \\ i + 1 & \text{for } v = 2k - l + i + 1, \quad 0 \leqslant i < l - 1, \\ l & \text{for } v > 2k. \end{cases} \tag{8.1}$$

Null-property:

$$N_t(\lambda, l, k, v) = 0 \quad \text{for } v < v_0(t, \lambda, l, k) \text{ and } t > 1.$$

It follows from (8.1) that $v_0(2, 1, l, k) = 2k - l + 1$. It is not difficult to see that $v_0(3, 1, l, k) = 3(k - l + 1) + l - 1$.

Monotonicity:

$$N_t(\lambda, l, k, v) \qquad N_t(\lambda, l, k, v + 1), \tag{8.2}$$

and the inequality is strict for $v < tk$ if at least one of its sides is not equal to zero.

Stabilization by v:

$$N_t(1, l, k, w) = \text{const} = N_t(1, l, k, th) \tag{8.3}$$

for all $w \geqslant tk$.

Stabilization by k:

For fixed t and l, under the conditions $k > k_0 = (t-1)(l-1)$ and $v \geqslant t(k+1)$, the following equality holds:

$$N_t(1, l, k, v) = N_t(1, l, k+1, v). \tag{8.4}$$

9. Another approach to the packing problem

Let $\mathcal{B} = \{B_1, \ldots, B_t\}$ be a $(1, l, k, v)$-packing. Denote by E_J the set of elements which are contained only in the blocks numbered by indices from J, $J \subseteq I(t)$. Clearly, E_J's are just the same as components of inseparability in Section 2. Put $n_J = |E_J|$. It follows from the definition of packing that

$$\sum_{J \ni m} n_J = k \quad \text{for every } m \in I(t); \tag{9.1}$$

$$\sum_{J \ni i,j} n_J < l \quad \text{for all } i, j \in I(t), \quad i \neq j; \tag{9.2}$$

$$\sum_J n_J = v. \tag{9.3}$$

Conversely, given a collection $\{n_J : J \subseteq I(t)\}$ which satisfies (9.1)–(9.3), it is not difficult to obtain the corresponding packing. Thus the conditions (9.1)–(9.3) are necessary and sufficient for the existence of a packing corresponding to the collection of numbers $\{n_J\}$.

Packings corresponding to the same collection $\{n_J\}$ are clearly isomorphic. But it is possible for different collections to yield isomorphic packings. In order for $\{n_J\}$ to be a complete invariant for packings, it is necessary to have, in addition to (9.1)–(9.3), conditions for selecting from among all collections yielding the same packing one (canonical) collection $\{n_J\}$.

Consider the case $t = 3$. In this case conditions (9.1)–(9.3) become

$$\begin{cases} n_1 + n_{12} + n_{13} + n_{123} = k \\ n_2 + n_{12} + n_{23} + n_{123} = k \\ n_3 + n_{13} + n_{23} + n_{123} = k \\ n_{12} + n_{123} < l \\ n_{13} + n_{123} < l \\ n_{23} + n_{123} < l \\ n_0 + n_1 + n_2 + n_3 + n_{12} + n_{13} + n_{23} + n_{123} = v. \end{cases} \tag{9.4}$$

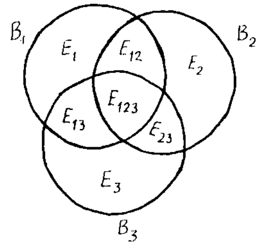


Fig. 4.

The structure of a packing with $t = 3$ is schematically drawn in Fig. 4.

To reach our goal it suffices to require that the preference conditions given in Fig. 5 be satisfied. Here + means that the collection n_J is being made canonical, i.e. included in the list, and − means that it is being rejected.

Table 3 contains author's program in Fortran-4 which implements, for given l, k and v, the construction of all collections

$$n_0, n_1, n_2, n_3, n_{12}, n_{13}, n_{23}, n_{123}$$

that satisfy conditions (9.1)–(9.3), and the selection from them of canonical ones.

Table 4 contains an example of the final output of the program: for given l, k and v it outputs the value of $N_3(1, l, k, v)$ and the list of vectors $(n_{123}, n_{12}, n_{13}, n_{23})$ which determine all nonisomorphic packings.

Table 5 contains several values of $N_3(1, l, k, v)$ obtained by means of this program. This table may be considerably expanded.

In the case $t = 4$ it is not difficult to implement a generation of collections $\{n_J\}$ and a "sieve" through conditions (9.1)–(9.3). More complicated but quite feasible task is to form a preference scheme.

Note that for arbitrary t there are exactly 2^t n_J's, thus the size of the system (9.1)–(9.3) grows fast. This complicates the practical implementation of the method, described in Section 9, for the large values of t.

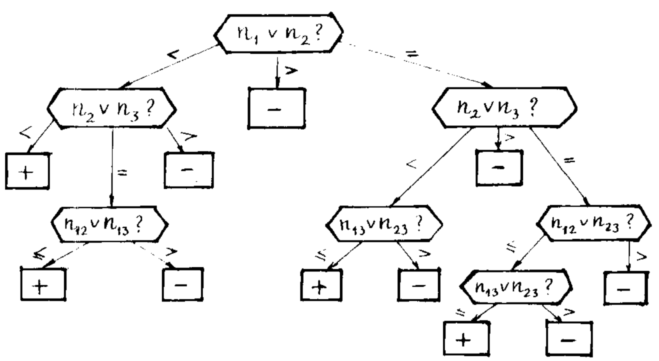


Fig. 5.

Table 3. Program for computing $N_3(1, l, k, v)$.

```
C FIND VALUE N3(1,L,K,V)
      DIMENSION MT (500, 4)
  117 READ 1, NV, NK, NL
    1 FORMAT (3I3)
      IF (NV) 119, 119, 118
  118 NS = 0
      M = 0
      IF (NV - 3*NK + 3*(NL - 1))115, 111, 111
  111 DO 2 I = 1, NL
      DO 2 J = I, NL
      DO 2 K = J, NL
      I1 = I - 1
      J1 = J - 1
      K1 = K + 1
      IF (I1 + J1 + NS - NK)3, 3, 2
    3 IF (I1 + K1 + NS - NK)4, 4, 2
    4 IF (J1 + K1 + NS - NK)5, 5, 2
    5 IF (I1 - NL + NS + 1)6, 6, 2
    6 IF (J1 - NL + NS + 1)7, 7, 2
    7 IF (K1 - NL + NS + 1)8, 8, 2
    8 IF (I1 + J1 + K1 - 3*NK + 2*NS + NV)2, 9, 9
    9 IF (I1 + J1 + K1 + NS - NV)19, 19, 2
   19 M = M + 1
      MT(M, 1) = NS
      MT(M, 2) = I1
      MT(M, 3) = J1
      MT(M, 4) = K1
    2 CONTINUE
      IF (NS - NL + 1)121, 115, 115
  121 NS = NS + 1
      GO TO 111
  115 PRINT 10, NL, NK, NV, M
   10 FORMAT (5X,'N3(1,',I3,',',I3,',',I3,') = ',I3)
      IF (M) 117, 117, 125
  125 CONTINUE
      PRINT 11, ((MT(I, J), J = 1, 4), I = 1, M)
   11 FORMAT (3X, 4I3, 2X, 4I3, 2X, 4I3, 2X, 4I3)
      GO TO 117
  119 PRINT 120
  120 FORMAT (3X, 'WORK IS FINISHED')
      STOP
      END
```

Table 4. Final output of the program N3LKV.

N3(1, 3, 4, 13) = 15

0 0 0 0	0 0 0 1	0 0 0 2	0 0 1 1
0 0 1 2	0 0 2 2	0 1 1 1	0 1 1 2
0 1 2 2	0 2 2 2	1 0 0 0	1 0 0 1
1 0 1 1	1 1 1 1	2 0 0 0	

Table 5. Some values of $N_3(1, l, k, v)$.

l	k	v	N_3	l	k	v	N_3	l	k	v	N_3	l	k	v	N_3
2	3	$\leqslant 5$	0	3	4	11	14	4	5	8	4	4	8	20	26
		6	1			$\geqslant 12$	15			9	10			21	30
		7	3	3	5	$\leqslant 8$	0			10	16			22	33
		8	4			9	1			11	22			23	34
		$\geqslant 9$	5			10	3			12	26			$\leqslant 24$	35
2	4	$\leqslant 8$	0			11	7			13	29	5	6	7	0
		9	1			12	10			14	30			8	1
		10	3			13	13			$\geqslant 15$	31			9	5
		11	4			14	14	4	6	$\leqslant 8$	0			10	13
		$\geqslant 12$	5			$\geqslant 15$	15			9	1			11	22
2	5	$\leqslant 11$	0	3	6	$\leqslant 11$	0			10	3			12	33
		12	1			12	1			11	7			13	41
		13	3			13	3			12	14			14	48
		14	4			14	7			13	20			15	52
		$\geqslant 15$	5			15	10			14	26			16	55
2	6	$\leqslant 14$	0			16	13			15	30			17	56
		15	1			17	14			16	33			$\geqslant 18$	57
		16	3			$\geqslant 18$	15			17	34	5	7	$\leqslant 9$	0
		17	4	3	7	$\leqslant 14$	0			$\geqslant 18$	35			10	1
		18	5			15	1	4	7	$\leqslant 11$	0			11	4
2	7	$\geqslant 17$	0			16	3			12	1			12	10
		$\leqslant 18$	1			17	7			13	3			13	20
		19	3			18	10			14	7			14	30
		20	4			19	13			15	14			15	41
		$\geqslant 21$	5			20	14			16	20			16	49
2	8	$\geqslant 20$	0			$\geqslant 21$	15			17	26			17	56
		$\leqslant 21$	1	3	8	$\leqslant 17$	0			18	30			18	60
		22	3			18	1			19	33			19	63
		23	4			19	3			20	34			20	64
		$\geqslant 24$	5			20	7			$\geqslant 21$	35			$\geqslant 21$	65
3	4	5	0			21	10	4	8	$\leqslant 14$	0	5	8	$\leqslant 11$	0
		6	1			22	13			15	1			12	1
		7	3			23	14			16	3			13	3
		8	7			$\geqslant 24$	15			17	7			14	7
		9	10	4	5	6	0			18	14			15	14
		10	13			7	1			19	20			16	25
														17	35
5	8	18	46	6	7	18	88	6	8	23	109	7	8	$\geqslant 24$	144
		19	54			19	91			$\geqslant 24$	110	4	11	$\leqslant 23$	0
		20	61			20	92	7	8	9	0			24	1
		21	65			$\geqslant 21$	93			10	1			25	3
		22	68	6	8	$\leqslant 10$	0			11	5			26	7
		23	69			11	1			12	15			27	14
		$\geqslant 24$	70			12	5			13	29			28	20
6	7	8	0			13	13			14	48			29	26
		9	1			14	26			15	68			30	30
		10	5			15	41			16	89			31	33
		11	14			16	58			17	105			32	34
		12	26			17	72			18	119			$\geqslant 33$	35
		13	41			18	85			19	128	3	15	40	3
		14	55			19	94			20	135	3	15	41	7
		15	68			20	101			21	139	4	15	40	20
		16	77			21	105			22	142	6	10	25	110
		17	84			22	108			23	143				

10. Conclusion

We conclude with two particular problems:

1. What is the number $N_t(\lambda, l, k, v)$ of maximal (λ, l, k, v)-packings containing exactly t blocks?
2. What is the minimal size $T(\lambda, l, k, v)$ of a minimal (λ, l, k, v)-packing?

References

[1] M.K. Fort and G.A. Hedlund, Minimal coverings of pairs by triples, Pacific J. Math. 8 (1958) 709–719.
[2] J. Schönheim, On coverings, Pacific J. Math. 14 (1964) 1405–1411.
[3] J. Schönheim, On maximal systems of k-tuples, Studia Sci. Math. Hungar. 1 (1966) 363–368.
[4] J.L. Allston, R.G. Stanton and A. Wirmani-Prasad, Computation of the exact covering number $g(1, 3, 11)$, Utilitas Math. 28 (1985) 193–200.
[5] H. Hanani, Balanced incomplete block designs and related designs, Discrete Math. 11 (1975) 255–369.
[6] R.G. Stanton and P.H. Dirksen, Computation of $g(1, 3, 12)$, Lecture Notes Math. 560 (Springer, 1976) 232–239.
[7] R.G. Stanton, Old and new results on perfect coverings, Lecture Notes Math. 952 (Springer, 1981) 142–149.
[8] I.P. Neporoznev and A.J. Petrenjuk, Konstruktivnoye perečislenie sistem grupp par i oglavlennye sistemy trojek Štejnera, Kombinatornyj Analiz, 2 (Moscow 1972) 17–37.
[9] L.P. Petrenjuk and A.J. Petrenjuk, O perečislenii soversennykh 1-faktorizacii polnykh grafov, Kibernetika (Kiev, 1980) No. 1, 6–8.
[10] A.J. Petrenjuk, Extremal'nye točnye kombinatornye pokrytia (Kirovograd Inst. Agricultural Machinery, Kirovograd, 1985) 36 pp. (Deposited in UkrNIINTI, No. 910 Uk-85Dep.)
[11] A.J. Petrenjuk, O konstruktivnom perečislenii upakovok i pokrytii, Kirovograd (Inst. Agricultural Machinery, Kirovograd, 1985) 18 pp. (Deposited in UkrNIINTI, No. 1366 Uk-85Dep.)
[12] R.G. Stanton, M.J. Rogers, R.F. Quinn and D.D. Cowan, Bipackings of pairs by triples, and isomorphism classes of small bipackings, J. Austral. Math. Soc. (A) 34 (1983) 214–228.

Discrete Mathematics 77 (1989) 255–258
North-Holland

THE EXISTENCE OF SIMPLE $S_3(3, 4, v)$

K. PHELPS, D.R. STINSON and S.A. VANSTONE

Department of Mathematics, Georgia Institute of Technology, Atlanta, Georgia, U.S.A.
Department of Computer Science, University of Manitoba, Winnipeg, Manitoba, R3T 2N2 Canada
Department of Combinatories & Optimization, University of Waterloo, Waterloo, Ontario, N2L 3G1 Canada

It has been known for some time that an $S_3(3, 4, v)$ exists iff v is even. The constructions which prove this result, in general, give designs having repeated blocks. Recently, it was shown that a simple $S_3(3, 4, v)$ exists if v is even and $v \not\equiv 4 \pmod{12}$. In this paper we give an elementary proof of the existence of simple $S_3(3, 4, v)$s for all even v, $v > 4$.

1. Introduction

This paper deals with the construction of simple $S_3(3, 4, v)$s (for undefined terms and notation the reader is referred to Beth et al. [1]). It was previously shown by Hanani [2] that an $S_2(3, 4, v)$ exists iff v is even but the construction establishing this result gives, in general, designs with repeated blocks. Köhler [4] has constructed simple cyclic $S_3(3, 4, v)$ for all $v \equiv 2 \pmod 4$ and Jungnickel and Vanstone [3] recently proved the existence of simple $S_3(3, 4, v)$ for all even v, $v \not\equiv 4 \pmod{12}$. The purpose of this paper is to prove the following theorem.

Theorem 1.1. *A simple $S_3(3, 4, v)$ exists iff v is even and $v \neq 4$.*

It is obvious that v even and $v \neq 4$ is necessary. We proceed to establish the sufficiency in the next sections.

2. Designs from 1-factorization

For completeness we will describe a general construction method for designs $S_3(3, 4, v)$ due to Lonz and Vanstone [5].

Let $\boldsymbol{H}$ be any 1-factorization of K_{2m}, where K_{2m} is the complete graph on a $2m$-set V. For each factor $F \in \boldsymbol{H}$ and for each pair of distinct edges $e, e' \in F$, form the set of four endpoints of e and e'. Denote the collection of all such 4-sets by $\boldsymbol{B}$. It is easily checked that $D_{\boldsymbol{H}} = (V, \boldsymbol{B})$ is an $S_3(3, 4, 2m)$. As in [3] we call $D_{\boldsymbol{H}}$ the $S_3(3, 4, 2m)$ associated with $\boldsymbol{H}$. In order to construct simple designs we make use of the following.

Theorem 2.1. *Let $\boldsymbol{H}$ be a 1-factorization of K_{2m}. $D_{\boldsymbol{H}}$ is simple iff the union of any two distinct 1-factors of $\boldsymbol{H}$ does not contain a 4-cycle.*

The proof of this result is straightforward and so is omitted. In order to establish Theorem 1.1 we need only construct for each positive integer $m \geqslant 3$ a 1-factorization $\boldsymbol{H}$ of K_{2m} having the property that the union of any two distinct 1-factors of $\boldsymbol{H}$ does not contain a 4-cycle. This we will do in the next section.

3. Main result

In this section we consider the following 1-factorizations of K_{2m} for various values of m.

$\boldsymbol{H}_1$: label the vertices of K_{2m} with the elements of $\boldsymbol{Z}_{2m-1} \cup \{\infty\}$ where ∞ is an indeterminate. Let $E_i = \{(i, \infty)\} \cup \{(i+j, i-j)\colon\ 1 \leqslant j \leqslant m-1\}$, $0 \leqslant i \leqslant 2m-2$. Then $\boldsymbol{H}_1 = \{E_i\colon 0 \leqslant i \leqslant 2m-2\}$ is a 1-factorization of K_{2m} for any positive integer m.

$\boldsymbol{H}_2$: Label the vertices of K_{2m} for m odd with the elements of $\boldsymbol{Z}_m \times I_2$. For convenience we denote (i, k) by i_k. Let

$$\begin{aligned} F_i = {} & \{(i_1, i_2)\} \cup \{((i+j)_1, (i-j)_1)\colon 1 \leqslant j \leqslant (m-1)/2\} \\ & \cup \{((i+j)_2, (i-j)_2)\colon 1 \leqslant j \leqslant (m-1)/2\}, \quad 0 \leqslant i \leqslant m-1 \end{aligned}$$

and

$$F_i = \{(j_1, (i+j)_2)\colon 0 \leqslant j \leqslant m-1\}, \quad m+1 \leqslant i \leqslant 2m-1.$$

$\boldsymbol{H}_2 = \{F_i\colon 0 \leqslant i \leqslant 2m-2\}$ is a 1-factorization of K_{2m} when m is odd.

$\boldsymbol{H}_3$: Suppose $2m = 3t+1$ and we label the vertices of K_{2m} with the elements of $(\boldsymbol{Z}_t \times I_3) \cup \{\infty\}$ where ∞ is an indeterminate. We define the following 1-factors of K_{2m}.

$$\begin{aligned} F_i = {} & \{(\infty, i_1)\} \cup \{((i+j)_1, (i-j)_1)\colon 1 \leqslant j \leqslant (t-1)/2\} \\ & \cup \{(j_2, (j-i)_3)\colon 0 \leqslant j \leqslant t-1\}, \quad 0 \leqslant i \leqslant t-1 \\ G_i = {} & \{(\infty, i_2)\} \cup \{((i+j)_2, (i-j)_2)\colon 1 \leqslant j \leqslant (t-1)/2\} \\ & \cup \{(j_3, (i-j-1)_1)\colon 0 \leqslant j \leqslant t-1\}, \quad 0 \leqslant i \leqslant t-1 \end{aligned}$$

and

$$\begin{aligned} H_i = {} & \{(\infty, i_3)\} \cup \{((i+j)_3, (i-j)_3)\colon 1 \leqslant j \leqslant (t-1)/2\} \\ & \cup \{(j_1, (i+j-1)_2)\colon 0 \leqslant j \leqslant t-1\}, \quad 0 \leqslant i \leqslant t-1. \end{aligned}$$

It is easily checked that $\boldsymbol{H}_3 = \{F_i, G_i, H_i\colon 0 \leqslant i \leqslant t-1\}$ is a 1-factorization of K_{2m}.

It was shown in [3] that $D_{\boldsymbol{H}_1}$ is simple provided $m \not\equiv 2 \pmod 3$. We require the following results.

Theorem 3.1. *D_{H_2} is simple for all positive integers $m \equiv 5 \pmod 6$.*

Proof. We first consider the 1-factors F_i and F_j where $i \neq j$, $0 \leq i, j \leq (m-1)/2$. If a 4-cycle is created in the union of these then it must involve pairs in F_i of the form $((j+i)_k, (-j+i)_k)$ and $((h-i)_k, (-h+i)_k)$ where k is either 1 or 2. But in F_j we have the pairs

$$((j+i)_k, (h+i)_k) \quad \text{and} \quad ((-j+i)_k, (-h+i)_k)$$

or

$$((j+i)_k, (-h+i)_k) \quad \text{and} \quad ((-j+i)_k, (h+i)_k).$$

Since the sum of elements in a pair is constant we have in the first case

$$j+h+2i = -j-h+2i \quad \text{or} \quad 2(j+h) = 0$$

implying $j = -h$ which is impossible. In the second case we have

$$j-h+2i = -j+h+2i \quad \text{or} \quad 2(j-h) = 0$$

implying $j = h$ which is impossible. Hence, no 4-cycle is possible in this case.

Suppose we now consider F_i, F_j where $i \neq j$ and $m \leq i, j \leq 2m-2$. If $(h_1, (j+i)_2)$ and $(l_1, (l+i)_2)$ are pairs in F_i forming a 4-cycle with F_j then

$$l-h+i = h-l+i \quad \text{or} \quad 2(l-h) = 0$$

which implies $l = h$.

Finally, we consider F_i, F_j where $i \neq j$, and $0 \leq i \leq (m-1)/2$, $m \leq j \leq 2m-2$. Suppose the pairs $((i+k)_1, (i-k)_1)$ and $(i+h)_2, (i-h)_2)$ form a 4-cycle with edges from F_j. Since differences in pairs of F_j are constant we must have

$$(i+h)-(i+k) = (i-h)-(i-k)$$

or

$$(i+h)-(i-k) = (i-h)-(i+k).$$

In the first case $2(h-k) = 0$ implies $h = k$ and in the second $h = -k$ which is also impossible since both h and k are distinct, nonnegative and at most $(m-1)/2$. This completes the proof of the theorem. □

Theorem 3.2. *D_{H_1} is simple for all positive integers $m \equiv 2 \pmod 6$.*

Proof. Since $m \equiv 2 \pmod 6$ $v = 12l + 4$ for some integer l. Construct $\boldsymbol{H}_3$ with $t = 4l + 1$.

It is easily seen that if two pairs from a 1-factor of F_i form a 4-cycle with some other 1-factor then the subscripts occurring in these pairs must occur an equal number of times. We also note that the pairs in F_i with subscript 1 form a 1-factor of K_{t+1} and since $2l + 1 \neq 2 \pmod 6$ no two pairs of this type can form a 4-cycle.

The only remaining possibility is a pair of the form (∞, i_1), $(k_2, (k-i)_3)$. If these form a 4-cycle with a pair (∞, j_2), $(h_3, (j-h-1)_1)$ then $k=j$ and $j=k+1$ which is impossible. Hence no F_i can give a 4-cycle. It remains to show that no G_i or H_i can give a 4-cycle. Most of the arguments for F_i carry over to G_i and H_i. Suppose the pair (∞, i_2), $(k_3, (i-k-1)_1)$ in G_i forms a 4-cycle with the pair (∞, j_3), $(h_1, (j+h-1)_2)$ in H_j. Then $j=k$, $i-k-1=h$ and $i=j+h-1$ or $j=k$ and $j=k+2$ which is impossible. This completes the proof. □

Proof of Theorem 1.1. As mentioned earlier the necessity that v is even and $v \neq 4$ is easily established.

If $v=2m$ and $m \not\equiv 2 \pmod 3$ the result was established in [3]. Now if $m \equiv 2 \pmod 3$ we consider two cases. First if $m \equiv 5 \pmod 6$ then the result follows directly from Theorem 3.1. If $m \equiv 2 \pmod 6$ then $2m = 12l+4$ for some integer l. The result follows from Theorem 3.2 and the proof is complete. □

4. Conclusion

In this paper we have established the existence of simple $S_3(3, 4, v)$s using an elementary direct construction. It also follows from this paper and [3] that simple resolvable $S_3(3, 4, v)$s exist for all $v \equiv 0 \pmod 4$, $v > 4$.

References

[1] T. Beth, D. Jungnickel and H. Lenz, Design Theory (Bibliographische Institut, Mannheim, Wien, Zurich, 1985).

[2] H. Hanani, On some tactical configurations, Canad. J. Math. 15 (1963) 705–722.

[3] D. Jungnickel and S.A. Vanstone, On resolvable designs $S_3(3, 4, v)$, JCT Series A, 43 (1986) 334–337.

[4] E. Köhler, k-difference cycles and the construction of cyclic t-designs, in Geometries and groups, Lecture Notes in Mathematics 893 (Springer-Verlag, 1981) 195–203.

[5] S.A. Lonz and S.A. Vanstone, private communication.

Discrete Mathematics 77 (1989) 259–279
North-Holland

ON COMBINATORIAL DESIGNS WITH SUBDESIGNS

Rolf REES
Dept. of Math. and Comp. Sci. Mount Allison University, Sackville, New Brunswick, E0A 3CO Canada

D.R. STINSON
Dept. of Computer Science, University of Manitoba, Manitoba, Canada

We develop some powerful techniques by which (certain classes of) combinatorial designs with pre-specified subdesigns can be constructed. We use our method to give nearly complete solutions (i.e. to within a finite number of cases) to several problems, including the existence of Kirkman Triple Systems with Subsystems, the existence of $(v, 4, 1)$-BIBDs with subdesigns and the existence of (certain) complementary decompositions with sub-decompositions.

1. Introduction

In this paper we are concerned with methods for constructing combinatorial designs having (or missing) subdesigns of some prespecified size. In applying our methods we will be considering several open problems regarding the existence of pairwise balanced designs with subdesigns. Such problems are not new to the literature. For example, a Steiner Triple System (STS) is a pair (X, B) where X is a (finite) set of points and B is a collection of 3-subsets (triples) of X such that any pair of distinct points is contained in exactly one triple. A *subsystem* (X', B') of a Steiner Triple System (X, B) is an STS with $X' \subseteq X$ and $B' \subseteq B$. The general problem of constructing Steiner Triple Systems containing subsystems of arbitrary size was considered and solved by Doyen and Wilson [7] (see also [31]): given any integers v and w with $v, w \equiv 1$ or 3 modulo 6 and $v \geq 2w + 1$ there exists an STS(v) containing a sub-STS(w).

A pairwise balanced design is called *resolvable* if its block set admits a partition into *parallel classes*, i.e. each parallel class forms a partition of the point set. Thus a resolvable pairwise balanced design can be thought of as a triple (X, B, P) where X is the set of points, B the set of blocks and where P is a partition of B into parallel classes. Then a *subdesign* of (X, B, P) is a triple (X', B', P') where $X' \subseteq X$, $B' \subseteq B$, and P' is a partition of B' into parallel classes on X' such that for each $p' \in P'$ there is a $p \in P$ with $p' \subseteq p$. This latter condition says that each parallel class on X' must be 'inherited' from a parallel class on X. The simplest example of this is a one-factorization of K_{2n} containing a sub-one-factorization of some $K_{2s} \subseteq K_{2n}$. From the foregoing definition it is clear that one must have $n \geq 2s$, and indeed it is well known that the condition $n \geq 2s$ is sufficient to guarantee the existence of such a design (for a short proof of this fact the reader is referred to [26, Lemma 2.2]; for a very good general survey on one-factorizations see [14]).

In this paper we will develop a simple but powerful technique by which, in essentially two steps, one may construct certain classes of combinatorial designs having subdesigns of any desired size. We will of course be restricting ourselves to a few specific problems, but the techniques here employed can be generalized in an obvious manner. In the first step, which is really the main step in the constructions, we will develop a class of group-divisible designs with block size 4 having group sizes from the set $\{3, 6, 9\}$ together with a 'special' group of size r where (subject to obvious necessary conditions) r can be chosen as large or as small as one likes (see Section 3). Then in the second step one applies weights to the points in the group-divisible design (the weights chosen according to the specific problem under consideration) and then uses standard "filling in" constructions to obtain the desired combinatorial design. In this construction the group of size r 'becomes' the sub-design. (The group-divisible design is really just acting as a weak form of a Mandatory Representation design (see [13]).)

We will apply our group-divisible designs to solve several important open problems.

The first problem that we will consider involves the study of Kirkman Triple Systems with Subsystems (see Section 4). A *Kirkman Triple System* KTS(v) is a resolvable STS(v); it is well known that such a system exists if and only if $v \equiv 3$ modulo 6 (see [24] or [9]). Recalling the definition of a subsystem in a resolvable design it is easy to see that if a KTS(v) contains a (proper) sub-KTS(w), we must have $v \geqslant 3w$. The following two results encompass what is known on this problem to date.

Theorem 1.1 [Stinson, [34]]. *If* $v \equiv w \equiv 3$ modulo 6 *and* $v \geqslant 4w - 9$ *then there exists a* KTS(v) *containing a sub*-KTS(w), *except possibly when* $(v, w) = (81, 15)$ *or* $(87, 21)$.

Theorem 1.2 [Rees and Stinson, [28]]. *Let* $w \equiv 3$ modulo 6. *Then there exist* KTS($3w$), KTS($3w + 6$) *and* KTS($3w + 12$) *containing a sub*-KTS(w), *except possibly for* KTS($3w + 12$) *when* $w = 45, 51, 63$ *or* 87.

We will herein prove the following result.

Theorem (4.4). *Let* $v \equiv w \equiv 3$ modulo 6 *and* $v \geqslant 3w$. *Then there exists a* KTS(v) *containing a sub*-KTS(w) *whenever* $v - w \geqslant 822$, *with eighty-six unsettled values of* $v - w$ *below this order.*

A second problem that we will consider (in Section 5) is one that has attracted a considerable amount of interest in recent years, namely that of determining for which v, $w \equiv 1$ or 4 modulo 12 with $v \geq 3w + 1$ does there exist a $(v, 4, 1)$-BIBD containing a sub-$(w, 4, 1)$-BIBD (i.e. the 'block size four' analogue to the Doyen–Wilson Theorem). We can (roughly) summarize the results known to date on this problem as follows.

Theorem 1.3 [Brouwer and Lenz, [4]]. *If* $w \equiv 1$ modulo 12 *then there exists a* $(v, 4, 1)$-BIBD *containing a sub*-$(w, 4, 1)$-BIBD *whenever* $v \equiv 1$ *or* 4 modulo 12 *and* $v \geq 13w + 36h - 12$, *where h is the least residue of* $(w - 1)/12$ modulo 4. *If* $w \equiv 4$ modulo 12 *then such a design exists whenever* $v \equiv 1$ *or* 4 modulo 12 *and* $v \geq 13w + 36h - 39$, *where h is the least residue of* $(w - 4)/12$ modulo 4.

Theorem 1.4 [Wei and Zhu, [35]]. (i) *If* $w \equiv 1$ *or* 4 modulo 12 *and* $w \geq 85$ *then there exists a* $(v, 4, 1)$-BIBD *containing a sub*-$(w, 4, 1)$ *whenever* $v \equiv 1$ *or* 4 modulo 12 *and* $v \geq 4w - 12$. (ii) *If* $w \equiv 4$ modulo 12 *or* $w \equiv 1$ *or* 13 modulo 48, *and if further* $w > 85$, *then such a design exists whenever* $v \equiv 1$ *or* 4 modulo 12 *and* $v \geq 3w + 1$.

We will prove the following results.

Theorem (Lemma 5.1). *Let* $v \equiv w \equiv 1$ *or* 4 modulo 12, $v \geq 3w + 4$ *and* $v - w \geq 1644$. *Then there exists a* $(v, 4, 1)$-BIBD *containing a sub*-$(w, 4, 1)$-BIBD.

Theorem (Lemmas 5.3 and 5.4). *Let* v, $w \equiv 1$ *or* 4 modulo 12 *where* $v - w$ *is an odd integer* ≥ 1611. *If* $w \geq 373$ *then there exists a* $(v, 4, 1)$-BIBD *containing a sub*-$(w, 4, 1)$-BIBD *whenever* $v \geq 3w + 1$. *If* $w < 373$ *then there exists a* $(v, 4, 1)$-BIBD *containing a sub*-$(w, 4, 1)$-BIBD *whenever* $3w + 1 \leq v \leq 15w + 28$.

Together with Theorem 1.3 our results will reduce the further study of this problem to a finite number of cases (see Theorem 5.5).

Finally, in Section 6 we will turn our attention to constructing sub-designs in (certain) 'complementary decompositions'. Let $n > 0$ and let $\mathcal{G} = \{G_1, \ldots, G_\lambda\}$ be a decomposition of K_n. Then a *complementary decomposition* $\lambda K_v \to \mathcal{G}$ is a decomposition $\mathcal{D}$ of the complete multigraph λK_v into K_n's (i.e. a (v, n, λ)-BIBD) with the property that for each $j = 1, \ldots, \lambda$ the set $\{G_j \subseteq K_n : K_n \in \mathcal{D}\}$ is a decomposition of K_v (we will refer to $\mathcal{D}$ as the *root*); note that this necessarily means that each $G_j \in \mathcal{G}$ contains the same number (namely $(n(n-1))/2\lambda$) of edges. Note that the case $\lambda = 1$ corresponds to constructing $(v, n, 1)$-BIBDs.

Where $\lambda > 1$ the best-known examples of these designs are the so-called Nested Steiner Triple Systems. A Steiner Triple System STS(v) is said to be *nested* if one can add a point to each triple in the system and so obtain a $(v, 4, 2)$-BIBD. The spectrum of these designs was determined by Stinson [32]:

Theorem 1.5. *There exists a nested* STS(v) *if and only if* $v \equiv 1$ modulo 6.

It is easy to see that a nested STS(v) is equivalent to a complementary decomposition $2K_v \to \{K_{1,3}, K_{1,3}^c\}$. There is one other possible complementary decomposition $2K_v \to \{G, G^c\}$ where G has four vertices, namely where $G = G^c = P_3$ (the path with three edges); the spectrum of these designs was given by Granville, Moisiadis and Rees [8].

Theorem 1.6. *There exists a complementary decomposition* $2K_v \to \{P_3, P_3\}$ *if and only if* $v \equiv 1$ modulo 3.

A second interesting problem was considered in [8]. Let us call two decompositions $\mathcal{G}_1 = \{G_1^1, \ldots, G_\lambda^1\}$ and $\mathcal{G}_2 = \{G_1^2, \ldots, G_\lambda^2\}$ of K_n *distinct* if for no permutation σ on $\{1, \ldots, \lambda\}$ is it true that $G_i^1 \simeq G_{\sigma(i)}^2$ for all $i = 1, \ldots, \lambda$. Then a (v, n, λ)-BIBD (viewed as a decomposition $\mathcal{D}$ of $\lambda K_v \to K_n$) is called *pandecomposable* if for any set $\mathcal{G}_1, \ldots, \mathcal{G}_k$ of distinct decompositions of K_n (each with λ graphs) there exists, for each $i = 1, \ldots, k$, a complementary decomposition $\lambda K_v \to \mathcal{G}_i$ with $\mathcal{D}$ as its root. For example the following design is a pandecomposable $(7, 4, 2)$-BIBD (to each block a, b, c, d associate the graphs $K_{1,3}$ and $K_{1,3}^c$ where the $K_{1,3}$ has a on one side and b, c, d on the other, and also the graphs P_3 and P_3^c where P_3 is the path abcd).

0, 4, 2, 1	4, 1, 6, 5
1, 5, 3, 2	5, 2, 0, 6
2, 6, 4, 3	6, 3, 1, 0
3, 0, 5, 4	

The following result was obtained in [8].

Theorem 1.7 [Granville, Moisiadis and Rees]. *There exists a pandecomposable* $(v, 4, 2)$-BIBD *if and only if* $v \equiv 1$ modulo 6.

A subsystem in a complementary decomposition $\lambda K_v \to \mathcal{G}$ is just a complementary decomposition $\lambda K_w \to \mathcal{G}$ for some complete multisubgraph $\lambda K_w \subseteq \lambda K_v$. In particular, the root of the subsystem (a (w, n, λ)-BIBD) is a sub-BIBD of the root of the 'mother' system (a (v, n, λ)-BIBD). We will be interested in determining the spectrum of subsystems in complementary decompositions of the type given by Theorems 1.6 and 1.7. Note that, since in each case the roots are BIBDs with $k = 4$, a necessary condition for a system of order v to have a subsystem of order w is that $v \geq 3w + 1$. We will prove the following two results:

Theorem (6.2). *Let v and w be given with* $v \equiv w \equiv 1$ modulo 6, $v \geq 3w + 4$ *and* $v - w \geq 822$. *Then there exists a pandecomposable* $(v, 4, 2)$-BIBD *containing a sub-pandecomposable* $(w, 4, 2)$-BIBD.

Theorem (6.4). *Let v and w be given with $v \equiv w \equiv 1$ modulo 3, $v \geq 3w + 1$ and $v - w \geq 411$. Then there exists a complementary decomposition $2K_v \to \{P_3, P_3\}$ containing a subsystem $2K_w \to \{P_3, P_3\}$.*

Remark. Note that as a corollary to the first result we have a solution (to within a finite number of cases) for the spectrum of subsystems in nested Steiner Triple Systems; as a corollary to the second result we have a similar solution for the spectrum of subsystems in $(v, 4, 2)$-BIBDs. (See Corollaries 6.3 and 6.5 in Section 6.)

2. Definitions and preliminary results

Of central importance to our work here will be the notions of a group-divisible design (GDD) and an incomplete group-divisible design (IGDD). A *group-divisible design* is a triple (X, G, B) where X is a set of points, G is a partition of X into *groups* and B is a collection of subsets of X (*blocks*) such that

(i) $|B_i \cap G_j| \leq 1$ for all $B_i \in B$ and $G_j \in G$, and

(ii) any pair of points from distinct groups occurs in exactly one block.

An *incomplete group-divisible design* is a quadruple (X, Y, G, B) where X is a set of points, Y is a (possibly empty) subset of X, G is a partition of X into groups and B is a collection of blocks such that

(i) $|B_i \cap G_j| \leq 1$ for all $B_i \in B$ and $G_j \in G$, and

(ii) any pair of points x and y from distinct groups occurs in exactly one block unless both x and y are in Y, in which case x and y do not occur together in any block. Note that when $Y = \emptyset$ an IGDD is just a GDD.

We will usually describe GDDs and IGDDs by means of an exponential notation: a K-GDD of type $g_1^{t_1}g_2^{t_2}\cdots g_r^{t_r}$ is a GDD in which there are t_i groups of size g_i, $i = 1, \ldots, r$, and in which each block has size from the set K; a K-IGDD of type $(g_1, h_1)^{t_1}(g_2, h_2)^{t_2}\cdots(g_r, h_r)^{t_r}$ is an IGDD (X, Y, G, B) in which there are t_i groups of size g_i, each with the property that its intersection with Y has cardinality h_i, $i = 1, \ldots, r$, and in which each block has size from the set K. When some $h_i = 0$ we will suppress it; thus a 4-IGDD of type $(9,3)^4 6^1$ means a 4-IGDD of type $(9,3)^4(6,0)^1$. We will also use other (standard) notations from time to time, as it appears convenient. For example we can replace the foregoing notation with K-GDD of type S, where S is the multiset consisting of t_i copies of g_i, or K-IGDD of type S, where S is the multiset consisting of t_i copies of the (ordered) pair (g_i, h_i), $i = 1, \ldots, r$. Finally, we will use the notation $\mathrm{GD}[K, M; v]$ to mean a group-divisible design on v points in which each block has size from the set K and each group has size from the set M. A $\mathrm{PBD}(K; v)$ will denote a pairwise balanced design (of index unity) on v points in which each block has size from the set K. Where there is exactly one block (resp. group) of some size $k \in K$ (resp. $m \in M$) we will indicate this by writing k^* (resp. m^*).

We shall need some preliminary results before proceeding to Section 3. A group-divisible design is called *resolvable* if its block set can be partitioned into parallel classes. In [27] the authors considered the problem of constructing resolvable 3-GDDs and obtained a result which implies the following.

Theorem 2.1 [Rees and Stinson]. *Let g and u be given where $gu \equiv 0$ modulo 3 and $g(u-1) \equiv 0$ modulo 2, $(g, u) \neq (2, 3)$, $(2, 6)$ or $(6, 3)$. Then there exists a resolvable 3-GDD of type g^u, except possibly when*
(i) $g \equiv 6$ modulo 12 *and* $u = 11$ *or* 14;
(ii) $g \equiv 2$ *or* 10 modulo 12 *and* $u = 6$.

Assaf and Hartman [1] have constructed resolvable 3-GDDs of types 6^{11} and 6^{14}, which easily gives

Theorem 2.2 [Assaf and Hartman]. *There exist resolvable 3-GDDs of type g^{11} and g^{14}, where $g \equiv 6$ modulo 12.*

A *frame* is a group-divisible design (X, G, B) whose block set can be partitioned into *holey parallel classes*, i.e. each holey parallel class is a partition of $X - G_j$ for some group $G_j \in G$. The groups in a frame are usually referred to as *holes*. A *Kirkman frame* is a frame in which each block has size 3; the spectrum of Kirkman Frames with uniform hole size was determined in [34].

Theorem 2.3 [Stinson]. *There exists a Kirkman Frame of type g^u if and only if g is even, $u \geq 4$ and $g(u-1) \equiv 0$ modulo 3.*

Remark. It is noted in [34] that in a Kirkman frame (X, G, B) there are $\frac{1}{2}|G_j|$ holey parallel classes of triples that partition $X - G_j$, for each $G_j \in G$. It follows immediately that a Kirkman frame of type g^u is equivalent to a 4-IGDD of type $(\frac{3}{2}g, \frac{1}{2}g)^u$ (for a fuller discussion of this equivalence the reader is referred to [33]).

We will be relying heavily on results that are known concerning resolvable BIBDs with block size 5. Our principal source of these designs is the work of W. H. Mills (see references) who has shown that for all $r > 36$ with $r \equiv 1$ or 6 modulo 15 there exists an $(r, 6, 1)$-BIBD, with 165 possible exceptions. More recently, Mullin, Hoffman and Lindner [22] and Mullin [21] have reduced the size of the list of doubtful values to 96. We are of course using the fact that for each k the set of replication numbers for resolvable $(v, k, 1)$-BIBDs is PBD-closed (see e.g. [25]) and that there is a resolvable $(25, 5, 1)$-BIBD, so that whenever an $(r, 6, 1)$-BIBD exists then so does a resolvable $(4r + 1, 5, 1)$-BIBD. That is, by using Table 1 in [21] together with Lemma 1.3 in [22], it follows that the set of replication numbers for resolvable BIBDs with block size 5 contains the set of integers congruent to 1 or 6 modulo 15, with the following possible exceptions:

Table 1.

36	46	61	141	166	171	196	201	226	231
246	256	261	276	286	291	316	321	336	346
351	376	406	411	436	441	466	471	486	496
501	526	561	591	616	621	646	651	676	706
711	736	741	766	771	796	801	831	886	891
916	946	1011	1066	1071	1096	1101	1131	1141	1156
1161	1176	1186	1191	1221	1246	1251	1276	1396	1401
1456	1461	1486	1491	1516	1521	1546	1611	1641	1671
1816	1821	1851	1881	1971	2031	2241	2601	3201	3471
3501	4191	4221	5391	5901					

Remark. It will be of use to us later on to notice that there are never more than three 'consecutive' (i.e. consecutive in the set $\{n \in \mathbb{Z}^+ : n \equiv 1 \text{ or } 6 \text{ modulo } 15\}$) integers among the entries in Table 1.

Finally, we will use the usual notation TD(k, n) to mean a transversal design with k groups of size n, that is, a k-GDD of type n^k. Unless indicated otherwise, our source for these designs will be [2].

3. A new class of group-divisible designs with block size 4

In this section we will construct our group-divisible designs, using as our primary tool the following construction.

Construction 3.1. Let (X, Y, G, B) be an incomplete group-divisible design and let $w : X \to \mathbb{Z}^+ \cup \{0\}$ and $d : X \to \mathbb{Z}^+ \cup \{0\}$ be nonnegative integer functions on X, where $d(x) \leq w(x)$ for all $x \in X$. Let a be a fixed nonnegative integer. Suppose that

(i) for each block $b \in B$ there is a K-IGDD of type $\{(w(x), d(x)) : x \in b\}$,

(ii) there is a K-IGDD of type

$$\left\{\left(\sum_{x \in G_j \cap Y} w(x), \sum_{x \in G_j \cap Y} d(x)\right) : G_j \in G\right\},$$

and

(iii) for each $G_j \in G$ there is a K-GDD on $a + \sum_{x \in G_j} w(x)$ points having a group of size a and a group of size $\sum_{x \in G_j} d(x)$.

Then there is a K-GDD on $a + \sum_{x \in X} w(x)$ points having a group of size a and a group of size $\sum_{x \in X} d(x)$.

Remark. By setting $Y = \emptyset$ and $a = 0$ in the above construction we obtain an equivalent version of construction 4.4 in [23].

Lemma 3.2. *Let a, j and h be integers where $a=3$ or 6, $j>1$ and $h \geqslant 0$, and suppose that there exists a* $\{5, 6\}$-IGDD (X, Y, G, B) $(G=\{G_1, \ldots, G_j\})$ *having the following properties*:

(i) $|G_1| \geqslant 3$ *and for each* $i=2, \ldots, j$ $|G_i| \in \{3, 4, 5\}$;

(ii) $G_1 \cap Y = \emptyset$ *and for each* $i=2, \ldots, j$ $|G_i \cap Y| \in \{0, h\}$; *also, if for some* i, $G_i \cap Y \neq \emptyset$ *then the same is true for at least four values of* i.

Then for each $u \equiv 0$ modulo 3 *with* $3|Y| \leqslant u \leqslant 3|X|$ *there is a* GD$[4, \{3, 6, 9, u^*\}; 6|X| + u + a]$.

Proof. We use Construction 3.1. Let $d: X \rightarrow \{0, 3\}$ be an assignment of the points such that $d(y)=3$ for all $y \in Y$, $d(x)=d(x')$ for all $x, x' \in G_1$ and $\sum_{x \in X} d(x) = u$. Such an assignment exists since $|X - Y - G_1| \geqslant |G_1|$ (this follows easily from the hypothesis). Let $w(x) = 6 + d(x)$ for all $x \in X$. Replace each block b in the incomplete group-divisible design by the relevant 4-IGDD, i.e. of type $\{(w(x), d(x)): x \in b\}$ (the type will be $(9,3)^i 6^{|b|-i}$ for some i, see appendix), and if $h \neq 0$ replace the 'missing' subdesign (i.e. on the points of Y) by a 4-IGDD of type $(9h, 3h)^{|Y|/h}$ (see Theorem 2.3 and the remark following it). The groups in the incomplete group-divisible design are to be replaced by the relevant 4-GDDs, according to Table 2. This completes the proof. □

Corollary 3.3. *Suppose that there is a* GD$[\{5,6\}, \{3,4,5,r^*\}; s]$ *with more than one group, where* $r \geqslant 3$. *Then for each* $u \equiv 0$ modulo 3 *with* $0 \leqslant u \leqslant 3s$ *and each* $a \in \{3, 6\}$ *there is a* GD$[4, \{3, 6, 9, u^*\}; 6s + u + a]$.

Proof. Use Lemma 3.2 with $h=0$ (so that $Y=\emptyset$ and condition (ii) is vacuous). □

We are ready now to prove the main result of this section.

Theorem 3.4. *Let* $\mathcal{S} = \{20, 24, 25, 28, 29, 30, 31, 36, 40, 44, 45, 52, 59, 60, 63, 64, 65\} \cup \{n \in \mathbb{Z}: n \geqslant 68\}$ *and let* $a \in \{3, 6\}$. *Then for each* $s \in \mathcal{S}$ *and each* $u \equiv 0$ modulo 3 *with* $0 \leqslant u \leqslant 3s$ *there exists a* GD$[4, \{3, 6, 9, u^*\}; 6s + u + a]$.

Proof. We use Corollary 3.3, exhibiting for each $s \in \mathcal{S}$ a $\{5, 6\}$-GDD satisfying the hypothesis of that corollary.

$s = 20$ remove a point from a $(21, 5, 1)$-BIBD.

$s = 24, 25$ remove either one point or no points from a $(25, 5, 1)$-BIBD.

$s = 28, 29, 30$ remove either three, two or one collinear point(s) from a $(31, 6, 1)$-BIBD.

$s = 31$ there is a resolvable 4-GDD of type 3^8 (see e.g. [11, Section 3]); Add a group 'at infinity' of size 7 to this design.

$s = 36$ add a group 'at infinity' of size 8 to a resolvable $(28, 4, 1)$-BIBD.

$s = 40$ remove a point from a $(41, 5, 1)$-BIBD.

Table 2.

a	$\lvert G_i\rvert$	$\sum_{x\in G_i} d(x)$	4-GDD of type	Source
3	3	0	$3^5 6^1$	add six infinite points to a KTS(15)
3	3	3	3^8	remove a point from a (25, 4, 1)-BIBD
3	3	6	$3^1 6^4$	[28, appendix]
3	3	9	$3^7 9^1$	add nine infinite points to a KTS(21)
3	4	0	3^9	remove a point from a (28, 4, 1)-BIBD
3	4	3	$3^8 6^1$	remove a point from a PBD({4, 7*}; 31)([3])
3	4	6	$3^9 6^1$	remove a point from a PBD({4, 7*}; 34)([3])
3	4	9	$3^6 9^2$	[28, appendix]
3	4	12	$3^9 12^1$	add twelve infinite points to a KTS(27)
3	5	0	$3^9 6^1$	remove a point from a PBD({4, 7*}; 34)([3])
3	5	3	3^{12}	remove a point from a (37, 4, 1)-BIBD
3	5	6	$3^1 6^6$	appendix
3	5	9	$3^{11} 9^1$	appendix
3	5	12	$3^9 6^1 12^1$	[28, appendix]
3	5	15	$3^{11} 15^1$	add fifteen infinite points to a KTS(33)
3	$\geqslant 6$ and even	0	$3^{2\lvert G_i\rvert+1}$	remove a point from a $(6\lvert G_i\rvert+4, 4, 1)$-BIBD
3	$\geqslant 7$ and odd	0	$3^{2\lvert G_i\rvert-1}6^1$	remove a point from a PBD({4, 7*}; $6\lvert G_i\rvert+4$)([3])
3	$\geqslant 6$	$3\lvert G_i\rvert$	$3^{2\lvert G_i\rvert+1}(3\lvert G_i\rvert)^1$	add $3\lvert G_i\rvert$ infinite points to a KTS($6\lvert G_i\rvert+3$)
6	3	0	$3^4 6^2$	appendix
6	3	3	$3^1 6^4$	[28, appendix]
6	3	6	6^5	[6]
6	3	9	$6^4 9^1$	add nine infinite points to a resolvable 3-GDD of type 6^4 (Theorem 2.1)
6	4	0	6^5	[6]
6	4	3	$3^9 6^1$	remove a point from a PBD({4, 7*}; 34)([3])
6	4	6	6^6	[6]
6	4	9	$6^5 9^1$	[27, appendix]
6	4	12	$6^5 12^1$	add twelve infinite points to a resolvable 3-GDD of type 6^5 (Theorem 2.1)
6	5	0	6^6	[6]
6	5	3	$3^1 6^6$	appendix
6	5	6	6^7	[6]
6	5	9	$6^6 9^1$	appendix
6	5	12	$6^6 12^1$	appendix
6	5	15	$6^6 15^1$	add fifteen infinite points to a resolvable 3-GDD of type 6^6 (Theorem 2.1)
6	$\geqslant 6$	0	$6^{\lvert G_i\rvert+1}$	[6]
6	$\geqslant 6$	$3\lvert G_i\rvert$	$6^{\lvert G_i\rvert+1}(3\lvert G_i\rvert)^1$	add $3\lvert G_i\rvert$ infinite points to a resolvable 3-GDD of type $6^{\lvert G_i\rvert+1}$ (Theorems 2.1 and 2.2)

$s = 44, 45$ there is a $(45, 5, 1)$-BIBD with a parallel class of blocks (see e.g. [12]); remove either one point or no points from this design.
$s = 52$ add a group 'at infinity' of size 12 to a resolvable $(40, 4, 1)$-BIBD.
$s = 59$ remove a block and a point from a $(66, 6, 1)$-BIBD (the resulting GDD has type $4^6 5^7$).
$s = 60, 63, 64, 65$ remove either six, three, two or one collinear point(s) from a $(66, 6, 1)$-BIBD.
$68 \leq s \leq 80$ add a group 'at infinity' of size s-65 to a resolvable $(65, 5, 1)$-BIBD.
$80 \leq s \leq 94$ Start with a resolvable TD$(5, 15)$ and construct on each group the design obtained by removing a point from the affine plane of order 4. We can do this in such a way that the resulting design is a resolvable $\{4, 5\}$-GDD of type 3^{25}, having five parallel classes of quadruples and quintuples and fourteen classes of quintuples. Now add a group 'at infinity' of size s-75 to this design (the first five infinite points must complete the 'mixed' parallel classes).
$88 \leq s \leq 105$ add a group 'at infinity' of size s-85 to a resolvable $(85, 5, 1)$-BIBD.
$98 \leq s \leq 114$ Start with a resolvable TD$(5, 19)$ and on each group construct a copy of the design obtained by adding three points 'at infinity' to the affine plane of order 4. This can give us a $\{4, 5\}$-GDD of type $3^5 4^{20}$ in which there is a parallel class containing 20 quadruples and 3 quintuples and in which there are a further eighteen parallel classes of quintuples. Add a group 'at infinity' of size s-95 (the first infinite point completing the parallel class containing the quadruples).
$108 \leq s \leq 125$ Start with a resolvable TD$(5, 21)$ and on each group construct a $(21, 5, 1)$-BIBD. Now add a group 'at infinity' of size s-105 to this design (the group-type will be $5^{21}(s\text{-}105)^1$).
$123 \leq s \leq 149$ Start with a resolvable TD$(5, 24)$ (4 MOLS of order 24 have been constructed by Roth and Peters [30]) and on each group construct a copy of the design obtained by removing a point from the affine plane of order 5. This can be done so that the resulting design is a resolvable 5-GDD of type 4^{30}; now add a group 'at infinity' of size s-120 to this design.
$148 \leq s \leq 174$ Take a resolvable TD$(5, 29)$ and construct on each group a copy of the design obtained by adding four 'infinite' points to the affine plane of order 5. Adding a group 'at infinity' of size s-145 yields a GDD with group-type $4^5 5^{25} (s\text{-}145)^1$.
$158 \leq s \leq 185$ Take a resolvable TD$(5, 31)$ and construct a $(31, 6, 1)$-BIBD on each group; then add a group 'at infinity' of size s-155 (the group-type will be $5^{31}(s\text{-}155)^1$).
$180 \leq s \leq 214$ Start with a resolvable TD$(5, 35)$ and on each group construct a copy of the design obtained by removing a block and a point from a $(41, 5, 1)$-BIBD. This we can do so that the resulting design is a $\{4, 5\}$-GDD of type $3^{25} 4^{25}$ in which there are five parallel classes of quadruples and quintuples and thirty-four parallel classes of quintuples. Add a group 'at infinity' of size s-175 to this design (the first five infinite points completing the 'mixed' parallel classes).

$208 \leq s \leq 255$ add a group 'at infinity' of size s-205 to a resolvable $(205, 5, 1)$-BIBD.
$228 \leq s \leq 269$ take a resolvable TD$(5, 45)$, constructing a $(45, 5, 1)$-BIBD on each group, and then adding a group 'at infinity' of size s-225 (the group-type will be $5^{45}(s\text{-}225)^1$).
$s \geq 268$ From here on we use resolvable $(4r+1, 5, 1)$-BIBDs, starting with $r = 66$. The reader is now referred to Table 1. Recalling that there are never more than three 'consecutive' entries in this table we can always write $s = 4r + 1 + t$ where r is the replication number of a resolvable BIBD and $3 \leq t \leq \min\{r-1, 122\}$. Now add a group 'at infinity' of size t to a resolvable $(4r+1, 5, 1)$-BIBD.

This completes the proof of Theorem 3.4. □

Remark. Regarding the values in the set $\mathbb{Z}^+ - \mathcal{S}$ in Theorem 3.4 it is tedious but straightforward to check that if $s \leq 19$ or $s = 21$, 22, 23, 26 or 27 then no $\{5, 6\}$-GDD satisfying the desired properties can exist.

4. Kirkman triple systems with subsystems

In this section we will prove the following result.

Theorem 4.1. *Suppose that* $v \equiv w \equiv 3$ modulo 6, $v \geq 3w$ *and* $v - w = 12s + 6$ *or* $12s + 12$, *where* $s \in \mathcal{S} \cup \{0, 1, 2, 3, 4, 5, 6, 7\}$ *($\mathcal{S}$ is the set defined in Theorem 3.4). Then there exists a* KTS(v) *containing a sub*-KTS(w).

We will use the following special case of Construction 3.1 to provide Theorem 4.1:

Construction 4.2. Let (X, G, B) be a group divisible design with block sizes from the set $\{n \in \mathbb{Z}^+ : n \equiv 1 \text{ modulo } 3\}$, and let m be a positive even integer. Then there exists a KTS$(m\,|X| + 3)$ containing subsystems of size $m\,|G_j| + 3$, $G_j \in G$.

Proof. Apply Construction 3.1 with $Y = \emptyset$, $a = 3$, $w(x) = \frac{3}{2}m$ and $d(x) = \frac{1}{2}m$ for all $x \in X$. The required input designs exist by Theorem 2.3 and the remark following it. □

Before proceeding to the proof of Theorem 4.1 we obtain the following designs.

Lemma 4.3. *There exist* KTS(81) *with a sub*-KTS(15), KTS(87) *with a sub*-KTS(21), KTS(117) *with a sub*-KTS(33) *and a* KTS(135) *with a sub*-KTS(39).

Proof. The first two designs are obtained by applying Construction 4.2 (with $m=2$) to a 4-GDD of type $6^5 9^1$ (see appendix of [27]) or a 4-GGD of type $3^{11}9^1$ (appendix). The fourth design is obtained by applying Construction 4.2 (with $m=4$) to a 4-GDD of type $3^8 9^1$ (this GDD can be obtained by adding nine infinite points to a resolvable 3-GDD of type 4^6 (Theorem 2.1)). To get a KTS(117) with a sub-KTS(33) proceed as follows. We first construct the following PBD($\{4, 10^*, 16^*\}, 58$):
Points: $(\mathbb{Z}_{16} \times \{1,2,3\}) \cup (\{a\} \times \mathbb{Z}_2) \cup \{\infty_i : 1 \leq i \leq 8\}$.
Blocks: The block of size 10 is $(\{a\} \times \mathbb{Z}_2) \cup \{\infty_i : 1 \leq i \leq 8\}$ and the block of size 16 is $\mathbb{Z}_{16} \times \{3\}$. The blocks of size 4 are obtained by developing the following modulo 16 (the subscripts on a are to be evaluated modulo 2):

$a_0 2_1 5_1 0_3$	$\infty_5 10_1 5_2 0_3$	$9_1 15_1 13_2 0_3$
$a_1 9_2 12_2 0_3$	$\infty_6 11_1 0_2 0_3$	$4_2 11_2 14_1 0_3$
$\infty_1 0_1 3_2 0_3$	$\infty_7 12_1 8_2 0_3$	$0_1 1_1 0_2 2_2$
$\infty_2 3_1 10_2 0_3$	$\infty_8 13_1 6_2 0_3$	$0_1 4_1 8_1 12_1$
$\infty_3 4_1 14_2 0_3$	$1_1 6_1 8_1 0_3$	$0_2 4_2 8_2 12_2$
$\infty_4 7_1 15_2 0_3$	$1_2 2_2 7_2 0_3$	

Now remove a point to obtain a $\{4, 10\}$-GDD of type $3^{14}15^1$ and apply Construction 4.2 (with $m=2$) to this GDD. □

Proof of Theorem 4.1. If $s = 0$, 1, 2, 3, 4, 5, 6 or 7 use Theorems 1.1 and 1.2 and Lemma 4.3. Now let $s \in \mathcal{S}$. If $v - w = 12s + 6$ apply Theorem 3.4 with $a = 3$ and $u = (w-3)/2$ (note that since $v \geq 3w$ we have $0 \leq u \leq 3s$) to construct a GD[4, $\{3, 6, 9, (w-3)2^*\}$; $(v-3)/2$]. Then use Construction 4.2 (with $m=2$) to obtain a KTS(v) with a sub-KTS(w), as desired. If $v - w = 12s + 12$ proceed as above using instead $a = 6$. □

As an immediate corollary to Theorem 4.1 we have:

Theorem 4.4. *Let* $v \equiv w \equiv 3$ modulo 6, $v \geq 3w$ *and* $v - w \geq 822$. *Then there exists a* KTS(v) *containing a sub*-KTS(w).

5. Balanced incomplete block designs (block size 4 and $\lambda = 1$) with subdesigns

Here we will prove our result on embeddings of (w, 4, 1)-BIBDs.

Lemma 5.1. *Let* $v \equiv w \equiv 1$ *or* 4 modulo 12, $v \geq 3w + 4$ *and* $v - w \geq 1644$. *Then there is a* (v, 4, 1)-BIBD *containing a sub*-(w, 4, 1)-BIBD.

Proof. Let $h = \frac{1}{4}(v - w)$ and $u = \lfloor (w-1)/4 \rfloor$, and let $s = \lfloor (h-3)/6 \rfloor$. Since $v - w \geq 1644$ we have $s \geq 68$, and furthermore

(i) if $v \equiv w \equiv 4$ modulo 12 and h is odd then

$$3s = (h-3)/2 \geq (2w-8)/8 = u \geq 0,$$

(ii) if $v \equiv w \equiv 4$ modulo 12 and h is even then

$$3s = \frac{h-6}{2} \geq \frac{(2w+16)-24}{8} = \frac{2w-8}{8} = u \geq 0,$$

(iii) if $v \equiv w \equiv 1$ modulo 12 and h is odd then

$$3s = \frac{h-3}{2} \geq \frac{2w-2}{8} = u \geq 0, \quad \text{and}$$

(iv) if $v \equiv w \equiv 1$ modulo 12 and h is even then

$$3s = \frac{h-6}{2} \geq \frac{(2w+22)-24}{8} = \frac{2w-2}{8} = u \geq 0.$$

Thus we can use Theorem 3.4 (with $a = 3$ when h is odd, or $a = 6$ when h is even) to construct a GD[4, $\{3, 6, 9, u^*\}$; $h + u$]. Now use Wilson's Fundamental Construction [36] (this is really just a special case of Construction 3.1, i.e. with $a = 0$ and $w(x) = d(x)$ for all $x \in X$) on this group-divisible design, replacing each point by four new ones, to obtain a GD[4, $\{12, 24, 36, 4u^*\}$; $4(h + u)$]; add one or four 'ideal' points (depending on whether $w \equiv 1$ or 4 modulo 12) and fill in the relevant BIBDs. □

Before proceeding we will need the following simple lemma.

Lemma 5.2. *Let $s \geq 268$. Then there is an integer t with $4 \leq t \leq \min\{\frac{1}{7}s, 123\}$ for which a $\{5, 6\}$-IGDD of type $4^{(s-5t)/4}(5, 1)^t$ exists. (Note that this IGDD has s points.)*

Proof. We proceed essentially in the same way as the case $s \geq 268$ in the proof of Theorem 3.4. Again referring the reader to Table 1 we can write $s = 4r + t$ where r is the replication number of a resolvable BIBD with block size 5 ($r \geq 66$) and $4 \leq t \leq \min\{\frac{1}{7}s, 123\}$. (Certainly t need never be greater than 123 since Table 1 does not contain more than three 'consecutive' entries; on the other hand it can be checked that the largest value that t/s need take occurs when $s = 307$, when we must write $307 = 4 \cdot 66 + 43$, so that $t/s = 43/307 < \frac{1}{7}$.) Add t points 'at infinity' to a resolvable $(4r + 1, 5, 1)$-BIBD and then remove a point other than one of the ones just added. A $\{5, 6\}$-IGDD of type $4^{r-t}(5, 1)^t$ is obtained (the 'missing' subdesign occurs on the t new points). □

Lemma 5.3. *Let v, $w \equiv 1$ or 4 modulo 12 where $v \geq 3w+1$ and $v-w$ is an odd integer ≥ 1611. If $w \geq 373$ then there is a $(v, 4, 1)$-BIBD containing a sub-$(w, 4, 1)$-BIBD.*

Proof. Let $s = \frac{1}{6}(v-w-3)$; since $v-w \geq 1611$ we have $s \geq 268$. From Lemma 5.2 there is a $\{5,6\}$-IGDD (X, Y, G, B) of type $4^{(s-5t)/4}(5, 1)^t$ for some $4 \leq t \leq 123$. Now we apply Lemma 3.2 with $h=1$, $|Y|=t$ and $a=3$, and with $u = w-1$. Note that $u \geq 3t$ since $w \geq 373$; moreover, since s and t have the same parity it is easily deduced that $u-3t \equiv 0$ modulo 6. This means (see the proof of Lemma 3.2) that we can assign the function d to X in such a way that for each group $G_i \in G$ an even number of points in $G_i - Y$ are assigned a value of 3; in turn (see Table 2) the only triples $(a, |G_i|, \Sigma d(x))$ that will arise are $(3,4,0)$, $(3,4,6)$, $(3,4,12)$, $(3,5,3)$, $(3,5,9)$ or $(3,5,15)$. In this way we obtain a GD$[4, \{3, u^*\}; 6s+u+3]$, i.e. a GD$[4, \{3, (w-1)^*\}; v-1]$. Now just add a point to 'complete' the groups, and construct a $(w, 4, 1)$-BIBD on the block of size w. □

Lemma 5.4. *Let v, $w \equiv 1$ or 4 modulo 12 where $3w+1 \leq v \leq 15w+28$ and $v-w$ is an odd integer ≥ 1611. Then there exists a $(v, 4, 1)$-BIBD containing a sub-$(w, 4, 1)$-BIBD.*

Proof. Proceed as in the proof of Lemma 5.3, using instead the inequality $4 \leq t \leq \frac{1}{7}s$ (from Lemma 5.2). We will again use Lemma 3.2 with $h=1$, $|Y|=t$, $a=3$ and $u=w-1$. We must therefore only show that $u \geq 3t$.

By hypothesis, $v \leq 15w+28$. Since $v = 6s+w+3$ it follows that $s \leq \frac{7}{3}w + \frac{25}{6}$. On the other hand $s \geq 7t$, so that $w \geq 3t - \frac{25}{14}$. But $w \equiv 1$ modulo 3 so that in fact $w \geq 3t+1$, i.e. $u \geq 3t$, as desired. □

Together with Theorem 1.3, Lemmas 5.1, 5.3 and 5.4 yield the following block size 4 analogue to the Doyen–Wilson Theorem (missing a finite number of cases).

Theorem 5.5. *Let v, $w \equiv 1$ or 4 modulo 12, $v \geq 3w+1$ and $v-w \geq 1635$. Then there exists a $(v, 4, 1)$-BIBD containing a sub-$(w, 4, 1)$-BIBD.*

Proof. If $v-w$ is even, or $v-w$ is odd and $w \geq 373$ then we use Lemmas 5.1 or 5.3 respectively. If $v-w$ is odd and w is 'small', i.e. $w \leq 124$, then use Theorem 1.3 (which asserts that a $(w, 4, 1)$-BIBD can always be embedded in some $(v, 4, 1)$-BIBD whenever $v \geq 13w+96$). For values of w between 133 and 364 use Lemma 5.4 in conjunction with Theorem 1.3. □

6. Subdesigns in complementary decompositions

In this section we obtain some results on subdesigns in complementary decompositions. We will need the following design, which appears in Lemma 2.4 of [8]:

Lemma 6.1. *There is a pandecomposable covering of the complete multipartite graph $K_{2,2,2,2}$ by K_4's.*

Proof. Take the following design, whose blocks are to be interpreted as in the example preceding Theorem 1.7:

Groups: 0, 1   2, 3   4, 5   6, 7

Blocks:	0, 2, 7, 4	4, 2, 6, 1
	1, 3, 6, 5	5, 3, 7, 0
	2, 1, 5, 7	6, 0, 5, 2
	3, 0, 4, 6	7, 1, 4, 3

□

Theorem 6.2. *Let $v \equiv w \equiv 1$ modulo 6, $v \geq 3w+4$ and $v-w \geq 822$. Then there exists a pandecomposable* $(v, 4, 2)$-BIBD *containing a sub-pandecomposable* $(w, 4, 2)$-BIBD.

Proof. Use Theorem 3.4 to construct a GD[4, $\{3, 6, 9, (w-1)/2^*\}$; $(v-1)/2$] (i.e. let $s = \lfloor (v-w-6)/12 \rfloor$). Now apply Wilson's Fundamental Construction [36], replacing each point by two new ones and each block by the design in Lemma 6.1; add one 'ideal' point and fill in pandecomposable $(7, 4, 2)$-, $(13, 4, 2)$-, $(19, 4, 2)$- and $(w, 4, 2)$-BIBDs. □

As an immediate consequence of Theorem 6.2 we have

Corollary 6.3. *Let $v \equiv w \equiv 1$ modulo 6, $v \geq 3w+4$ and $v-w \geq 822$. Then there exists a nested* STS(v) *containing a sub-nested* STS(w).

Theorem 6.4. *Let $v \equiv w \equiv 1$ modulo 3, $v \geq 3w+1$ and $v-w \geq 411$. Then there exists a complementary decomposition $2K_v \rightarrow \{P_3, P_3\}$ containing a sub-complementary decomposition $2K_w \rightarrow \{P_3, P_3\}$.*

Proof. Use Theorem 3.4 (with $s = \lfloor (v-w-3)/6 \rfloor$) to construct a GD[4, $\{3, 6, 9, (w-1)^*\}$; $v-1$]. Add a point to 'complete' the groups and so obtain a PBD($\{4, 7, 10, w^*\}$; v) and then construct a complementary path decomposition on each block. □

Since the root of a complementary decomposition $2K_v \to \{P_3, P_3\}$ is a $(v, 4, 2)$-BIBD Theorem 6.4 now yields the following version of Theorem 5.5 for embeddings of $(v, 4, 2)$-BIBDs:

Corollary 6.5. *Let* $v \equiv w \equiv 1$ modulo 3, $v \geq 3w + 1$ *and* $v - w \geq 411$. *Then there exists a* $(v, 4, 2)$-BIBD *containing a sub*-$(w, 4, 2)$-BIBD.

Remark. The embeddings given by Corollary 6.5 will, in general, contain repeated blocks.

7. Conclusion

We expect that the techniques employed in Section 3 of this paper will be very useful in considering a wide variety of problems concerning subdesigns in combinatorial designs. This is because Construction 3.1 can of course be used to construct group-divisible designs, analogous to those in Lemma 3.2, for larger block sizes.

Concerning the present material, we can already use Lemma 3.2 to go a long way towards solving the spectrum for partially resolvable partitions PRP $2\text{-}(3, 4, v; m)$ (i.e. a PBD$(\{3, 4\}; v)$ whose triples can be arranged into m parallel classes, see [10]); a few difficulties remain, however, and we hope to report on this in a future paper.

We will also report on some recent progress made concerning the unsettled cases in Sections 4 and 5. For example, at the time of writing, there are just fifty pairs (v, w) remaining for which the existence of a KTS(v) containing a sub-KTS(w) has not yet been established.

Note added in proof. Since the time of writing we have become aware that R. Wei and L. Zhu, in a follow-up paper to [35] entitled 'Embeddings of $S(2, 4, v)$', have come very close to a complete solution for subdesigns in BIBDs with block size 4 and $\lambda = 1$.

References

[1] A.M. Assaf and A. Hartman, Resolvable Group Divisible Designs with block size 3 (this volume).
[2] T. Beth, D. Jungnickel and H. Lenz, Design Theory (Bibliographisches Institut, Zürich, 1985).
[3] A.E. Brouwer, Optimal packings of K_4's into a K_n, J. Combin. Theory A 26 (1979) 278–297.
[4] A. Brouwer and H. Lenz, Unterräume von Blockplänen, Geometrie-Symposium Siegen 1977 (Birkhäuser-Verlag, Basel, 1979).
[5] A. Brouwer and H. Lenz, Subspaces of linear spaces of line size 4, Europ. J. Combin. 2 (1981) 323–330.
[6] A.E. Brouwer, H. Hanani and A. Schrijver, Group Divisible Designs with block-size four, Discrete Math. 20 (1977) 1–10.
[7] J. Doyen and R.M. Wilson, Embeddings of Steiner Triple Systems, Discrete Math. 5 (1973) 229–239.

[8] A. Granville, A. Moisiadis and R. Rees, On complementary decompositions of the complete graph. Graphs and Combinatorics 5 (1989) 57–61,

[9] H. Hanani, D.K. Ray-Chaudhuri and R.M. Wilson, On resolvable designs, Discrete Math. 3 (1972) 343–357.

[10] C. Huang, E. Mendelsohn and A. Rosa, On partially resolvable t-partitions, Annals Discrete Maths. 12 (1982) 169–183.

[11] E.R. Lamken and S.A. Vanstone, Elliptic semiplanes and group divisible designs with orthogonal resolutions, Aequationes Mathematicae 30 (1986) 80–92.

[12] R. Mathon and A. Rosa, Some results on the existence and enumeration of BIBDs, Mathematics Report 125 (McMaster University, 1985).

[13] E. Mendelsohn and R. Rees, Mandatory representation designs, J. Combin. Theory A, 49 (1988) 349–362.

[14] E. Mendelsohn and A. Rosa, One-factorizations of the complete graph-A survey, J. Graph Theory 9 (1985) 43–65.

[15] W.H. Mills, A new block design, Proc. SE Conf. Combinatorics, Graph Theory and Computing (Boca Raton, Fla., 1975) 461–465.

[16] W.H. Mills, Two new block designs, Utilitas Math. 7 (1975) 73–75.

[17] W.H. Mills, The construction of balanced incomplete block designs with $\lambda = 1$, Proc. 7th Conf. Numerical Maths. and Computing, University of Manitoba (1977) 131–148.

[18] W.H. Mills, The construction of BIBDs using non-abelian Groups, Proc. SE Conf. Combinatorics, Graph Theory and Computing (Boca Raton, Fla., 1978) 519–526.

[19] W.H. Mills, The construction of balanced incomplete block designs, Proc. SE Conf. Combinatorics, Graph Theory and Computing (1979) 73–86.

[20] W.H. Mills, Balanced incomplete block designs with $k = 6$ and $\lambda = 1$, in D.M. Jackson and S.A. Vanstone, Eds, Enumeration and Design (Academic Press, New York, 1984) 239–244.

[21] R.C. Mullin, Finite bases for some PBD-closed sets, (this volume).

[22] R.C. Mullin, D.G. Hoffman and C.C. Lindner, A few more BIBDs with $k = 6$ and $\lambda = 1$, Annals of Discrete Math. 34 (1987) 379–384.

[23] R.C. Mullin, P.J. Schellenberg, S.A. Vanstone and W.D. Wallis, On the existence of frames, Discrete Math. 37 (1981) 79–104.

[24] D.K. Ray-Chaudhuri and R.M. Wilson, Solution of Kirkman's schoolgirl problem, Symp. Pure Math 19 (AMS, 1971) 187–204.

[25] D.K. Ray-Chaudhuri and R.M. Wilson, The existence of resolvable block designs, in A Survey of Combinatorial Theory (North-Holland, 1973) 361–375.

[26] R. Rees, The perfect pair-covering numbers $cp\ (K_u \vee K_m^c)$, $u = m + 2$, $m + 3$ and $m + 4$, Utilitas Math., 32 (1987) 193–216.

[27] R. Rees and D.R. Stinson, On resolvable group-divisible designs with block size 3, Ars Comb. 23 (1987) 107–120.

[28] R. Rees and D.R. Stinson, Kirkman Triple Systems with maximum subsystems, Ars Combin. 25 (1988).

[29] R. Rees and D.R. Stinson, On the number of blocks in a perfect covering of v points, to appear in Discrete Math.

[30] R. Roth and M. Peters, Four pairwise orthogonal Latin squares of order 24, J. Combin. Theory A 44 (1987) 152–155.

[31] G. Stern and H. Lenz, Steiner Triple Systems with given subspaces; another proof of the Doyen–Wilson Theorem, Bolletino U.M.I. (5) 17-A (1980) 109–114.

[32] D.R. Stinson, The spectrum of nested Steiner Triple Systems, Graphs and Combinatorics 1 (1985) 189–191.

[33] D.R. Stinson, The equivalence of certain incomplete transversal designs and frames, Ars Combin. 22 (1986) 81–87.

[34] D.R. Stinson, Frames for Kirkman Triple Systems, Discrete Math. 65 (1987) 289–300.

[35] R. Wei and L. Zhu, Embeddings of Steiner Systems $S(2, 4, v)$, Annals of Discrete Math. 34 (1987) 465–470.

[36] R.M. Wilson, Constructions and uses of pairwise balanced designs, Math. Cent. Tracts 55 (1974) 18–41.

Appendix

Incomplete group-divisible designs with block size 4:

A 4-IGDD *of type* $(9, 3)^5$

See Theorem 2.3 and the remark following it.

A 4-IGDD *of type* $(9, 3)^4 6^1$

See the appendix in [28].

A 4-IGDD *of type* $(9, 3)^3 6^2$

Points: $(\mathbb{Z}_6 \times \{1, 2, 3, 4, 5\}) \cup (\{a, b, c\} \times \mathbb{Z}_3)$.

Groups: $\{\mathbb{Z}_6 \times \{j\} : j = 1, 2\} \cup \{(\mathbb{Z}_6 \times \{3\}) \cup (\{a\} \times \mathbb{Z}_3)\}$
$\cup \{(\mathbb{Z}_6 \times \{4\}) \cup (\{b\} \times \mathbb{Z}_3)\} \cup \{(\mathbb{Z}_6 \times \{5\}) \cup (\{c\} \times \mathbb{Z}_3)\}$.

Subgroups: $\{\{a\} \times \mathbb{Z}_3\} \cup \{\{b\} \times \mathbb{Z}_3\} \cup \{\{c\} \times \mathbb{Z}_3\}$.

Blocks: develop the following modulo 6 (the subscripts on a, b and c are to be evaluated modulo 3):

$0_1 0_2 0_3 b_0$	$0_1 5_2 0_5 b_1$
$0_1 1_3 3_5 b_2$	$0_2 5_3 4_5 b_1$
$0_1 2_2 3_4 a_2$	$0_1 1_2 4_5 a_0$
$0_2 4_4 0_5 a_1$	$0_1 0_4 1_5 a_1$
$0_1 4_2 5_3 c_0$	$0_1 3_2 2_4 c_1$
$0_1 3_3 1_4 c_2$	$0_2 3_3 0_4 c_0$
$0_1 2_3 4_4 2_5$	$0_1 4_3 5_4 5_5$
$0_2 4_3 3_4 2_5$	$0_2 2_3 2_4 5_5$

A 4-IGDD *of type* $(9, 3)^2 6^3$

Points: $(\mathbb{Z}_3 \times \{1, 2, 3, 4, 5, 6\}) \cup (\{a\} \times \mathbb{Z}_3) \cup (\{b\} \times \mathbb{Z}_3) \cup (\{c\} \times \mathbb{Z}_3)$
$\cup \{\infty_i : 1 \leq i \leq 9\}$.

Groups: $\{\{j\} \times \{1, 2, 3, 4, 5, 6\} : j = 0, 1, 2\} \cup \{(\{a\} \times \mathbb{Z}_3) \cup (\{b\} \times \mathbb{Z}_3)$
$\cup (\{c\} \times \mathbb{Z}_3)\} \cup \{\{\infty_i : 1 \leq i \leq 9\}\}$.

Subgroups: $\{\{a\} \times \mathbb{Z}_3\} \cup \{\{\infty_1, \infty_2, \infty_3\}\}$.

Blocks: develop the following modulo 3:

$a_0 0_1 1_3 2_5$	$a_0 \infty_8 2_2 0_4$	$b_0 \infty_5 2_1 0_6$	$c_0 \infty_3 2_2 1_3$
$a_0 0_2 2_4 1_6$	$a_0 \infty_9 2_3 0_6$	$b_0 \infty_6 2_3 1_4$	$c_0 \infty_4 0_2 1_5$
$a_0 \infty_4 1_1 0_3$	$b_0 \infty_1 2_4 1_5$	$b_0 \infty_7 2_2 0_3$	$c_0 \infty_5 2_3 0_4$
$a_0 \infty_5 1_2 0_5$	$b_0 \infty_2 0_2 2_6$	$b_0 \infty_8 1_3 0_5$	$c_0 \infty_6 2_1 1_2$
$a_0 \infty_6 1_5 2_6$	$b_0 \infty_3 1_1 2_5$	$b_0 \infty_9 0_1 1_2$	$c_0 \infty_7 2_5 1_6$
$a_0 \infty_7 2_1 1_4$	$b_0 \infty_4 0_4 1_6$	$c_0 \infty_1 0_3 2_6$	$c_0 \infty_8 1_1 0_6$
$\infty_1 0_1 1_1 2_1$	$\infty_2 0_3 1_3 2_3$	$c_0 \infty_2 0_1 1_4$	$c_0 \infty_9 2_4 0_5$
$\infty_1 0_2 1_2 2_2$	$\infty_2 0_5 1_5 2_5$	$\infty_3 0_4 1_4 2_4$	$\infty_3 0_6 1_6 2_6$

A 4-IGDD *of type* $(9, 3)^1 6^4$

This is just a 4-GDD of type $6^4 9^1$, obtainable by adding nine infinite points to a resolvable 3-GDD of type 6^4 (Theorem 2.1).

A 4-IGDD of type $(9, 3)^6$

See Theorem 2.3 and the remark following it.

A 4-IGDD *of type* $(9, 3)^5 6^1$

See the appendix in [28].

A 4-IGDD *of type* $(9, 3)^4 6^2$

Points: $\mathbb{Z}_{12} \times \{1, 2, 3, 4\}$.

Groups: $\{\{0+i, 4+i, 8+i\} \times \{1, 2, 4\} : i = 0, 1, 2, 3\}$
$\cup \{\{0+i, 2+i, 4+i, 6+i, 8+i, 10+i\} \times \{3\} : i = 0, 1\}$.

Subgroups: $\{\{0+i, 4+i, 8+i\} \times \{4\} : i = 0, 1, 2, 3\}$.

Blocks: develop the following modulo 12:

$0_1 1_1 2_2 0_3$	$0_1 3_2 5_2 2_3$
$1_1 3_1 10_2 0_4$	$2_1 10_3 11_3 0_4$
$6_1 11_1 0_3 0_4$	$5_1 3_2 8_3 0_4$
$7_1 1_2 5_3 0_4$	$10_1 9_2 3_3 0_4$
$9_1 1_3 4_3 0_4$	$2_2 7_2 9_3 0_4$
$5_2 6_2 6_3 0_4$	$11_2 2_3 7_3 0_4$
$0_1 3_1 6_1 9_1$	$0_2 3_2 6_2 9_2$

A 4-IGDD *of type* $(9, 3)^3 6^3$

Points: $\mathbb{Z}_9 \times \{1, 2, 3, 4, 5\}$.

Groups: $\{\{0+i, 3+i, 6+i\} \times \{1, 2, 5\} : i = 0, 1, 2\}$
$\cup \{\{0+i, 3+i, 6+i\} \times \{3, 4\} : i = 0, 1, 2\}$.

Subgroups: $\{\{0+i, 3+i, 6+i\} \times \{5\} : i = 0, 1, 2\}$.

Blocks: develop the following modulo 9:

$0_1 1_1 2_2 0_3$	$2_2 1_4 8_4 0_5$	$1_1 0_4 5_4 0_5$
$0_1 2_1 4_3 3_4$	$5_2 7_2 6_3 0_5$	$4_1 8_1 5_3 0_5$
$0_1 7_2 3_3 7_4$	$4_3 8_3 6_4 0_5$	$5_1 4_2 7_4 0_5$
$7_1 3_4 4_4 0_5$	$0_1 4_2 5_2 0_4$	$8_2 2_3 3_3 0_5$
$2_1 0_3 7_3 0_5$	$0_2 4_2 6_3 2_4$	$1_2 1_3 2_4 0_5$

A 4-IGDD *of type* $(9, 3)^2 6^4$

Points: $\mathbb{Z}_6 \times \{1, 2, 3, 4, 5, 6, 7\}$.

Groups: $\{\mathbb{Z}_6 \times \{j\} : j = 5, 6\} \cup \{\{0+i, 2+i, 4+i\} \times \{3, 4\} : i = 0, 1\}$
$\cup \{\{0+i, 2+i, 4+i\} \times \{1, 2, 7\} : i = 0, 1\}$.

Subgroups: $\{\{0+i, 2+i, 4+i\} \times \{7\} : i = 0, 1\}$.

Blocks: develop the following modulo 6:

$0_1 1_2 0_5 0_6$	$0_2 0_4 2_5 1_7$	$0_1 2_3 2_6 1_7$
$0_1 5_2 0_3 1_4$	$0_3 4_5 5_6 2_7$	$0_1 3_4 3_6 3_7$
$0_2 1_2 4_3 1_6$	$0_4 5_5 4_6 2_7$	$0_2 5_3 3_6 5_7$
$0_1 5_3 2_4 1_6$	$0_1 3_2 1_5 5_6$	$0_3 1_3 3_5 4_7$
$0_2 3_4 1_5 4_6$	$0_1 1_1 5_4 5_5$	$0_4 1_4 3_6 4_7$
$0_1 0_4 3_5 5_7$	$0_1 3_3 2_5 4_6$	$0_1 3_1 0_3 3_3$
$0_2 2_3 3_5 3_7$	$0_2 0_3 5_4 0_5$	$0_2 3_2 0_4 3_4$

A 4-IGDD *of type* $(9, 3)^1 6^5$

This is just a 4-GDD of type $6^5 9^1$, and can be found in the appendix of [27].

Remark. The 4-IGDDs with no groups of size 9 are of course just 4-GDDs of types 6^5, 6^6, and so exist by [6].

Group-divisible designs with block size 4:

A 4-GDD *of type* $3^1 6^6$

Points: $\mathbb{Z}_{36} \cup (\{a\} \times \mathbb{Z}_3)$.

Groups: $\{\{0+i, 6+i, 12+i, 18+i, 24+i, 30+i\}: i = 0, 1, 2, 3, 4, 5\}$
$\cup \{\{a\} \times \mathbb{Z}_3\}$.

Blocks: develop the following modulo 36 (the subscript on a is to be evaluated modulo 3):

$$0, 1, 3, 11 \quad 0, 5, 14, 21 \quad 0, 4, 17, a_0$$

A 4-GDD *of type* $3^{11} 9^1$

Points: $(\mathbb{Z}_6 \times \{1, 2, 3, 4, 5, 6\}) \cup (\{a, b\} \times \mathbb{Z}_3)$.

Groups: $\{\{0+i, 2+i, 4+i\} \times \{j\}: i = 0, 1; j = 1, 2, 3, 4, 5\} \cup \{\{a\} \times \mathbb{Z}_3\}$
$\cup \{(\mathbb{Z}_6 \times \{6\}) \cup (\{b\} \times \mathbb{Z}_3)\}$.

Blocks: develop the following modulo 6 (the subscripts on a and b are to be evaluated modulo 3):

$0_1 0_3 0_4 0_6$	$0_3 1_3 0_5 b_0$	$0_1 0_2 1_2 b_2$
$0_1 3_2 1_4 3_6$	$0_2 5_3 0_4 1_4$	$0_1 5_4 5_5 b_0$
$0_1 4_3 5_6 a_0$	$0_1 2_2 3_3 1_6$	$0_1 1_1 5_2 2_3$
$0_2 5_5 3_6 a_2$	$0_1 5_3 3_4 4_6$	$0_2 4_3 0_5 1_5$
$0_2 2_3 3_5 4_6$	$0_1 0_5 2_6 a_2$	$0_1 3_1 1_5 4_5$
$0_3 5_4 4_5 3_6$	$0_2 2_4 4_5 1_6$	$0_2 3_2 a_0 b_0$
$0_2 0_3 3_4 a_1$	$0_2 5_4 2_5 2_6$	$0_3 3_3 a_0 b_1$
$0_1 4_4 2_5 b_1$	$0_1 2_4 3_5 a_1$	$0_4 3_4 a_0 b_2$

A 4-GDD *of type* $3^4 6^2$

Points: $\mathbb{Z}_{12} \cup (\{a\} \times \mathbb{Z}_6) \cup (\{b\} \times \mathbb{Z}_2) \cup \{\infty_i : 1 \leq i \leq 4\}$.

Groups: $\{\{0+i, 4+i, 8+i\}: i = 0, 1, 2, 3\} \cup \{\{a\} \times \mathbb{Z}_6\}$
$\cup \{(\{b\} \times \mathbb{Z}_2) \cup \{\infty_i : 1 \leq i \leq 4\}\}$.

Blocks: the following, for $i = 0, 1, 2, 3, 4, 5$ (the subscripts on b are to be evaluated modulo 2):

$a_i(0+2i)(1+2i)\infty_1$	$a_i b_i (2+2i)(4+2i)$
$a_i(3+2i)(8+2i)\infty_2$	$a_i b_{i+1}(5+2i)(7+2i)$
$a_i(6+2i)(11+2i)\infty_3$	$(0+2i)(3+2i)(6+2i)(9+2i)$
$a_i(9+2i)(10+2i)\infty_4$	

A 4-GDD *of type* $6^6 9^1$
Points: $\mathbb{Z}_{36} \cup (\{a\} \times \mathbb{Z}_9)$.
Groups: $\{\{0+i, 6+i, 12+i, 18+i, 24+i, 30+i\}: i = 0, 1, 2, 3, 4, 5\}$
$\cup \{\{a\} \times \mathbb{Z}_9\}$.
Blocks: develop the following modulo 36 (the subscripts on a are to be evaluated modulo 9):

$$0, 1, 5, 27 \quad 1, 17, 34, a_0 \quad 0, 2, 13, a_0 \quad 5, 12, 33, a_0$$

A 4-GDD *of type* $6^6 12^1$
Points: $(\mathbb{Z}_{12} \times \{1, 2, 3\}) \cup \{\infty_i : 1 \leqslant i \leqslant 12\}$.
Groups: $\{\{0+i, 6+i\} \times \{1, 2, 3\} : i = 0, 1, 2, 3, 4, 5\} \cup \{\{\infty_i : 1 \leqslant i \leqslant 12\}\}$.
Blocks: develop the following modulo 12:

$$\begin{array}{ll}
\infty_1 0_1 5_2 4_3 & \infty_2 0_1 4_2 2_3 \\
\infty_3 0_1 8_2 5_3 & \infty_4 0_1 3_2 11_3 \\
\infty_5 0_1 1_2 8_3 & \infty_7 0_1 2_2 7_3 \\
\infty_8 0_1 11_2 3_3 & \infty_9 0_1 10_2 1_3 \\
\infty_{10} 0_1 7_2 9_3 & \infty_{11} 0_1 9_2 10_3
\end{array}$$

then, for each $j = 1, 2, 3$ construct a 4-GDD of type 2^7 on the groups $\{\{0+i, 6+i\} \times \{j\} : i = 0, 1, 2, 3, 4, 5\} \cup \{\{\infty_6, \infty_{12}\}\}$ (a 4-GDD of type 2^7 is obtained by developing the block $0, 1, 4, 6$ modulo 14).

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 281–284
North-Holland

CYCLICAL STEINER TRIPLE SYSTEMS ORTHOGONAL TO THEIR OPPOSITES

Shmuel SCHREIBER
Dept. of Mathematics and Computer Science, Bar-Ilan University, Ramat Gan 52100, Israel

Presented to Professor Haim Hanani on his 75th birthday.

A Steiner Triple System (STS) consists of a set X together with a collection B of 3-subsets of X such that every pair of elements of X occurs in exactly one member of B. (X, B_1) and (X, B_2) are said to be *orthogonal* if $B_1 \cap B_2 = \emptyset$ and for $(x, y, z) \in B_1$, $(u, v, z) \in B_1$ there exists no $w \in X$ such that (x, y, w) *and* $(u, v, w) \in B_2$.

It should be noted that this terminology is not unique. Mullin and Vanstone [1] and Rosa [2, p. 125] prefer to call such pairs of STSs *perpendicular*. However, Mendelsohn [3] reserves this term for a 4-column array of elements of X, any 3 of which form a STS; here we shall retain the older term, orthogonal.

Mullin and Nemeth [4], (as quoted in [2]), have shown that for X = a finite field of order $6q + 1$, with generator g, one may obtain a pair of orthogonal STS's on X by including q sets of the form $\{h + g^r, h + g^{r+2q}, h + g^{r+4q}\}$ in B_1, for all $h \in X$, while B_2 will consist of the triple $\{h - g^r, h - g^{r+2q}, h - g^{r+4q}\}$ for appropriate values of r between 0 and $q - 1$. This partially solves the existence problem for orthogonal pairs, and ample literature is quoted in [2].

In what follows, we present something of a natural extension of this result.

Let X be a set of order $6q + 1$, closed under addition. Thus X might be Z_{6q+1}, or the set of all ordered *pairs*, triples, k-tuples of some $\mathbb{Z}_m$ with m^2, m^3 or $m^k = 6q + 1$ (in which case, addition is to be understood componentwise). By some abuse of language, we shall call the STS (X, B) *cyclical* if $(a, b, c) \in B$ implies $(a + h, b + h, c + h) \in B$ for every $h \in X$. A counting argument will show that in this case, B consists of q sequence each containing $|X|$ triples.

Lemma 1. *If* (X, B) *is a cyclical* STS, *and* $(a, b, c) \in B$, *then* $(-b, -a, d) \notin B$ *for any* $d \in X$.

Proof. Taking $h = a + b$, $(-b + h, -a + h, d + h) = (a, b, a + b + d)$; thus the pair (a, b) would appear twice. □

Definition. For a STS (X, B), call $(X, -B)$ the *opposite* STS, where $-B$ is the set of triples $(-a, -b, -c)$ for $(a, b, c) \in B$. By Lemma 1, if (X, B) is a *cyclic* STS, $(X, -B)$ is disjoint from it.

Let again X be a set of order $6q+1$, closed under addition. If the elements of X are the k-tuples of Z_m, with $m^k = 6q+1$, then obviously $(m, 3) = 1$. Then for any triple (a, b, c) of elements of X, there exists a $h \in X$, such that $(a+h) + (b+h) + (c+h)$ sum to zero modulo m, since for the rth component of h we may always solve $a_r + b_r + c_r + 3h_r \equiv 0 \pmod{m}$. Moreover, this h is unique, for adding any $h' \in X$ will add a multiple of 3 to each nonzero component. Call $(a+h, b+h, c+h)$ the *zero-sum* triple of the sequence containing (a, b, c), and we obtain

Lemma 2. *In a cyclical* STS (X, B), *with* $|X| = 6q+1$, *each sequence of* B *contains a unique zero-sum triple.*

Proposition 1. *Let* $|X| = 6q+1$, (X, B_1) *a cyclical STS and* $(X, B_2) = (X, -B_1)$ *the opposite cyclical* STS; *if no element of* X *appears more than once in the* $3q$ *elements of the zero-sum triples of* B_1, *then* (X, B_1) *is orthogonal to* (X, B_2).

Preliminary remark. The conditions imposed by Mullin and Nemeth are somewhat more restrictive: none of the q zero-sum triples of B_2 can have an element in common with a zero-sum triple of B_1.

Proof. Note first that by Lemma 1, B_1 and B_2 can have no triple in common.

For the orthogonality condition to fail, there should be two triples $(x, y, z), (u, v, z) \in B_1$ and $(x, y, w), (u, v, w) \in B_2$; since we are dealing with *cyclical* STSs, this is equivalent to $(x-z, y-z, 0)$ and $(u-z, v-z, 0) \in B_1$ as against $(x-z, y-z, w-z)$ and $(u-z, v-z, w-z) \in B_2$. It is therefore sufficient to consider in B_2 the companions of pairs of elements of X_1 having zero as third element in triples of B_1.

To check the circumstances more explicitly, suppose sequences 1, 2, 3 of B_1 contain the zero-sum triples

$$(a_1, b_1, -a_1-b_1); (a_2, b_2, -a_2-b_2); (a_3, b_3, -a_3-b_3)$$

(all g entries distinct by hypothesis), from which we may derive, respectively

$$(0, b_1-a_1, -2a_1-b_1), (a_2-b_2, 0, -a_2-2b_2), (2a_3+b_3, a_3+2b_3, 0) \in B_1$$

and consequently

$$(0, a_1-b_1, 2a_1+b_1), (b_2-a_2, 0, a_2+2b_2); (-2a_3-b_3, -a_3-2b_3, 0) \in B_2.$$

To restore the nonzero entries of the first 3 triples, we have to add $-3a_1$ to the first, $-3b_2$ to the second, and $3a_3+3b_3$ to the third, giving

$$(-3a_1, -2a_1-b_1, b_1-a_1), (-a_2-2b_2, -3b_2, a_2-b_2),$$
$$(a_3+2b_3, 2a_3+b_3, 3a_3+3b_3) \in B_2.$$

But since $(|X|, 3) = 1$ and a_1, b_2, $a_3 + b_3$ are distinct by hypothesis, the factor -3 does not affect the inequality and this completes the proof. □

Example. $X = \mathbb{Z}_{19}$. The Mullin–Nemeth solution, in one version, gives

$$(1,7,11),(2,3,14),(4,6,9) \in B_1; (5,16,17),(10,13,15),(8,12,18) \in B_2,$$

and Proposition 1 offers an additional solution

$$(1,6,12),(4,7,8),(9,11,18) \in B_1; (1,8,10),(7,13,18),(11,12,15) \in B_2,$$

which, as one may easily verify, is not equivalent to the one above.

Proposition 2. *Let* (X, B_1), (X, B_2) *be a pair of cyclical* STSs *satisfying the conditions of Proposition* 1, *and let* (Y, B_3), (Y, B_4) *be another such pair. Then for* $Z =: X \times Y$, *a choice of zero-sum triples* B_5 *and* B_6 *may be found such that the cyclical* STSs *on* Z *generated by* B_5 *and* B_6 *be again orthogonal.*

Proof. One such choice whose verification, while somewhat tedious, is straightforward would be:

(α) for every zero-sum triple $(x_1, x_2, x_3) \in B_1$, put $((x_1, 0)(x_2, 0), (x_3, 0) \in B_5$;

(β) choose a cyclic order in the zero-sum triples $(y_1, y_2, y_3) \in B_3$, and for every (x_1, x_2, x_3) as above include in B_5,

$$((x_1, y_1), (x_2, y_2), (x_3, y_3)); ((x_1, y_2), (x_2, y_3), (x_3, y_1));$$
$$((x_1, y_3), (x_2, y_1), (x_3, y_2)); ((x_1, -y_1), (x_2, -y_2), (x_3, -y_3));$$
$$((x_1, -y_2), (x_2, -y_3), (x_3, -y_1)); ((x_1, -y_3), (x_2, -y_1), (x_3, -y_2));$$

(γ) add all the triples of the form $((0, y_1), (0, y_2), (0, y_3))$. □

The reader might wish to check the following example, with $X = \mathbb{Z}_{13}$, $B_1 \ni (1, 3, 9), (2, 6, 5)$; $Y = \mathbb{Z}_7$, $B_3 \ni (1, 2, 4) \Rightarrow Z = \mathbb{Z}_{91}$, comparing the residues modulo 13 and modulo 7 of the following 15 triples

(α) (14, 42, 35), (28, 84, 70)
(β) (1, 16, 74) (15, 58, 18)
(79, 81, 22) (2, 32, 57)
(53, 29, 9) (67, 71, 44)
(27, 68, 87) (41, 19, 31)
(66, 55, 61) (80, 6, 5)
(40, 3, 48) (54, 45, 83)
(γ) (78, 65, 39).

It is very probable that Lindner and Mendelsohn [5], (as quoted in [2], loc. cit.), already had a similar construction for product orders, based on the results of

Mullin and Nemeth. They conclude that the existence problem for orthogonal STSs of order $6k+1$ would be solved if $6k+1$ were a product of two primes $\equiv(-1) \pmod 6$.

Following this, I invited Ron Chernin of Tel-Aviv University to do an exhaustive computer search for a cyclical STS of the smallest possible order, 55, but he found no solutions satisfying the condition of Proposition 1.

References

[1] R.C. Mullin and S.A. Vanstone, Steiner systems and Room squares, Annals of Discrete Math. 7 (1980) 95–104.
[2] A. Rosa, Intersection properties of Steiner systems, Annals of Discrete Math. 7 (1980) 115–128.
[3] E. Mendelsohn, Perpendicular arrays of triple systems, Annals of Discrete Math. 7 (1980) 89–94.
[4] R.C. Mullin and E. Nemeth, On furnishing Room squares, J. Combin. Theory 7 (1969) 266–272.
[5] C.C. Lindner and N.S. Mendelsohn, Construction of perpendicular Steiner quasigroups, Aeq. Math. 9 (1973) 150–156.

Discrete Mathematics 77 (1989) 285–297
North-Holland

SYMMETRIC QUASIGROUPS OF ODD ORDER

Shmuel SCHREIBER
Dept. of Mathematics and Computer Science, Bar-Ilan University, Ramat Gan 52100, Israel

Presented to Professor Haim Hanani on his 75th birthday,
with sincere good wishes.

Quasigroups of yet another type turn out to be related to Steiner Triple Systems, though the connection is rather loose and not as precise as in the various coordinatizing bijections described in [3]. However, families of *pairs* formed by abelian groups of odd order and quasigroups defined on the same set of elements have repeatedly been used in the literature to construct Large Sets [8] of Steiner Triple Systems. In Section 1, these quasigroups and their association with abelian groups are described, while Section 2 is devoted to applications to STSs.

1. Definitions and basic properties

1.1. *Quasigroups and squodds*

A quasigroup on a set X is a mapping $(\cdot)$ from $X \cdot X$ onto X such that of three elements of X satisfying $a \cdot b = c$, any two determine the third uniquely; that is, for any $x \in X$, the mapping $y \to x \cdot y$ of X into X is one-to-one onto, a permutation. The operation (and the quasigroup) is said to be *totally symmetric* if $a \cdot b = c$ implies $b \cdot a = c$ and $c \cdot a = b$. We shall often write x^2 for $x \cdot x$, although this is only customary in the associative case, and call it the *square* of x. An element x of a quasigroup is called *idempotent* if it equals its own square, $x = x \cdot x$.

Suppose the totally symmetric quasigroup $Q(\cdot)$ on the set X contains an idempotent ω, and no other x for which $x \cdot x = \omega$, which also excludes $\omega \cdot x = x$. Then the multiplication by ω permutes the elements of $X \setminus \omega$ in pairs, since $\omega \cdot x = \omega$ for $x \neq \omega$ would imply $\omega \cdot \omega = x$, contrary to the assumption $\omega \cdot \omega = \omega$. Thus the order v of X, if finite, must be odd. If in addition, one requires ω to be the *only* idempotent, this order has to be prime to 3, as can be seen by counting the v^2 entries in the standard multiplication table of Q; indeed, an equality such as $a \cdot b = c$, with all threes values distinct, requires six entries, one for each ordered pair of factors, while one of the form $a \cdot a = b$ requires 3 entries. Adding one for $\omega \cdot \omega = \omega$, we find $v^2 \equiv 1 (\mathrm{mod}\, 3)$. Write X^* for $X \setminus \omega$. The quasigroups to be discussed will satisfy some more restrictions.

Definition 1.1.1. A SQUODD (short for Symmetric Quasigroups of Odd Order)

$Q(\cdot)$ on a set X of order v is
(i) a totally symmetric quasigroup with a unique idempotent $\omega \in X$, for which
(ii) the mapping $x \to x \cdot x$ is a *permutation* π of the set $X^* = X \setminus \omega$ and
(iii) every cycle of π is of even length.

Example 1.1.2.

	ω	a	b	c	d
ω	ω	c	d	a	b
a	c	b	a	ω	d
b	d	a	c	b	ω
c	a	ω	b	d	c
d	b	d	ω	c	a

$\leftrightarrow (\omega\omega\omega), (\omega ac), (\omega bd), (aab), (bbc), (ccd), (dda).$

It is often convenient to list the squodd by enumerating its $(v+1)(v+2)/6$ triples, instead of the full multiplication table.

Remark 1.1.3. No cycle in the permutation π can be of length less than 4, since a cycle of length 2, $x \cdot x = y$, $y \cdot y = x$ would require $x \cdot y = x$ and $x \cdot y = y$ at the same time.

1.2. Graph notation and direct sums

Given a squodd $Q(\cdot)$ on a set of order v, form a graph of v vertices, labelled by the (unordered) pairs (x, x^2), $x \in X$, two vertices being connected by an edge if their labels have an entry in common; then the graph will consist of a single *loop* on the vertex (ω, ω) and of one or more cycles of even order. It is well known that a graph containing no cycles of odd order is *bipartite*, that is, its vertices may be partitioned (eventually in more than one way) into two classes, with no edge connecting two vertices of the same class. The whole graph so obtained, which will be termed the *diagonal graph* of the squodd $Q(\cdot)$, will thus consist of one *odd* component, the loop on (ω, ω), and a bipartite graph with vertices labelled by certain pairs of elements of X^*, which we will call the *main part* of the diagonal graph.

Definition 1.2.1. Given two graphs, G_1 with vertex set X_1 and G_2 with vertex set X_2, the *direct sum* $G_1 \oplus G_2$ will be a graph whose vertices are the *ordered* pairs (x_1, x_2), $x_i \in X_i$, in which $((x_1, x_2), (y_1, y_2))$ form an edge if and only if (x_1, y_1) is an edge of G_1 *and* (x_2, y_2) one of G_2.

The following lemma will also find application later on:

Lemma 1.2.2. *The direct sum of two graphs is bipartite if and only if at least one of the summands is bipartite.*

Proof. Since the only graphs that are not bipartite are the ones containing cycles of odd order, it is sufficient to verify the easily checked claim that a cycle of order a in the sum can only be generated by a cycle of order b in one summand, and one of order c in the other, where a is the least common multiple of b and c. □

Definition 1.2.3. Let $Q_1(\llcorner)$ be a squodd on the set X_1, with idempotent ω_1, and $Q_2(\urcorner)$ a squodd on the set X_2, with idempotent ω_2; then the *direct sum* of Q_1 and Q_2, denoted by $Q_1 \oplus Q_2$, is a quasigroup $Q(*)$ on $X_1 \times X_2$, with $(x_1, x_2) * (y_1, y_2) = (z_1, z_2)$ if and only if $x_1 \llcorner y_1 = z_1$ *and* $x_2 \urcorner y_2 = z_2$, $(x_i, y_i, z_i \in X_i)$.

Proposition 1.2.4. *The direct sum of two squodds is a squodd. Moreover, if the direct sum of two quasigroups satisfying conditions* (i) *and* (ii) *of Definition* 1.1.1 *satisfies condition* (iii) *as well, so does each summand.*

Proof. It is obviously enough to verify the second statement.

The diagonal graph of the sum consists of 4 parts:

(1) the loop with single vertex (ω_1, ω_2),

(2) the part derived from elements of the form (x_1, ω_2), with $x_1 \in X_1^*$, which is isomorphic to the *main part* of the diagonal graph of $Q_1(\llcorner)$,

(3) the part derived from elements of the form (ω_1, x_2) with $x_2 \in X_2^*$, isomorphic to the *main part* of the diagonal graph of $Q_2(\urcorner)$,

(4) the part derived from elements of the form (x_1, x_2) with $x_1 \in X_1^*$ and $x_2 \in X_2^*$ isomorphic to the *direct sum* (in the sense of Definition 1.2.1) of the main parts of the diagonal graphs of the summands, and thus to the direct sum of parts (2) and (3).

By Lemma 1.2.2, the graph consisting of parts (2), (3) and (4) – which is the main part of the diagonal graph of $Q(*)$ – will be bipartite if, and only if, parts (2) and (3) are bipartite, too. □

1.3. Squodds and abelian groups; The main example

For some of the constructions in the sequel, the multiplicative order of -2 modulo an odd prime p is relevant.

Lemma 1.3.1.

(α) *If* $p \equiv 3 \pmod 8$, *the multiplicative order of* -2 *is an odd integer*;

(β) *If* $p \equiv 5 \pmod 8$, *the multiplicative order of* -2 *is a multiple of* 4;

(γ) *If* $p \equiv 7 \pmod 8$, *the multiplicative order of* -2 *is twice an odd number*;

(δ) *If* $p \equiv 1 \pmod 8$, *the multiplicative order of* -2 *may be either odd, or a multiple of* 4, *or twice an odd number.*

(In fact, a heuristic consideration, which can be made precise by a zeta-function argument, will show that for $6N$ primes selected at random from the sequence $8k+1$, with N large, about N will satisfy condition (α), another N condition (γ), and $4N$ condition (β).)

Proof. All four statements follow from the fact (see any elementary text on the Theory of Numbers) that $\underline{-2}$ is a quadratic residue for primes $\equiv 1$ or $3 \pmod 8$ and a non-residue for primes $\equiv 5$ or $7 \pmod 8$. □

Definition 1.3.1.1 An odd prime p will be designated as an α-prime, a β-prime, or a γ-prime, according to the condition in Lemma 1.3.1 satisfied by the multiplicative order of $-2 \pmod p$.

Definition 1.3.1.2 Let A be an abelian group, written additively, on a set X of order v, $(v, 6) = 1$, let $h \in A$ and $Q(\cdot)$ a Totally Symmetric quasigroup on X. Then the quasigroup $Q(*)$, defined by

$$(x+h)*(y+h) = (x \cdot y) + h$$

(which is obviously isomorphic to $Q(\cdot)$) will be called an h-shift of $Q(\cdot)$ with respect to A.

Definition 1.3.1.3 Let A be an abelian group, written additively, on a set X of order v, $(v, 6) = 1$, and $h \in A$. Then we shall designate the quasigroup $Q(*)$, defined by

$$x * y = z \Leftrightarrow x + y + z = 3h \text{ in } A$$

as $\mathrm{Der}_h A$, and we shall write $\mathrm{Der}(A)$ for $\mathrm{Der}_0(A)$.

Proposition 1.3.2. *For A and h as above, $\mathrm{Der}_h(A)$ will be a squodd if, and only if, no α-prime divides the order v of A.*

Proof. The quasigroup will obviously be totally symmetric, with the *unique* idempotent h; for, with $k \neq h$ and $3k = 3h$ we have $3(k-h) = 0$ and thus, by the hypothesis on v, $k = h$, a contradiction. Similarly, no diagonal element is repeated, for $a_1 + a_1 + b = a_2 + a_2 + b = 3h$ implies $2a_2 = 2a_1$, thus again $a_2 = a_1$, v being odd. It only remains to check whether all cycles in the diagonal permutation of $A \setminus (h)$ are of even length, and for this we may obviously assume $h = 0$.

Given any $a \neq 0$ in A, its order will be some w, dividing v. The diagonal cycle generated by a in $\mathrm{Der}_0(A)$ will then be

$$\langle a, (-2)^1 a, (-2)^2 a, \ldots, (-2)^{k-1} a \rangle, \quad \text{with } (-2)^k \equiv 1 \pmod w.$$

For w a β-prime or a γ-prime, k will be even, by Lemma 1.3.1. If w is some power p^r of a β-prime or a γ-prime p, k will be the exponent of -2 for p, multiplied by some power $\leqslant r$ of p, thus again even. If w is a product of such prime powers, k will again be even, being the l.c.m. of the exponents for the single prime powers. Recall finally that if v is divisible by any α-prime p, A will necessarily contain some element b of order p, which, again by Lemma 1.3.1, will generate a cycle of odd length. □

As an example we may translate Example 1.1.2 above into $\mathrm{Der}_2(C_5)$, setting $\omega = 2$, $a = 0$, $b = 1$, $c = 4$, $d = 3$; or consider $\mathrm{Der}_4(C_7)$, which gives the triples:

$$(005), (014), (023), (066), (113), (122), (156), (246), (255), (336), (345), (444).$$

However, if we attempt the same operation on C_{11} with, say, 0 as idempotent, we shall find the two *odd* diagonal cycles $\langle 1, 9, 4, 3, 5\rangle$ and $\langle 2, 7, 8, 6, 10\rangle$. We shall, however, see in a later section that squodds exist of any finite order, prime to 6.

Whether or not the order v of A, $(v, 6) = 1$, satisfies the restriction of Proposition 1.3.2, we have:

Proposition 1.3.2.1 *For $h, k \in A$, $k \neq h$, $\mathrm{Der}_k(A)$ and $\mathrm{Der}_h(A)$ have no triple in common.*

Proof. If $x + y + z = 3h = 3k$, then $3(k - h) = 0$. Thus $k - h = 0$ by the hypothesis on v. □

This is equivalent to saying that no two triples in $\mathrm{Der}_k(A)$ are *shifts* of each other, or belong to the same additive A-orbit. It is easy to check that there are $(v + 1)(v + 2)/6$ such orbits of triples: one for triples with three equal entries, $v - 1$ for triples with one entry repeated and $(v - 1)(v - 2)/6$ for triples with 3 distinct entries.

Definition 1.3.2.2 Given an abelian group A, and a squodd $Q(\cdot)$, on a set X of order v, $(v, 6) = 1$, the pair (A, Q) will be called an I-pair if all triples of $Q(\cdot)$ belong to different A-orbits (or: if no two triples of $Q(\cdot)$ are *A-congruent*).

If we consider the diagonal entries of $Q(\cdot)$, $(x, x \cdot x)$ as (unordered) *pairs* rather than as triples with one entry repeated, we certainly *cannot* require all $v - 1$ of these to fall into different A-orbits, since there are only $(v - 1)/2$ such orbits. We may, however, require:

Definition 1.3.3. Given an abelian group A, and a squodd $Q(\cdot)$ on a set X of order v, $(v, 6) = 1$; if no two triples of $Q(\cdot)$ with 3 distinct entries are A-congruent, and if, in addition, the main part of the diagonal graph of $Q(\cdot)$ remains bipartite when one connects by an edge any two vertices representing pairs of elements in the same A-orbit, we shall call the pair (A, Q) a D-pair.

This condition, incidentally, ensures the appearance of exactly two pairs from each A-orbit, covering the $v-1$ diagonal entries (x, x^2) with $x^2 \neq x$; for if three congruent pairs were to appear, the added edges would form a triangle.

Example 1.3.3.1 $\mathrm{Der}(C_5)$ does *not* form a D-pair with C_5: the diagonal sequence is $(1,3)$, $(3,4)$, $(4,2)$, $(2,1)$, the vertices of a quadrangle. But since $4-2=3-1$ and $2-1=4-3$, the two additional edges turn this into the Complete Graph on 4 vertices, K_4, which is certainly not bipartite.

Example 1.3.3.2 $\mathrm{Der}_4(C_7)$, considered above, forms a D-pair with C_7. The vertices $(0,5)$, $(5,2)$, $(2,1)$, $(1,3)$, $(3,6)$, $(6,0)$ form a hexagon, in which the additional edges $((0,5),(1,3))$, $((5,2),(3,6))$ and $((2,1),(6,0))$ close *even* cycles. We shall see that this is due to 7 being a γ-prime.

Examples 1.3.3.3 and 1.3.3.4. The reader is invited to check in detail that the following two squodds form D-pairs with C_{11}:

(α) [1]: (0 0 0), (0 1 6), (0 2 3), (0 4 8), (0 5 7), (0 9 10), (1 4 5), (1 7 9), (1 8 10), (2 6 7), (2 8 9), (2 4 10), (3 4 7), (3 5 10), (3 6 9), (5 6 8); (1 1 2), (2 2 5), (5 5 9), (9 9 4), (4 4 6), (6 6 10), (10 10 7), (7 7 8), (8 8 3), (3 3 1).

(β) [4]: (0 0 0), (0 1 10), (0 2 6), (0 3 5), (0 4 7), (0 8 9), (1 3 4), (1 5 6), (1 7 9), (2 4 9), (2 5 10), (2 7 8), (3 6 7), (3 9 10), (4 5 8), (6 8 10); (1 1 2), (2 3 3), (3 3 8), (8 8 1), (4 4 6), (6 6 9), (9 9 5), (5 5 7), (7 7 10), (10 10 4).

Note that these two squodds do *not* form I-pairs with C_{11}: thus in the first (7 7 8) and (1 1 2) are C_{11}-congruent, and so are (6 6 10) and (5 5 9), (8 8 3) and (9 9 4); while in the second, we find (2 2 3) and (1 1 2), (10 10 4) and (3 3 8), (5 5 7) and (4 4 6), (6 6 9) and (7 7 10).

Proposition 1.3.3.5 *Let A be an abelian group of order v, $(v,6)=1$, $h \in A$, and let* $\mathrm{Der}_h(A)$ *be a squodd. Then* $(A, \mathrm{Der}_h(A))$ *form a D-pair if, and only if, all the prime factors of v are γ-primes.*

Proof. Note that two pairs of elements of A, (a_1, a_2) and (b_1, b_2), are congruent if $b_2 - b_1 = \pm(a_2 - a_1)$, and that the differences between successive elements in the diagonal cycle generated by $x \neq h$,

$$\langle x, 3h-2x, -3h+4x, 9h-8x, -15h+16x, \ldots, h+(-2)^i(x-h), \ldots\rangle$$

equal $3(h-x)$ multiplied by successive powers of -2 modulo w, if w is the order of $x-h$ in A. Since $\mathrm{Der}_h(A)$ is a squodd, the multiplicative order of -2 in C_w, by Proposition 1.3.2, will be even, say $2k$. If w happens to be a β-prime or a γ-prime p, then $(-2)^k$ will equal -1 modulo p, and after k steps along the cycle we shall encounter a pair whose difference is $-3(h-x)$, congruent to the first, and from then onwards, pairs k steps apart will remain congruent to the end of the cycle. If p is a β-prime, k is even and (compare Example 1.3.3.1) the added edges will close odd cycles, while if p is a γ-prime, k is odd (compare Example 1.3.3.2) and the added edges will close even cycles, and thus the bipartite character of the main part of the diagonal graph will be preserved.

The rest of the proof follows exactly the same lines as that of Proposition 1.3.2. □

The D-pairs so obtained are automatically I-pairs, by Proposition 1.3.2.1 and Definition 1.3.2.2.

Following this, and in view of several applications further on, we may introduce

Definition 1.3.4. The pairs (A, Q) will be called an I-D-pair if it is both an I-pair and a D-pair.

By Proposition 1.3.3.5, $(C_{13}, \mathrm{Der}_h(C_{13}))$ cannot form an I-D-pair. However, not all such pairs are formed by derivation. The reader is invited to examine the following example of a squodd forming an I-D-pair with C_{13}:

Example 1.3.4.1 [2]. (0 0 0), (0 1 9), (0 2 7), (0 3 11), (0 4 6), (0 5 8), (0 10 12), (1 2 3), (1 4 5), (1 7 12), (1 8 11), (2 4 12), (2 6 11), (2 9 10), (3 4 8), (3 5 9), (3 7 10), (4 7 11), (5 6 12), (5 10 11), (6 7 9), (6 8 10), (8 9 12); (1 1 6), (6 6 3), (3 3 12), (12 12 11), (11 11 9), (9 9 4), (4 4 10), (10 10 1), (2 2 5), (5 5 7), (7 7 8), (8 8 2).

1.3.5. *Pairs and direct sum operations*

As both abelian groups and squodds are closed under direct sum operations, we may look at what happens to pairs in this context.

Proposition 1.3.5.1. *I-pairs are closed under Direct Sum operations. If both* (A_1, Q_1) *and* (A_2, Q_2) *are I-pairs, so is* $(A_1 \oplus A_2, Q_1 \oplus Q_2)$.

Proof omitted.

A similar statement for D-pairs does *not* hold. In fact:

Proposition 1.3.5.2. *I-D-pairs are closed under Direct Sum operations. Moreover, if* A_i, Q_i *are defined on a set* X_i, $i = 1, 2$, *and if* $(A_1 \oplus A_2, Q_1 \oplus Q_2)$ *is a D-pair, then each of* (A_i, Q_i) *is already an I-D-pair, and so is the sum.*

Proof. Since Lemma 1.2.2 ensures that the bipartite character of the main part of the diagonal graph containing the added edges in each summand will not be violated by the Direct Sum operation, it is enough to prove the second statement.

Let 0_i be the zero of A_i, and ω_i the idempotent of Q_i; then $Q_1 \oplus Q_2$ will contain elements of the form (ω_1, a_2) forming a squodd isomorphic to Q_2, whose pairs and triples are acted on by the shift-operations of the subgroup $\langle(0_1, h_2)\rangle$ of $A_1 \oplus A_2$, so (A_2, Q_2) should be at least a D-pair; and similarly for (A_1, Q_1).

Suppose one summand, say (A_2, Q_2), is *not* an I-D-pair; then its diagonal (compare Examples 1.3.3.3, 1.3.3.4) contains A_2-congruent triples, (a_2, a_2, b_2) and $(a_2+h_2, a_2+h_2, b_2+h_2)$. If $x_1 \cdot y_1 = z_1$ in Q_1, and all 3 entries of (x_1, y_1, z_1) are distinct, $Q_1 \oplus Q_2$ contains the two triples $((x_1, a_2), (y_1, a_2), (z_1, b_2))$ and $((x_1, a_2+h_2), (y_1, a_2+h_2), (z_1, b_2+h_2))$, the second being a shift of the first by $(0_1, h_2) \in A_1 \oplus A_2$, contrary to the first condition in Definition 1.3.3, and so $(A_1 \oplus A_2, Q_1 \oplus Q_2)$ cannot be a D-pair. $\square$

We conclude the first section with the following statement, whose proof will be omitted.

Proposition 1.3.5.3. *I-pairs, D-pairs and I-D-pairs are closed under shifting. If (A, Q) is an I-pair (D-pair, I-D-pair) and, for some $h \in A$, Q^* is an h-shift of Q* (cf. Definition 1.3.1.2) *then (A, Q^*) is again an I-pair (D-pair, I-D-pair).*

2. Applications

2.1. *Squodds, coloured graphs and Steiner Triple Systems*

Since this account is intended to appear in the present Volume, Steiner Triple Systems are bound to crop up. We shall indeed find that squodds lead to STSs, and vice versa, although in nowhere the precise manner is which Ganter and Werner use the various algebras in their paper [3] to coordinate these combinatorial structures. We shall therefore not present the reader with any of those bijections between definitions, by which these authors illustrate their elegant results – in the present case, it would smack of pretence. Anyway. . .

Proposition 2.1.1. (1) *Given a squodd $Q(\cdot)$ on a set X of order v, there is at least one way to derive from it a Steiner Triple System B on the $v+2$ marks $\langle X \cup \langle\infty_1, \infty_2\rangle\rangle$, where $\infty_1, \infty_2 \notin X$ are two additional marks.*

(2) *Given a Steiner Triple System (B) on a set Y, and a Flag – that is, a triple $(b_0; b_1, b_2) \in B$ in which b_0 is marked – there is at least one way to obtain from it a squodd $Q(\cdot)$ on $Y \backslash (b_1, b_2)$, whose idempotent is b_0.*

Proof. (α) Use the elements $(\omega, x, y, \ldots)$ of X to label, firstly, the vertices of the complete graph $G \sim K_v$ of order v, and secondly a Store of v colours. For each $y, z \in X$, $y \neq z$, we now colour the edge (y, z) of G with the colour x if $y \cdot z = x$ in Q, *and* if x is different from both y and z. Note that no two edges of the same colour can have a vertex in common, since if both (p, q) and (q, r) were to be coloured s, this would mean $q \cdot s = p$ and $q \cdot s = r$. This leaves uncoloured only the edges (x, x^2), $x \neq \omega$, and constitutes the first coloration, or F-coloration, of the edges of G. It is readily seen that the uncoloured edges form a two-factor of $G \backslash \omega$; that is, every vertex of $G \backslash \omega$ is the endpoint of 2 such edges. This two-factor, forming the main part of the diagonal graph of $Q(\cdot)$ – except that this time its vertices are labelled by single elements of X^* instead of *pairs* as in 1.2 – is made up of one or more cycles – closed simple polygons – each of some *even* order, by condition (iii) in Definition 1.1.1.

(β) The edges of even cycles being 2-colourable, that is, one may colour them in 2 different colours without edges of a given colour having a vertex in common, we now take two more colours, ∞_1 and ∞_2, and colour the edges in each cycle alternately ∞_1 and ∞_2. In doing this, it should be noted, we have one arbitrary choice when two-colouring the edges of each cycle. Call this the second coloration, or S-coloration, of the edges of G. Now we adjoin two vertices, ∞_1 and ∞_2. If (x, y) has been coloured ∞_i, we then connect x to the vertex ∞_i by an edge coloured y, and y by one coloured x. Finally, we connect ω and ∞_1 by an edge coloured ∞_2, and to ∞_2 by an edge coloured ∞_1, and ∞_1 and ∞_2 by an edge coloured ω. Thus we have obtained a partition of the edges of the complete graph on $X \cup \langle \infty_1, \infty_2 \rangle$ into triangles, each edge being coloured with the label of the opposite vertex, which partition is obviously a Steiner Triple System on $X \cup \langle \infty_1, \infty_2 \rangle$, and this concludes the proof of (1).

(γ) Conversely, if B is a Steiner Triple System on a set Y of order w, we label the vertices of a graph $H \simeq K_w$ by the elements of Y, and for each $(x, y, z) \in B$ we colour each edge of the triangle (x, y, z) by a colour bearing the label of the opposite vertex. If $b_1, b_2 \in Y$, let $(b_0, b_1, b_2) \in B$, that is, let b_0 be the third vertex of the corresponding triangle. Removing vertices b_1, b_2 and deleting all the edges through them from H, we are left with a complete graph $G \sim K_{w-2}$, in which the edges coloured b_1 form a 1-factor of $G \backslash b_0$, and so do the edges coloured b_2. This is an S-coloration of the edges of G. We note that these two 1-factors (which we might as well uncolour, obtaining an F-coloration of G) form together a two-factor of $G \backslash b_0$, consisting of one or more cycles of even length.

(δ) We now construct a squodd $Q(\cdot)$ on $Y - \langle b_1, b_2 \rangle$. If $(x, y, z) \in B \backslash (b_0, b_1, b_2)$, set $x \cdot y = z$; set $b_0 \cdot b_0 = b_0$. Next, *orient* each cycle in the two-factor in one of the two possible ways, and note that this again gives us one arbitrary choice per cycle. If an edge in this orientation has been directed from x to y, set $x \cdot x = y$. Now the totally symmetric mapping from $(Y - \langle b_1, b_2 \rangle) \times (Y - \langle b_1, b_2 \rangle)$ onto $Y - \langle b_1, b_2 \rangle$ has been defined for the whole domain, and we have a squodd. $\square$

Remark 2.1.2. Apart from the fact that the resulting G-graph depends on the choice Flag in B – or pair of elements b_1, b_2 in Y – the arbitrary choices in (β) and (δ) above are enough indication that there cannot be much connection between the structures of STSs and those of squodds obtained from them as described.

There are, up to isomorphism, two STSs of order 13; one, the cyclical one, has a larger group of automorphisms, of order 39. The other one has only a group of order 6, isomorphic to S_3. Its 78 possible flags give rise to no less than 17 classes of s-coloured G-graphs, and thus to a larger number of non-isomorphic squodds (from some of which one may obtain the first, cyclical STS of order 13). It is reasonable to assume that as the order increases, squodds proliferate still more quickly than STSs, which gives us some excuse not to go further into the question of their structure. So far, the only claim to the title of Variety in the algebraic sense that squodds have, is closure under Direct Sum operations (Proposition 1.2.4), but they certainly form a "variety" in the colloquial sense.

Corollary 2.1.3. *Squodds exist of any finite order prime to* 6.

Remark 2.1.4. The converse contribution of directly constructed squodds, say from Proposition 1.3.2 (Derivation) and 1.2.4 (Direct Sum) is rather modest, because of the absence of a direct construction for prime orders $p \equiv 3 (\mathrm{mod}\ 8)$.

2.2. *D-pairs and packings* (*or*: *Denniston Large Systems*)

For $(v, 6) = 1$, let us imagine $v + 2$ points in space, no 4 in the same plane, forming $v(v + 1)(v + 2)/6$ triangles, v through each edge. If we can use v colours to colour all these triangles so that no two triangles of the same colour have an edge in common, then on labelling the $v + 2$ points, or vertices with different marks, each pair of marks will appear just once as an edge of a triangle of a given colour, and the triads of vertices of this family of triangles will form an STS. Thus such a colouring achieves a partition of all the triads of marks into v disjoint STSs, or a Large Triple System on the $v + 2$ marks.

In particular, the set of labels may consist of the v elements of an abelian group A and of two more marks, $\infty_1, \infty_2 \notin A$. If, in this case, the set of triangles of a given colour is derived from any other such set by adding a fixed $h \in A^*$ to each vertex label other than ∞_1 or ∞_2, we speak of a Denniston Large System, or a Packing (with the aid of A) or an A-Packing.

Proposition 2.2.1. *Given an abelian group A on a set X of order v, $(v, 6) = 1$, and an A-Packing $B_0, B_1, \ldots, B_{v-1}$ on $Y =: X \cup \langle \infty_1, \infty_2 \rangle$, the squodd Q_i derived from the flag $(h_i, \infty_1, \infty_2) \in B_i$ as described in Proposition* 2.1.1 *above forms a D-pair (A, Q_i) with A. Conversely, the* STSs *on $X \cup \langle \infty_1, \infty_2 \rangle$ constructed from the squodd Q_i in a D-pair (A, Q_i) as described in Proposition* 2.1.1, *and from all A-shifts of Q_i, form an A-Packing on $X \cup \langle \infty_1, \infty_2 \rangle$.*

Proof. The first condition of Definition 1.3.3, on triples with 3 distinct entries, is satisfied by hypothesis. Also by hypothesis, no pair (x, y) with $(\infty_1, x, y) \in B_i$ can be A-congruent to another pair (x', y') with $(\infty_1, x', y') \in B_i$, and similarly for ∞_2. Thus, after the "orienting" step of stage δ) in the proof of 2.1.1, we may relabel each vertex in the diagonal graph, this time by a pair of marks, the original mark and the following one, and be assured that if (x, y) is congruent in A to (z, u) then $(\infty_1, x, y) \in B_i$ implies $(\infty_2, z, u) \in B_i$; thus adding an edge between (x, y) and (z, u) will not contravene the bipartite character of this graph.

This completes the proof of the direct claim. The proof of the converse is easy and will be omitted. □

The first Large Steiner System, found in 1850 by Kirkman and rediscovered by Cayley, is actually of this type, derived from the (unique) STS on 9 marks by fixing two entries and permuting the other 7 cyclically, one step at a time. The subject began to develop around 1973, with Teirlinck [10] showing how to derive a Large System of order $3w$ from one of order w, by a simple construction ("Triplicating"). Rosa [7], using Latin Squares with no subsquare of order 2, derived Large Systems of order $2w+1$ from given ones of order w ("Duplicating"). Denniston [1], concentrating on prime orders, constructed D-pairs with the cyclical group C_p for $p = 11$, 13, 17, 19, 23, 29, 31, 41, 47, 59, 67, exploiting for the larger values of p either the full multiplicative groups of $\mathbb{Z}_p^*$ or large subgroups M, in the sense that if $\lambda \in M$ and $x \cdot y = z$ in $Q(\cdot)$, $(\lambda x) \cdot (\lambda y) = \lambda z$ as well. Except for $p = 11$, 13 and 29, all of these actually form I-D-pairs. Therefore, with the hindsight of Proposition 1.3.5.2, we now know that just as there exists a Packing of order $31 + 2$ and one of order $67 + 2$ there exists one of order $31 \cdot 67 + 2 = 2079$ as well. (A Large System of this order may be obtained in yet another way: start with Kirkman's result of order 9, and proceed as indicated:

$$9 \xrightarrow{D} 19 \xrightarrow{T} 57 \xrightarrow{D} 115 \xrightarrow{D} 231 \xrightarrow{T} 693 \xrightarrow{T} 2079,$$

where D denotes Rosa's "duplication", and T, Teirlinck's "triplication".) The I-D-pair of Example 1.3.4.1, used in [2] to form a sequence of 13 *resolvable* STSs thus obtaining a Packing of order 15, may of course serve in such Direct Sum operations too. Around the same time, Wilson [11] and others became aware of the results of Proposition 1.3.3.5 above and derived Denniston Large Systems from the I-D-pairs so obtained. Denniston had been unaware of this, and his constructions for C_{23}, C_{31} and C_{47} show again that Derivation is not the unique source of I-D-pairs. The excellent summary of the state of the art up to around 1980 in [8] already mentions the general belief prevailing at the time that Large Systems exist for every feasible order >7; and in a series of papers in 1984, Lu [5, 6] covered nearly all the ground, so at the time of his premature death only six values were left in doubt (which, I am told, have also been settled since then).

2.3. *I-D-pairs and Teirlinck's Second Construction*

Since a computer search has shown that the only two D-pairs with C_{11} are those of Examples 1.3.3.3 and 1.3.3.4, we know from Proposition 1.3.5.2 that the Direct Sum of one of those with an I-D-pair of order v will *not* lead even to a D-pair of order $11v$; thus a Large System of order $11v+2$ cannot be obtained in this way. However, we owe to Teirlinck [10] the following remarkable result taken from [8], which seems a fitting note on which to close this account:

Theorem 2.3.1 (Teirlinck). *Given any Large System of order $u+2$, and an I-D-pair $(A, Q_0(\cdot))$ of order v, there exists a Large System of order $u \cdot v + 2$.*

Proof. Not matter what its structure, we may rename the entries in the triples of the given Large System to be the elements of $Z_u \cup \langle \infty_1, \infty_2 \rangle$ numbering the respective STSs $B_1, B_2, \ldots, B_u$. For simplicity, let $0 \in A$ be the idempotent of $Q_0(\cdot)$, and a_i that of its ith A-shift. Also, let F_1, F_2 be a bi-partition of the diagonal pairs of $Q_0(\cdot)$. We now construct $u \cdot v$ STSs C_{ij} on $V =: (A \times Z_u) \cup \langle \infty_1, \infty_2 \rangle$ as follows:

For each $a_i \in A$ and $j \in Z_u$, $C_{ij} = C_{ij}^{(1)} \cup C_{ij}^{(2)} \cup C_{ij}^{(3)}$, consisting of the following triples on V:

$$\begin{aligned}
C_{ij}^{(1)} = {} & \langle \infty_1, \infty_2, (a_i, z_j) \rangle \mid ((\infty_1, \infty_2, z_j) \in B_j) \cup \langle ((\infty_k, (a_i, x), (a_i, y)) \rangle \\
& \mid ((\infty_k, x, y) \in B_j) \cup \langle ((a_i, x), (a_i, y), (a_i, z)) \rangle \mid ((x, y, z) \in B_j), \ k = 1, 2; \\
C_{ij}^{(2)} = {} & \langle \infty_k, (a_i + b, x), (a_i + b \cdot b, x) \rangle \mid (b \in A^*, x \in Z_u, (b, b \cdot b) \in F_k, \ k = 1, 2)) \\
& \cup \langle ((a_i + b, x), (a_i + b, y), (a_i + b \cdot b, (x+y)/2 + j)) \rangle \\
& \mid (b \in A^*, \ x, y \in Z_u, \ y \neq x); \\
C_{ij}^{(3)} = {} & \langle (a_i + b, x), (a_i + c, y), (a_i + b \cdot c, (x + y + j)) \rangle \\
& \mid (x, y \in Z_u, \ b \neq c \neq b \cdot c \neq b \in A^*),
\end{aligned}$$

where in $C_{ij}^{(3)}$, each triple of $Q_0(\cdot)$ is taken on *one* fixed order with every pair x, y of Z_u. Notation might perhaps have been shorter if in $C_{ij}^{(2)}$ and $C_{ij}^{(3)}$ we had omitted a_i and taken the dot operation in $Q(\cdot)$ to be read as taking place in Q_i, the ith A-shift of $Q_0(\cdot)$, but with the present one it seems easier to verify that any triple of V actually appears in some C_{ij}. □

It should also be noted that, apart from Proposition 1.3.5.2, this is, so to say, the first instance of I-D-pairs finding "full employment". With I-pairs alone, we could not have the first term in $C_{ij}^{(2)}$, since the partition into two one-factors F_k would not work and $(\infty_k, (a_i + b, x), (a_i + b \cdot b, x))$ would reappear as some $(\infty_k, (c \cdot c, x), (c, x))$; while with D-pairs alone, for a given x and y, we should be meeting again triples from the second term of $C_{ij}^{(2)}$ as $(c, x), (c, y), (c \cdot c, (x+y)/2 + j)$. The reader might wish to verify this with the I-pair $(C_5, \mathrm{Der}(C_5))$, and with the two D-pairs of Examples 1.3.3.3 and 1.3.3.4.

References

[1] R.H.F. Denniston, Some packings with Steiner triple systems, Discrete Math. 9 (1974) 213–227.

[2] R.H.F. Denniston, Sylvester's problem of the 15 schoolgirls, Discrete Math. 9 (1974) 229–233.

[3] B. Ganter and H. Werner, Co-ordinating Steiner Systems, Ann. Discrete Math. 7 (1980) (Topics on Steiner Systems, C.C. Lindner and A. Rosa, eds.) 3–24.

[4] E.S. Kramer and D.M. Mesner, The possible (impossible) systems of 11 disjoint $S(2, 3, 13)$'s ($S(3, 4, 14)$'s) with automorphism of order 11, Utilitas Math. 7 (1975) 55–58.

[5] Jia-Xi Lu, On large sets of disjoint Steiner triple systems, I, II, III, J. Combin. Theory (A) 34 (1983) 140–146, 147–155, 156–182.

[6] Jia-Xi Lu, On large sets of disjoint Steiner triple systems, IV, V, VI, J. Combin. Theory (A) 37 (1984) 136–163, 164–188, 189–192.

[7] A. Rosa, A theorem on the maximum number of disjoint Steiner systems, J. Combin. Theory (1) 18 (1975) 305–312.

[8] A. Rosa, Intersection properties of Steiner systems, Ann. Discrete Math. 7 (1980) 115–128.

[9] L. Teirlinck, On the maximum number of disjoint Steiner Triple Systems, Discrete Math. 6 (1973) 299–300.

[10] L. Teirlinck, Combinatorial Structures, Thesis, Vrije Universiteit Brussel, Dept. voor Wiskunde, 1976.

[11] R.M. Wilson, Some partition of all triples into Steiner triple systems, Hypergraph Seminar, Ohio State Univ. 1972, Lecture Notes in Math. 411 (Springer, Berlin, 1974) 267–277.

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 299–305
North-Holland

PARTITIONING SETS OF QUADRUPLES INTO DESIGNS I

Martin J. SHARRY and Anne PENFOLD STREET
Dept. of Mathematics, University of Queensland, St. Lucia, Queensland 4067, Australia, and Dept. of Mathematics, University of Canterbury, Christchurch 1, New Zealand

To Professor Haim Hanani on his seventy-fifth birthday.

All of the non-isomorphic ways of partitioning the collection of all the quadruples chosen from a set of eight elements into five disjoint 2-(8, 4, 3) designs are determined.

1. Introduction

Many versions of the following question have been considered in combinatorics: how may a specified family of subsets, chosen from a given set, be partitioned in some "nice" way? Recent work on this topic includes, for instance, that of Harms et al. [1], Hartman [2], Kramer et al. [3], Teirlinck [8] and the authors [7].

A *t-design* based on a set, X, of v elements is a collection of k-subsets (blocks) chosen from X in such a way that each unordered t-subset of X occurs in precisely λ of the blocks. Such a design has parameters t-(v, k, λ). Two t-(v, k, λ) designs based on the same set X are said to be *disjoint* if and only if they have no block in common. If the set of all the $\binom{v}{k}$ k-subsets chosen from X can be partitioned into mutually disjoint t-(v, k, λ) designs, then these designs are said to form a *large set*. Here we partition the set of all $\binom{8}{4}$ 4-subsets (quadruples) of the set $X = \{1, 2, \ldots, 8\}$ and prove the following result.

Theorem. *The set of all the quadruples chosen from an* 8*-set can be partitioned into a large set of* 2-(8, 4, 3) *designs in precisely* 26 *non-isomorphic ways.*

The large sets are given in *Table 3*. An *automorphism of a large set* is a permutation of the elements of the underlying v-set which preserves the partition of the collection of blocks into designs. The full automorphism groups of the large sets, and the types of the designs occurring in each, are given in *Table 4*.

2. The designs

There are four isomorphism classes of 2-(8, 4, 3) designs, as determined by Nandi [6]. We refer to them as Q, R, S, T, according to whether they contain 7,

0012-365X/89/$3.50

Table 1. 2-(8, 4, 3) designs of types Q, R, S, T.
(*Note*: *Type* Q is also a 3-(8, 4, 1) design.)

q :	1234 1256 1278 1357 1368 1458 1467 2358 2367 2457 2468 3456 3478 5678
r :	1234 1235 1267 1368 1456 1478 1578 2378 2457 2468 2568 3458 3467 3567
s :	1234 1235 1267 1368 1456 1478 1578 2378 2458 2467 2568 3457 3468 3567
t :	1234 1235 1267 1368 1457 1468 1578 2378 2458 2467 2568 3456 3478 3567

Table 2. Automorphism groups, and their orbits, for the designs given in Table 1.

Design	Group order	Group generators	Orbits
q	1344	(56)(78), (34)(78), (12)(78), (57)(68), (23)(67), (34)(56)	1, 2, 3, 4, 5, 6, 7, 8
r	48	(23)(78), (12)(67), (45), (27)(38)	1, 2, 3, 6, 7, 8; 4, 5
s	12	(23)(78), (28)(37), (156)(387)	1, 5, 6; 2, 3, 7, 8; 4
t	21	(1273685), (123)(678)	1, 2, 3, 5, 6, 7, 8; 4

3, 1, 0 paris of complementary blocks respectively. Q is a 3-(8, 4, 1) design. *Table 1* lists designs of each type; *Table 2* gives the full automorphism groups of designs q, r, s, t, of types Q, R, S, T respectively.

If we take the seven blocks of q which contain i, and delete i from each of them, the remaining seven triples form a 2-(7, 3, 1) design for each $i = 1, 2, \ldots, 8$. This is the ***derived design*** with respect to i. The same procedure applied to r gives 2-(7, 3, 1) designs for two values of i, namely $i = 4$ and $i = 5$. Applied to s, or to t, it gives a 2-(7, 3, 1) design only for $i = 4$.

3. The partitions

Suppose that the $\binom{8}{4}$ quadruples chosen from $X = \{1, 2, \ldots, 8\}$ are partitioned into a large set of 2-(8, 4, 3) designs. If two of these 2-(8, 4, 3) designs are of type Q, then, for at least one value of i, the derived designs include three disjoint 2-(7, 3, 1) designs on the same 7-set. This is impossible (see [4]) so at most one design of type Q can occur in a large set.

Suppose that a large set does contain one design of type Q. Backtrack search shows that the remaining four designs in the large set must all be of type S, and that these large sets have automorphism groups of orders 3, 4, or 12. Further, if we fix the design of type Q to be q, as given in *Table 1*, then we find 896 such large sets, of which 112 have a group of order 12, 336 have a group of order 4, and 448 have a group of order 3. On the other hand, if we fix one of the designs of type S to be s, as given in Table *1*, then we find 32 such large sets, of which 4 have a group of order 12, 12 have a group of order 4, and 16 have group of order 3. These numbers provide a cross-check in the following way.

Using an isomorphism testing program of McKay [5], and direct computation

Table 3. The 26 non-isomorphic partitions of $\binom{8}{4}$ quadruples into 5×2-$(8,4,3)$ designs.

1 : 1234 1256 1278 1357 1368 1458 1467 2358 2367 2457 2468 3456 3478 5678
1235 1236 1247 1348 1456 1578 1678 2378 2458 2467 2568 3457 3468 3567
1237 1245 1268 1346 1358 1478 1567 2345 2368 2478 2567 3467 3578 4568
1238 1248 1267 1347 1356 1457 1568 2346 2357 2456 2578 3458 3678 4678
1246 1257 1258 1345 1367 1378 1468 2347 2348 2356 2678 3568 4567 4578

2 : 1234 1256 1278 1357 1368 1458 1467 2358 2367 2457 2468 3456 3478 5678
1235 1236 1247 1348 1456 1578 1678 2378 2458 2467 2568 3457 3468 3567
1237 1245 1268 1346 1358 1478 1567 2348 2357 2456 2678 3467 3568 4578
1238 1258 1267 1347 1356 1457 1468 2345 2346 2478 2567 3578 3678 4568
1246 1248 1257 1345 1367 1378 1568 2347 2356 2368 2578 3458 4567 4678

3 : 1234 1256 1278 1357 1368 1458 1467 2358 2367 2457 2468 3456 3478 5678
1235 1236 1247 1348 1456 1578 1678 2378 2458 2467 2568 3457 3468 3567
1237 1246 1258 1345 1378 1468 1567 2345 2368 2478 2567 3467 3568 4578
1238 1248 1267 1347 1356 1457 1568 2346 2357 2456 2578 3458 3678 4678
1245 1257 1268 1346 1358 1367 1478 2347 2348 2356 2678 3578 4567 4568

4 : 1234 1235 1267 1368 1456 1478 1578 2378 2457 2468 2568 3458 3467 3567
1236 1245 1248 1347 1358 1567 1678 2357 2368 2467 2578 3456 3478 4568
1237 1246 1258 1348 1367 1457 1568 2345 2356 2478 2678 3468 3578 4567
1238 1256 1278 1345 1357 1467 1468 2346 2347 2458 2567 3568 3678 4578
1247 1257 1268 1346 1356 1378 1458 2348 2358 2367 2456 3457 4678 5678

5 : 1234 1235 1267 1368 1456 1478 1578 2378 2457 2468 2568 3458 3467 3567
1236 1245 1248 1347 1358 1567 1678 2357 2368 2467 2578 3456 3478 4568
1237 1246 1278 1348 1356 1457 1568 2346 2358 2458 2567 3457 3678 4678
1238 1257 1268 1345 1367 1458 1467 2347 2356 2456 2478 3468 3578 5678
1247 1256 1258 1346 1357 1378 1468 2345 2348 2367 2678 3568 4567 4578

6 : 1234 1235 1267 1368 1456 1478 1578 2378 2457 2468 2568 3458 3467 3567
1236 1245 1248 1347 1358 1567 1678 2357 2368 2467 2578 3456 3478 4568
1237 1257 1268 1348 1356 1458 1467 2346 2358 2456 2478 3457 3678 5678
1238 1246 1278 1345 1367 1457 1568 2347 2356 2458 2567 3468 3578 4678
1247 1256 1258 1346 1357 1378 1468 2345 2348 2367 2678 3568 4567 4578

7 : 1234 1235 1267 1368 1456 1478 1578 2378 2457 2468 2568 3458 3467 3567
1236 1245 1248 1347 1378 1567 1568 2357 2358 2467 2678 3456 3468 4578
1237 1257 1268 1346 1358 1458 1467 2348 2356 2456 2478 3457 3678 5678
1238 1247 1256 1345 1357 1468 1678 2346 2367 2458 2578 3478 3568 4567
1246 1258 1278 1348 1356 1367 1457 2345 2347 2368 2567 3578 4568 4678

8 : 1234 1235 1267 1368 1456 1478 1578 2378 2457 2468 2568 3458 3467 3567
1236 1245 1248 1347 1378 1567 1568 2357 2358 2467 2678 3456 3468 4578
1237 1257 1268 1346 1358 1458 1467 2348 2356 2456 2478 3457 3678 5678
1238 1256 1278 1345 1367 1457 1468 2346 2347 2458 2567 3568 3578 4678
1246 1247 1258 1348 1356 1357 1678 2345 2367 2368 2578 3478 4567 4568

9 : 1234 1235 1267 1368 1456 1478 1578 2378 2457 2468 2568 3458 3467 3567
1236 1245 1248 1357 1358 1467 1678 2347 2368 2567 2578 3456 3478 4568
1237 1256 1258 1348 1367 1457 1468 2345 2346 2478 2678 3568 3578 4567
1238 1246 1278 1345 1347 1567 1568 2356 2357 2458 2467 3468 3678 4578
1247 1257 1268 1346 1356 1378 1458 2348 2358 2367 2456 3457 4678 5678

10 : 1234 1235 1267 1368 1456 1478 1578 2378 2457 2468 2568 3458 3467 3567
1236 1245 1248 1357 1358 1467 1678 2347 2368 2567 2578 3456 3478 4568
1237 1256 1278 1348 1356 1457 1468 2346 2358 2458 2467 3457 3678 5678
1238 1246 1257 1347 1367 1458 1568 2345 2356 2478 2678 3468 3578 4567
1247 1258 1268 1345 1346 1378 1567 2348 2357 2367 2456 3568 4578 4678

Table 3 (continued).

11 :	1234	1235	1267	1368	1456	1478	1578	2378	2457	2468	2568	3458	3467	3567
	1236	1245	1248	1357	1358	1467	1678	2347	2368	2567	2578	3456	3478	4568
	1237	1256	1278	1348	1356	1457	1468	2346	2358	2458	2467	3457	3678	5678
	1238	1257	1268	1346	1347	1458	1567	2345	2367	2456	2478	3568	3578	4678
	1246	1247	1258	1345	1367	1378	1568	2348	2356	2357	2678	3468	4567	4578
12 :	1234	1235	1267	1368	1456	1478	1578	2378	2457	2468	2568	3458	3467	3567
	1236	1245	1248	1357	1378	1467	1568	2347	2358	2567	2678	3456	3468	4578
	1237	1246	1258	1348	1356	1457	1678	2348	2356	2467	2578	3457	3678	4568
	1238	1257	1268	1346	1347	1458	1567	2345	2367	2456	2478	3568	3578	4678
	1247	1256	1278	1345	1358	1367	1468	2346	2357	2368	2458	3478	4567	5678
13 :	1234	1235	1267	1368	1456	1478	1578	2378	2457	2468	2568	3458	3467	3567
	1236	1245	1248	1357	1378	1467	1568	2347	2358	2567	2678	3456	3468	4578
	1237	1247	1268	1346	1358	1458	1567	2348	2356	2456	2578	3457	3678	4678
	1238	1256	1278	1345	1367	1457	1468	2346	2357	2458	2467	3478	3568	5678
	1246	1257	1258	1347	1348	1356	1678	2345	2367	2368	2478	3578	4567	4568
14 :	1234	1235	1267	1368	1456	1478	1578	2378	2457	2468	2568	3458	3467	3567
	1236	1245	1278	1347	1348	1567	1568	2357	2368	2458	2467	3456	3578	4678
	1237	1246	1258	1346	1358	1457	1678	2348	2356	2478	2567	3457	3678	4568
	1238	1247	1268	1356	1357	1458	1467	2345	2367	2456	2578	3468	3478	5678
	1248	1256	1257	1345	1367	1378	1468	2346	2347	2358	2678	3568	4567	4578
15 :	1234	1235	1267	1368	1456	1478	1578	2378	2458	2467	2568	3457	3468	3567
	1236	1237	1245	1348	1457	1568	1678	2358	2468	2478	2567	3456	3467	3578
	1238	1247	1258	1346	1357	1468	1567	2347	2356	2456	2678	3458	3678	4578
	1246	1257	1268	1347	1356	1378	1458	2345	2348	2367	2578	3568	4567	4678
	1248	1256	1278	1345	1358	1367	1467	2346	2357	2368	2457	3478	4568	5678
16 :	1234	1235	1267	1368	1456	1478	1578	2378	2458	2467	2568	3457	3468	3567
	1236	1237	1245	1348	1457	1568	1678	2358	2468	2478	2567	3456	3467	3578
	1238	1247	1258	1347	1356	1468	1567	2346	2357	2456	2678	3458	3678	4578
	1246	1257	1268	1345	1367	1378	1458	2347	2348	2356	2578	3568	4567	4678
	1248	1256	1278	1346	1357	1358	1467	2345	2367	2368	2457	3478	4568	5678
17 :	1234	1235	1267	1368	1456	1478	1578	2378	2458	2467	2568	3457	3468	3567
	1236	1237	1248	1358	1457	1467	1568	2345	2468	2567	2578	3456	3478	3678
	1238	1246	1257	1347	1356	1458	1678	2348	2356	2457	2678	3467	3578	4568
	1245	1268	1278	1346	1348	1357	1567	2347	2358	2367	2456	3568	4578	4678
	1247	1256	1258	1345	1367	1378	1468	2346	2357	2368	2478	3458	4567	5678
18 :	1234	1235	1267	1368	1456	1478	1578	2378	2458	2467	2568	3457	3468	3567
	1236	1237	1248	1358	1457	1467	1568	2345	2468	2567	2578	3456	3478	3678
	1238	1247	1256	1346	1357	1458	1678	2348	2356	2457	2678	3467	3578	4568
	1245	1257	1268	1347	1356	1378	1468	2346	2358	2367	2478	3458	4567	5678
	1246	1258	1278	1345	1348	1367	1567	2347	2357	2368	2456	3568	4578	4678
19 :	1234	1235	1267	1368	1456	1478	1578	2378	2458	2467	2568	3457	3468	3567
	1236	1237	1248	1358	1457	1467	1568	2345	2468	2567	2578	3456	3478	3678
	1238	1247	1256	1346	1357	1458	1678	2348	2357	2456	2678	3467	3568	4578
	1245	1268	1278	1347	1348	1356	1567	2346	2358	2367	2457	3578	4568	4678
	1246	1257	1258	1345	1367	1378	1468	2347	2356	2368	2478	3458	4567	5678
20 :	1234	1235	1267	1368	1456	1478	1578	2378	2458	2467	2568	3457	3468	3567
	1236	1237	1248	1358	1457	1467	1568	2345	2468	2567	2578	3456	3478	3678
	1238	1247	1256	1346	1357	1458	1678	2357	2368	2456	2478	3458	3467	5678
	1245	1268	1278	1347	1348	1356	1567	2346	2358	2367	2457	3578	4568	4678
	1246	1257	1258	1345	1367	1378	1468	2347	2348	2356	2678	3568	4567	4578

Table 3 (continued).

21 :	1234	1235	1267	1368	1456	1478	1578	2378	2458	2467	2568	3457	3468	3567
	1236	1237	1248	1358	1457	1468	1567	2345	2456	2578	2678	3467	3478	3568
	1238	1245	1278	1347	1356	1467	1568	2346	2357	2468	2567	3458	3678	4578
	1246	1257	1258	1345	1348	1367	1678	2347	2356	2368	2478	3578	4567	4568
	1247	1256	1268	1346	1357	1378	1458	2348	2358	2367	2457	3456	4678	5678
22 :	1234	1235	1267	1368	1456	1478	1578	2378	2458	2467	2568	3457	3468	3567
	1236	1237	1248	1358	1457	1468	1567	2345	2456	2578	2678	3467	3478	3568
	1238	1256	1278	1346	1357	1458	1467	2347	2356	2457	2468	3458	3678	5678
	1245	1257	1268	1347	1348	1356	1678	2346	2358	2367	2478	3578	4567	4568
	1246	1247	1258	1345	1367	1378	1568	2348	2357	2368	2567	3456	4578	4678
23 :	1234	1235	1267	1368	1456	1478	1578	2378	2458	2467	2568	3457	3468	3567
	1236	1245	1247	1357	1378	1468	1568	2348	2356	2578	2678	3458	3467	4567
	1237	1258	1268	1346	1348	1457	1567	2345	2367	2456	2478	3568	3578	4678
	1238	1246	1257	1347	1356	1458	1678	2347	2358	2468	2567	3456	3678	4578
	1248	1256	1278	1345	1358	1367	1467	2346	2357	2368	2457	3478	4568	5678
24 :	1234	1235	1267	1368	1456	1478	1578	2378	2458	2467	2568	3457	3468	3567
	1236	1245	1248	1357	1358	1467	1678	2347	2368	2567	2578	3456	3478	4568
	1237	1246	1278	1345	1348	1567	1568	2356	2358	2457	2468	3467	3678	4578
	1238	1256	1257	1347	1367	1458	1468	2345	2346	2478	2678	3568	3578	4567
	1247	1258	1268	1346	1356	1378	1457	2348	2357	2367	2456	3458	4678	5678
25 :	1234	1235	1267	1368	1456	1478	1578	2378	2458	2467	2568	3457	3468	3567
	1236	1245	1257	1347	1348	1568	1678	2358	2367	2468	2478	3456	3578	4567
	1237	1246	1258	1356	1378	1457	1468	2348	2356	2457	2678	3458	3467	5678
	1238	1247	1268	1345	1367	1458	1567	2346	2357	2456	2578	3478	3568	4678
	1248	1256	1278	1346	1357	1358	1467	2345	2347	2368	2567	3678	4568	4578
26 :	1234	1235	1267	1368	1457	1468	1578	2378	2458	2467	2568	3456	3478	3567
	1236	1245	1248	1358	1378	1467	1567	2347	2356	2578	2678	3457	3468	4568
	1237	1258	1268	1345	1367	1456	1478	2346	2348	2457	2567	3568	3578	4678
	1238	1247	1256	1346	1357	1458	1678	2357	2368	2456	2478	3458	3467	5678
	1246	1257	1278	1347	1348	1356	1568	2345	2358	2367	2468	3678	4567	4578

of permutations acting on large sets, we find that any two large sets containing a type Q design and four designs of type S are isomorphic if they have automorphism groups of the same order.

Using the information on automorphism groups of design given in *Table 2,* we see that there are $8!/1344 = 30$ distinct designs of type Q, $8!/48 = 840$ of type R, $8!/12 = 3360$ of type S and $8!/21 = 1920$ of type T. Similarly there are $8!/12$, $8!/4$ and $8!/3$ distinct large sets, with groups of orders 12, 4 3 respectively.

Consider a large set, with group of order 3. A particular design of type Q must occur in $(8!/3)/(8!/1344) = 448$ large sets of this type, and a particular design of type S in $((8!/3) \times 4)/(8!/12) = 16$ large sets of this type. This agrees with the results of the backtrack search.

The remaining results have been cross-checked by similar arguments.

The 26 classes of large sets are listed in *Table 3,* and further information on their properties in *Table 4.* In several cases, large sets with the same groups are not isomorphic to each other; for instance, there are nine non-isomorphic large sets with trivial automorphism group, seven with group of order three, four with

Table 4. Automorphism groups, and design types, of the partitions listed in *Table 3*.

Partition Number	Group Order	Group Generators	Design Types
1	4	(1683)(2475)	Q, $4S$
2	3	(156)(347)	Q, $4S$
3	12	(14)(23)(58)(67), (276)(458)	Q, $4S$
4	1	(1)	$2R$, $2S$, T
5	2	(16)(38)(45)	R, $4S$
6	2	(16)(35)(47)	$3R$, $2S$
7	6	(12)(38)(47), (162)(457)	$3R$, $2S$
8	2	(16)(38)(45)	R, $4S$
9	3	(123)(678)	$2R$, $3T$
10	3	(127)(456)	$3R$, $2T$
11	1	(1)	R, $2S$, $2T$
12	6	(273)(485), (16)(23)(58)	$3R$, $2S$
13	10	(37854), (16)(34)(57)	$5R$
14	2	(27)(38)(45)	R, $4S$
15	1	(1)	$4S$, T
16	1	(1)	$4S$, T
17	1	(1)	$3S$, $2T$
18	3	(165)(287)	$2S$, $3T$
19	1	(1)	$2S$, $3T$
20	1	(1)	$2S$, $3T$
21	1	(1)	$4S$, T
22	1	(1)	$3S$, $2T$
23	3	(165)(378)	$2S$, $3T$
24	3	(127)(456)	$3S$, $2T$
25	3	(186)(234)	$3S$, $2T$
26	5	(18564)	$5T$

group of order two, and two with (non-abelian) group of order six. There are two large sets with all designs of the same type, one with all type R, the other with all type T. The remaining large sets contain either three different types (two R, two S, one T, or one R, two S, two T), or a mixture of types R and S (in six different ways), types R and T (in two different ways) or types S and T (in eleven different ways).

Acknowledgements

Computation was carried out on a Pyramid 9810 (Department of Mathematics, University of Queensland) and a Sum 3/160 (Department of Mathematics, University of Canterbury). The work was sponsored by the Australian Research Grants Scheme. The second author was a Visiting Erskine Fellow at the University of Canterbury while the work was carried out.

References

[1] J.J. Harms, C.J. Colbourn and A.V. Ivanov, A census of (9, 3, 3) block designs without repeated blocks, Congressus Numerantium 57 (1987) 147–170.

[2] A. Hartman, Halving the complete design, Annals of Discrete Mathematics 34 (1987) 207–224.

[3] E.S. Kramer, D.L. Kreher, S.S. Magliveras and D.M. Mesner, Coherent Room rectangles from permutation groups, Ars Combinatoria 9 (1980) 101–111.

[4] R. Mathon, K.T. Phelps and A. Rosa, Small Steiner triple systems and their properties, Ars Combinatoria 15 (1983) 3–110.

[5] B.D. McKay, *nauty* User's Guide (Version 1.2), Australian National University Computer Science Technical Report TR-CS-87-03 (1987).

[6] H.K. Nandi, A further note on the non-isomorphic solutions of incomplete block designs, Sankhyā Ser. 7 (1945) 313–316.

[7] M.J. Sharry and A. Penfold Street, Partitioning sets of triples into designs, Ars Combinatoria 26B (1988) 51–66.

[8] L. Teirlinck, On large sets of disjoint quadruple systems, Ars Combinatoria 17 (1984) 173–176.

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 307–316
North-Holland

INFINITE FAMILIES OF STRICTLY CYCLIC STEINER QUADRUPLE SYSTEMS*

Helmut SIEMON
Sonnenrain 17, D-8701 Reichenberg, FRG

Dedicated to Haim Hanani on the occasion of his 75th birthday.

1. Introduction

A Steiner Quadruple System SQS(v) of order v is a pair (V, B) where V is a set with $v \in \mathbb{N}^*$ elements, B a subset of $\binom{V}{4}$ the elements of which are called blocks so that every 3-subset of V is contained in a unique block. H. Hanani [1] proved that the necessary condition $v \equiv 2, 4(6)$ for the existence of a SQS(v) is also sufficient. In papers by A. Hartman [2, 3] and Lenz [5] Hanani's proof was simplified. If, however, we require a SQS(v) to allow a given automorphism group the problem of the existence of SQS(v) is not yet solved completely, even if the automorphism group is cyclic of order v. A SQS(v) with a cyclic automorphism group C_v of order v is called cyclic, denoted CSQS(v). If the stabilizer of any quadruple of a CSQS(v) equals the identity (the orbits of C_v have all length v) we speak of a strictly cyclic SQS(v), denoting them sSQS(v). In [7] we constructed among other things sSQS($2 \cdot 5^\alpha$). In this paper we will extend our construction to sSQS($2p^\alpha$), $p \equiv 5(12)$ provided sSQS($2p$) exists containing the base quadruples $\{0, i, 2i, \frac{v}{2} + i\}$, $i = 1, 2, \ldots, (v-2)/4$ and all orbits invariant under the mapping $i \to -i \pmod v$.

To the list of recent papers which deal with cyclic Steiner Quadruple Systems (cf. [7]) we have to add the dissertation by Piotrowski [6], who proved, in the main part of his work, the following theorems:

(i) *A* SQS(v) *with dihedral group* D_v *of order* $2v$ *as automorphism group exists iff* $v \equiv 0(2)$, $v \not\equiv 0(3)$, $v \not\equiv 0(8)$, $v \geq 4$ *and if for any prime divisor* p *of* v *there exists a* SQS($2p$) *with* D_{2p} *as automorphism group.*

(ii) *For all prime numbers* $p \equiv 1(4)$ *and* $p \leq 229$, *or* $p \equiv 1(4)$ *and* $p \not\equiv 1, 49(60)$ *and* $p < 15000$ *there exists* SQS($2p$) *with the automorphism group* $A_v = \{(x \to ax + b \mid a, b \in Z_v$ *and* $\gcd(a, v) = 1\}$. *In case* $p \not\equiv 1(3)$ *this* SQS($2p$) *has* D_{2p} *as an automorphism group.*

The systems constructed in (i), (ii) are, according to a private communication from W. Piotrowski, all strictly cyclic for $v \not\equiv 0$ (4). However, the construction we offer in case $v = 2p^\alpha, p$ prime number and $p \equiv 5(12)$ is a direct continuation of our

* This investigation was presented at the 5th International Conference on Geometry, Haifa 1987.

0012-365X/89/$3.50

previous paper [7] and can be achieved, relatively easy, by using orbits graphs rather than the relevant graphs themselves as in Piotrowski's dissertation. Furthermore a modification of our construction might prove helpful in settling the existence problem for sSQS($2p$).

We use the definitions and results of [7][1] and observe that in order to determine a 1-factor of the graph $\mathrm{O\bar{G}S_2}(2p^\alpha)$ we have only to consider vertices which are neither admissible nor co-admissible[2] and which we call residual vertices (residual orbits). Let $\mathrm{RO}(2p^\alpha)$ be the set of all residual orbits and $\mathrm{RO\bar{G}S_2}(2p^\alpha)$ the corresponding subgraph of $\mathrm{O\bar{G}S_2}(2p^\alpha)$. We map $\mathrm{RO\bar{G}S_2}(2p^\alpha)$ by means of a natural homomorphism ψ^* onto $\mathrm{OGS_2}(2p)$. The fibres of ψ^* have all cardinality $p^{\alpha-1}$. Now if $\{B_1, B_2\}$ is an edge of $\mathrm{OGS_2}(2p)$ and $\mathfrak{F}(B_1)$, $\mathfrak{F}(B_2)$ are fibres of ψ^*, the elements of which are mapped onto B_1 resp. B_2, we can construct a bijection Φ: $\mathfrak{F}(\mathrm{B}_1) \to \mathfrak{F}(\mathrm{B}_2)$ so that for any $D \in \mathfrak{F}(B_1)$ the set $\{D, \Phi(D)\}$ is an edge of $\mathrm{RO\bar{G}S_2}(2p^\alpha)$. In case $\mathrm{OGS_2}(2p)$ has a 1-factor and if $\{B_1, B_2\}$ is an edge of a one factor, then $\{D, \Phi(D)\}$ is an edge of a 1-factor of $\mathrm{RO\bar{G}S_2}(2p^\alpha)$.

2. Definitions and preliminary results

Let $V = \{0, 1, \ldots, v-1\}$ be a set of cardinality v, $v \equiv 2$, $10(24)$, $v > 4$. A set $\{x, y, z\}$, x, y, $z \in V^*$ $(=V \setminus \{0\})$ with $x + y + z = v$ is called a difference triple. We conceive of x, y, z as smallest remainders modulo v. If $x \leq y \leq z$, we use $[x, y, z]$ instead of $\{x, y, z\}$. The difference triples of the form $[x, x, z]$ or $[x, y, y]$ or $[x, y, v/2]$ are uniquely completed as difference quadruples

$$\left\{x, x, \frac{v}{2} - x, \frac{v}{2} - x\right\}, \qquad \left\{\frac{v}{2} - y, \frac{v}{2} - y, y, y\right\}, \qquad \{x, x, y, y\}$$

respectively, which give rise to the base quadruples $\{0, i, 2i, v/2 + i\}$, $i = 1, 2, \ldots, (v-2)/4$.

Next we consider difference triples $[x, y, z]$ with $x < y < x$ and $z \neq v/2$. Let S be the set of all these difference triples. We define derivatives of $[x, y, z]$ as follows:

$$\begin{aligned} &\text{First derivative } [x, y, z]' := \{y, x + y, z - y\} \\ &\text{Second derivative } [x, y, z]'' := \{x, x + y, z - x\} \qquad (2.1) \\ &\text{Third derivative } [x, y, z]''' := \{y - x, x, z + x\}. \end{aligned}$$

For the geometric meaning of (2.1) see [7].

We define the following relation on S:

(R) For all difference triples Δ_1, Δ_2: $\Delta_1 R \Delta_2 \Leftrightarrow \Delta_2 = \Delta_1'$ or $\Delta_2 = \Delta_1''$ or $\Delta_2 = \Delta_1'''$.

[1] For definitions and preliminary results see also Section 2.
[2] See Section 3.1.

Using the relation R we define the following graph $\mathrm{GS}(v)$:

$$\begin{array}{l}\text{Vertices: elements of } S\\ \text{Edges: } \{\Delta_1, \Delta_2\} \text{ is an edge iff } \Delta_1 R \Delta_2.\end{array} \tag{2.2}$$

Proposition 2.1 ([4], [7]). *If* $\mathrm{GS}(v)$ *has a* 1*-factor then there exists a* $\mathrm{sSQS}(v)$.

$\mathrm{GS}(v)$ can be decomposed into two subgraphs $\mathrm{GS}_1(v)$, $\mathrm{GS}_2(v)$, which are not connected:

$$\begin{array}{ll}\mathrm{GS}_1(v)\colon & \begin{array}{l}\text{vertices: } [x, y, z] \quad \text{if } 2\nmid x \quad \text{or} \quad 2\nmid y \quad \text{or} \quad 2\nmid z\\ \text{edges defined as in } \mathrm{GS}(v)\end{array}\\ \\ \mathrm{GS}_2(v)\colon & \begin{array}{l}\text{vertices: } [x, y, z] \quad \text{if } 2 \mid x, y, z\\ \text{edges defined as in } \mathrm{GS}(v).\end{array}\end{array} \tag{2.3}$$

Let S_1 resp. S_2 be the sets of vertices of $\mathrm{GS}_1(v)$ resp. $\mathrm{GS}_2(v)$.

Proposition 2.2 ([4], [7]). $\mathrm{GS}(v)$ *has a* 1*-factor iff* $\mathrm{GS}_1(v)$ *and* $\mathrm{GS}_2(v)$ *both have a* 1*-factor.*

Proposition 2.3 ([7]). $\mathrm{GS}_1(v)$ *has a* 1*-factor.*

We investigate $\mathrm{GS}_2(v)$. If U is a subgroup of the automorphism group of $\mathrm{GS}_2(v)$ so that all orbits of U have equal length we define an orbit graph $\mathrm{OGS}_2(v)$:

$$\begin{array}{ll}\text{Vertices:} & \text{the orbits of } U\\ \text{Edges}\ \ : & \text{orbits } \mathrm{O}_1, \mathrm{O}_2 \text{ form an edge } \{\mathrm{O}_1, \mathrm{O}_2\} \text{ iff}\\ & \text{there exists } \Delta_1 \in \mathrm{O}_1,\ \Delta_2 \in \mathrm{O}_2 \text{ with } \Delta_1 R \Delta_2.\end{array} \tag{OG}$$

Proposition 2.4 ([7]). *If* $\mathrm{OGS}_2(v)$ *has a* 1*-factor, so has* $\mathrm{GS}_2(v)$.

If $m \in \mathbb{N}^*$ is relatively prime to v we define the following operation on the elements of S_2:

$$m[x, y, z] = \begin{cases}\{mx, my, mz\}, & \text{if } mx + my + mz = v\\ \{v - mx, v - my, v - mz\}, & \text{if } mx + my + mz = 2v\end{cases} \tag{2.4}$$

The mapping $\delta\colon [x, y, z] \to m[x, y, z]$ is an automorphism of $\mathrm{GS}_2(v)$.

Let $v = 2p^\alpha$, p prime number $\equiv 1$ or $5 \bmod 12$. We decompose the graph $\mathrm{GS}_2(2p^\alpha)$ into subgraphs, which are not connected:

$$\bar{\mathrm{G}}\mathrm{S}_2(2p^\alpha)\colon \begin{cases}\text{vertices: } [x, y, z], & \text{if } p \nmid x \quad \text{or} \quad p \nmid y \quad \text{or} \quad p \nmid z\\ \text{edges defined as in } \mathrm{GS}_2(2p^\alpha)\end{cases}$$

$$\underset{\sim}{\mathrm{G}}\mathrm{S}_2(2p^{\alpha-1})\colon \begin{cases}\text{vertices: } [x, y, z], & \text{if } p \mid x, y, z\\ \text{edges defined as in } \mathrm{GS}_2(2p^\alpha)\end{cases}$$

The graph $\underset{\sim}{\mathrm{G}}\mathrm{S}_2(2p^{\alpha-1})$ is isomorphic to $\mathrm{GS}_2(2p^{\alpha-1})$ (cf. [7]).

Proposition 2.5 ([7]). $GS_2(2p^{\alpha}) = \underset{\smile}{G}S_2(2p^{\alpha-1}) \cup \bar{G}S_2(2p^{\alpha})$.

When we know that $\bar{G}S_2(2p^{\alpha})$ has a 1-factor for all $\alpha \in \mathbb{N}^*$ we can use mathematical induction by means of Proposition 2.5 to prove that $GS_2(2p^{\alpha})$ has a 1-factor.

3. 1-factor of $\bar{G}S_2(2p^{\alpha})$

We let the unit group $E(2p^{\alpha})$, $p \equiv 5(12)$, operate on the vertices of $GS_2(2p^{\alpha})$. There are $t = (p^{\alpha} + p^{\alpha-1} - 6)/6$ orbits of length $(p^{\alpha-1}(p-1))/2$ (cf. [7], Lemma 4.4). Let $O_1, O_2, \ldots, O_t$ be the t orbits. If O_i contains $[x, y, z]$ with

$$2p \mid x \quad \text{or} \quad 2p \mid y \quad \text{or} \quad 2p \mid z \tag{2.5}$$

(observe that only one component is divisible by $2p$) then all triples in O_i have property (2.5). We call O_i admissible if all $[x, y, z] \in O_i$ have property (2.5). Let $A_1, \ldots, A_r$ be the admissible orbits and $B_1, B_2, \ldots, B_s$ the not admissible ones. When we replace $2 \cdot 5^n$ by $2p^{\alpha}$ in Theorem 1, [7] we obtain $r = \frac{1}{2}(p^{\alpha-1} - 1)$, $s = \frac{1}{3}(p^{\alpha} - 2p^{\alpha-1} - 3)/2$ and $r \leqslant s$ with equality only for $p = 5$. Let now $OGS_2(2p^{\alpha})$ be the orbit graph as defined in (OG) (with $E(2p^{\alpha})$ generating the orbits). In the following we will construct a 1-factor of $O\bar{G}S_2(2p^{\alpha})$.

3.1. *Admissible and co-admissible orbits*[3]

Let A_i be an admissible orbit. In A_i there exist vertices $\Delta_1 = [x_1, y_1, z_1]$, $\Delta_2 = [x_2, y_2, z_2]$, $\Delta_3 = [x_3, y_3, z_3]$ of $\bar{G}S_2(2p^{\alpha})$ with $x_1 \equiv 0(2p)$, $y_2 \equiv 0(2p)$, $z_3 \equiv 0(2p)$. Δ_1' cannot be contained in an admissible orbit because none of its components $y_1, y_1 + x_1, 2p^{\alpha} - (2y_1 + x_1)$ are divisible by $2p$. So Δ_1' must be contained in an orbit B_i which is not admissible. Then for all Δ, $\Delta = [x, y, z] \in A_i$ with $x \equiv 0(2p)$ one of the vertices Δ', Δ'', Δ''' must lie in B_i because of the automorphism property. Now $\Delta'' = \{x, x + y, 2p^{\alpha} - (2x + y)\}$, $\Delta''' = \{y - x, x, 2p^{\alpha} - y\}$ are in admissible orbits and $\Delta' = \{y, x + y, 2p - (2y + x)\}$ is not, so $\Delta' \in B_i$. By the same arguments one gets Δ_2'', $\Delta_3''' \in B_i$.

Let $\mathfrak{A}$ be the set of all admissible orbits. So the relation k given by

$$(k) \qquad [x, y, z]' \in k(A), \quad \text{if } [x, y, z] \in A \in \mathfrak{A}, \quad x \equiv 0(2p)$$

is a well-defined mapping from $\mathfrak{A}$ into the set of all not admissible orbits. We define $\mathfrak{B} := \{k(A) \mid A \in \mathfrak{A}\}$. When A is admissible let us call $k(A)$ co-admissible. So $\mathfrak{B}$ is the set of all co-admissible orbits. We show next:

$$k \text{ is an injective mapping from } \mathfrak{A} \text{ into } \mathfrak{B}. \tag{3.1}$$

(a) If $A \in \mathfrak{A}$, $B \in \mathfrak{B}$, $[x, y, z] \in A$, $x \equiv 0(2p)$, $[x, y, z]' \in B$ then no vertex other than $[x, y, z]$, connected with $[x, y, z]'$, is contained in an admissible orbit.

[3] For the convenience of the reader we repeat here the argument of the proof of Theorem 1 in [7] with $2p^{\alpha}$ instead of $2 \cdot 5^n$.

The vertices connected with $[x, y, z]'$ are $[x, y, z]$ and at the most two of the following:

$$\{x+y, x+2y, 2p-(2x+3y)\}, \{2p-(x+y), 2p-(x+2y), 2x+3y-2p)\}$$

$$\{y, x+2y, 2p-(x+3y)\}, \{2p-y, 2p-(x+2y), x+3y-2p\}.$$

None of these have components divisible by $2p$.

(b) Assume now $A_1, A_2 \in \mathfrak{A}$, $k(A_1)=k(A_2)$. In A_1 there exists $[x_1, y_1, z_1]$ with $x_1 \equiv 0(2p)$, $y_1 \not\equiv 0(2p)$ and $[x_1, y_1, z_1]' \in k(A_1)$. Since $k(A_1)=k(A_2)$ there exists $[x_2, y_2, z_2]$ in A_2 so that $[x_1, y_1, z_1]'$ is connected with $[x_2, y_2, z_2]$. From (a) we know that $[x_2, y_2, z_2]=[x_1, y_1, z_1]$ and hence $A_1=A_2$.

The edges $\{A, k(A)\}$ of $\mathrm{O\bar{G}S}_2(2p^\alpha)$ will be candidates for the elements of a 1-factor.

3.2. *The residual orbits*

If $p>5$, $p\equiv 5(12)$, there are $(p^{\alpha-1}(p-5))/6$ $(=(p^\alpha+p^{\alpha-1}-6)/6-2\frac{1}{2}(p^{\alpha-1}-1))$ orbits which are neither admissible nor co-admissible. We call these orbits of $\mathrm{O\bar{G}S}_2(2p^\alpha)$ *residual orbits*. Let $\mathrm{RO}(2p^\alpha)$ be the set of all residual orbits. The vertices of $\mathrm{O\bar{G}S}_2(2p^\alpha)$ are then given by $\mathfrak{A}\cup\mathfrak{B}\cup\mathrm{RO}(2p^\alpha)$ where the sets $\mathfrak{A}$, $\mathfrak{B}$, $\mathrm{RO}(2p^\alpha)$ are mutually disjoint. We now define the residual orbit graph $\mathrm{RO\bar{G}S}_2(2p^\alpha)$ as follows:

$$\mathrm{RO\bar{G}S}_2(2p^\alpha)\colon \begin{cases}\text{vertices: elements of } \mathrm{RO}(2p^\alpha)\\ \text{edges defined as in } \mathrm{O\bar{G}S}_2(2p^\alpha)\end{cases}.$$

In this section we will show that $\mathrm{RO\bar{G}S}_2(2p^\alpha)$ has a 1-factor, provided $\mathrm{OGS}_2(2p)$ has one.

In order to prepare the proof of this assertion we will first give a representation of the orbits of $\mathrm{\bar{G}S}_2(2p^\alpha)$ (note: $\mathrm{\bar{G}S}_2(2p)=\mathrm{GS}_2(2p)$).

3.2.1. *The representation of orbits*

In any orbit of $\mathrm{\bar{G}S}_2(2p^\alpha)$ there are exactly three vertices of $\mathrm{\bar{G}S}_2(2p^\alpha)$ with the first component $x=2$. To prove this, we have only to repeat the argument (i), Theorem 1, [7]. In the following it will be shown that the edges of $\mathrm{O\bar{G}S}_2(2p^\alpha)$, which are incident with a vertex O, can be obtained by using the second and third derivatives of the three elements $[2, y_1, z_1]$, $[2, y_2, z_2]$, $[2, y_3, z_3]\in \mathrm{O}$. These triples we therefore call *representing triples of the orbit.*

It is convenient to consider the components $x/2$, $y/2$, $z/2$ with $x/2+y/2+z/2=p^\alpha$ instead of x, y, z with $x+y+z=2p^\alpha$, because $x/2$, $y/2$, $z/2$ are relatively prime to p and thus there are inverse elements ξ_1, ξ_2, ξ_3 with $x/2\cdot\xi_1\equiv 1\,(p^\alpha)$ etc[4]. For this reason we define $[a, b, c]_r := [2a, 2b, 2c]$, $\{a, b, c\}_r := \{2a, 2b, 2c\}$. The index r shall remind of "reduced form".

[4] This device was first introduced in [4]. We will however adopt it to our needs.

Now

$$m[a,b,c]_r = m[2a,2b,2c]$$
$$= \begin{cases} \{m2a,\ m2b,\ m2c\}, & \text{if } m2a+m2b+m2c=2p^\alpha \\ \{2p^\alpha - m2a,\ 2p^\alpha - m2b,\ 2p^\alpha - m2c\}, & \text{if } m2a+m2b+m2c=4p^\alpha \end{cases}$$
$$= \begin{cases} \{ma,\ mb,\ mc\}_r, & \text{if } ma+mb+mc=p^\alpha \\ \{p^\alpha - ma,\ p^\alpha - mb,\ p^\alpha - mc\}_r, & \text{if } ma+mb+mc=2p^\alpha. \end{cases}$$

Especially we remark: If $ma=1$ or $mb=1$ or $mc=1$ then $ma+mb+mc \neq 2p^\alpha$. Now if the triple $\Delta = \{1, w, -(1+w)\}_r$ is an element of the orbit O, then we obtain the two other representing triples in reduced form as

$$\begin{aligned} &\frac{1}{w}[1, w, -(1+w)]_r = \left\{1, -\frac{1+w}{w}, \frac{1}{w}\right\}_r, \\ &-\frac{1}{1+w}[1, w, -(1+w)]_r = \left\{1, -\frac{w}{1+w}, -\frac{1}{1+w}\right\}_r. \end{aligned} \tag{3.2}$$

Let us call $\{1, y+1, z-1\}_r$, $\{1, y-1, z+1\}_r$ the *neighbours* of $[1, y, z]_r$. The neighbours of $[1, y, z]_r$ can be obtained by taking the second and third derivatives of $[1, y, z]_r$ in case $y<z$: $[1, y, z]_r'' = [2, 2y, 2z]'' = \{2, 2y+2, 2z-2\} = \{1, y+1, z-1\}_r$, $[1, y, z]_r''' = \{1, y-1, z+1\}_r$. We obtain the same neighbours (in reverse order) in case $z<y$: $[1, z, y]_r'' = \{1, z+1, y-1\}_r$, $[1, z, y]_r''' = \{1, z-1, y+1\}_r$.

We prove:

The orbit O containing $\{1, w, -(1+w)\}_r$, $\left\{1, -\frac{1+w}{w}, \frac{1}{w}\right\}_r$, $\left\{1, -\frac{w}{1+w}, -\frac{1}{1+w}\right\}_r$ can at most be connected by an edge with the following orbits C_1, C_2, C_3:

$$\begin{aligned} &\{1, 1+w, -(2+w)\}_r, \left\{1, -\frac{1+w}{2+w}, \frac{1}{2+w}\right\}_r, \left\{1, -\frac{2+w}{1+w}, \frac{1}{1+w}\right\}_r \in C_1 \\ &\{1, w-1, -w\}_r, \left\{1, -\frac{w-1}{w}, -\frac{1}{w}\right\}_r, \left\{1, -\frac{w}{w-1}, \frac{1}{w-1}\right\}_r \in C_2 \\ &\left\{1, \frac{w}{1+w}, -\frac{1+2w}{1+w}\right\}_r, \left\{1, -\frac{w}{1+2w}, -\frac{1+w}{1+2w}\right\}_r, \left\{1, -\frac{1+2w}{w}, \frac{1+w}{w}\right\}_r \in C_3. \end{aligned} \tag{3.3}$$

Proof. The set of neighbours of $\{1, y, z\}_r$ will be denoted by $n(1, y, z)$.

(i) $n(1, w, -(1+w)) = \{\{1, w+1, -(2+w)\}_r, \{1, w-1, -w\}_r\}$

$$n\left(1, -\frac{1+w}{w}, \frac{1}{w}\right) = \left\{\left\{1, -\frac{1}{w}, -\frac{w+1}{w}\right\}_r, \left\{1, -\frac{1+2w}{w}, \frac{1+w}{w}\right\}_r\right\}$$
$$n\left(1, -\frac{w}{1+w}, -\frac{1}{1+w}\right) = \left\{\left\{1, \frac{1}{1+w}, -\frac{2+w}{1+w}\right\}_r, \left\{1, -\frac{1+2w}{1+w}, \frac{w}{1+w}\right\}_r\right\}.$$

We can state that all neighbours of the representing triples of O are contained in either C_1 or C_2 or C_3. A neighbour may not be a vertex of the graph: $[1,7,9]_r$ is a vertex of $GS_2(2\cdot 17)$, but the neighbour $[1,8,8]_r$ is not. Here no orbit exists which contains $[1,7,9]_r''$. In this case $[1,7,9]_r'''$ exists.

(ii) Let $[x, y, z]_r \in O$. We will show now that $[x, y, z]_r'$, $[x, y, z]_r''$, $[x, y, z]_r'''$ are contained in C_1 or C_2 or C_3, if at all.

We obtain

$$\frac{1}{x}[x, y, z]_r = \left[1, \frac{y}{x}, -\frac{x+y}{x}\right]_r.$$

Take $w := y/x$. It follows that $-(1+w) = -(x+y)/x$. Now $[x, y, z]_r$, $\{1, w, -(1+w)\}_r'$ belong to O. Consider $[x, y, -(x+y)]_r' = \{y, x+y, -(2y+1)\}_r$. We have

$$\frac{1}{y}[x, y, -(x+y)]_r' = \left\{1, \frac{1+w}{w}, -\frac{1+2w}{w}\right\}_r$$

and know that $[x, y, -(x+y)]_r'$ is contained in the same orbit as

$$\left\{1, \frac{1+w}{w}, -\frac{1+2w}{w}\right\}_r,$$

hence follows $[x, y, -(x+y)]_r' \in C_3$. All other cases, namely

$$\frac{y}{x} = -(1+w), \qquad -\frac{1+w}{w}, \qquad \frac{1}{w}, \qquad -\frac{w}{1+w}, \qquad -\frac{1}{1+w}$$

can be treated accordingly. Considering $[x, y, z]_r''$, $[x, y, z]_r'''$, we proceed likewise.

Now (3.3) shows that the edges of the graph $RO\bar{G}S_2(2p^\alpha)$ are determined by neighbours of the representing triples (reduced form).

Corollary. *If $\{B_1, B_2\}$ is an edge of $O\bar{G}S_2(2p^\alpha)$, there are two of the representing triples of B_1 which have neighbours in B_2.*

3.2.2 *The fibres of ψ^**

Let $[X, Y, Z]$ be a vertex of $\bar{G}S_2(2p^\alpha)$ and $x \equiv X(2p)$, $y \equiv Y(2p)$, $z \equiv Z(2p)$ with $0 < x, y, z < 2p$. We define

$$[X, Y, Z]^\psi = \begin{cases} \{x, y, z\}, & \text{if } x+y+z = 2p \\ \{2p-x, 2p-y, 2p-z\}, & \text{if } x+y+z = 4p. \end{cases}$$

Only if $[X, Y, Z]$ is contained in an admissible (co-admissible) orbit, then $[X, Y, Z]^\psi = [a, b, c]$ yields $a = 0$ or $b = 0$ or $c = 0$ ($a = b$ or $a = c$ or $b = c$). So it follows that the union of all residual orbits is equal to the set of all pre-images of the set of vertices of $\bar{G}S_2(2p)$. Next we observe with O a vertex of $RO\bar{G}S_2(2p^\alpha)$:

> If $[X_1, Y_1, Z_1]$, $[X_2, Y_2, Z_2] \in O$ then
> $[X_1, Y_1, Z_1]^\psi$ and $[X_2, Y_2, Z_2]^\psi$ belong to the same orbit when (3.4)
> the unit group $E(2p)$ is operating on $GS_2(2p)$.

The remark (3.4) is obvious.

Let $\overline{[x, y, z]}$ be the orbit $[x, y, z]$ is contained in. Now ψ induces by (3.4) a mapping ψ^* from $\mathrm{RO\bar{G}S}_2(2p^\alpha)$ onto $\mathrm{OGS}_2(2p)$ in a natural way:

$$(\psi^*) \qquad \overline{[X, Y, Z]}^{\psi^*} = W \Leftrightarrow [X, Y, Z]^\psi \in W.$$

And we remark that ψ^* is a homomorphism from $\mathrm{RO\bar{G}S}_2(2p^\alpha)$ onto $\mathrm{OGS}_2(2p)$, which is readily seen.

Next we wish to prove that the fibres $\mathfrak{F}(B) = \{C \mid C \in \mathrm{RO}(2p^\alpha) \text{ and } C^{\psi^*} = B\}$ for all vertices B of $\mathrm{OSG}_2(2p)$ have cardinality $p^{\alpha-1}$.

For this reason we need the following

Lemma. *With* $[\![s]\!] := [s] + 1$, *s real, we obtain*:

(1) *If x is a natural number which satisfies the condition* $1 \leq x \leq p - 3$ *then*

$$\left[\!\!\left[\frac{p^\alpha - (x+3)}{2p}\right]\!\!\right] = \frac{p^{\alpha-1} + 1}{2}$$

(2) *If x is a natural number with* $p \leq x + 3 \leq 2p - 3$ *then*

$$\left[\!\!\left[\frac{p^\alpha - (x+3)}{2p}\right]\!\!\right] = \frac{p^{\alpha-1} - 1}{2}.$$

The proof of this Lemma is straightforward.

Proposition 3.1. *Let B be any vertex of* $\mathrm{OGS}_2(2p)$, $\mathfrak{F}(B)$ *a fibre of* ψ^*, *then* $|\mathfrak{F}(B)| = p^{\alpha-1}$.

Proof. Let $[2, y_1, z_1]$, $[2, y_2, z_2]$, $[2, y_3, z_3]$ be the representing triples of the orbit B. We determine now the pre-images of the triples under the mapping ψ.

For y_i, z_i, $i = 1, 2, 3$ the following inequalities hold;

$$4 \leq y_1 \leq p - 3, \qquad p + 1 \leq z_i \leq 2(p-3). \tag{3.5}$$

When $[2, Y, Z]$ is mapped onto $[2, y_i, z_i]$ by ψ the component Y has the form $Y = y_i + k_i 2p$ or $Y = z_i + t_i 2p$; $k_i, t_i \in \mathbb{N}^*$, $i = 1, 2, 3$. Because of $4 \leq Y \leq p^\alpha - 3$ we have to find maximal numbers $\bar{k}_1, \bar{k}_2, \bar{k}_3, \bar{t}_1, \bar{t}_2, \bar{t}_3$ with

$$y_i + (\bar{k}_i - 1)2p \leq p^\alpha - 3, \quad 4 \leq y_i \leq p - 3 \tag{3.6}$$

and $\qquad i = 1,2,3$

$$z_i + (\bar{t}_i - 1)2p \leq p^\alpha - 3, \quad p + 1 \leq z_i \leq 2(p-3). \tag{3.7}$$

Applying the Lemma we obtain

$$\bar{k}_i = \left[\!\!\left[\frac{p^\alpha - (y_i+3)}{2p}\right]\!\!\right] = \frac{p^{\alpha-1} + 1}{2}$$

$$\bar{t}_i = \left[\!\!\left[\frac{p^\alpha - (z_i+3)}{2p}\right]\!\!\right] = \frac{p^{\alpha-1} - 1}{2}$$

so that $\bar{k}_1+\bar{k}_2+\bar{k}_3+\bar{l}_1+\bar{l}_2+\bar{l}_3=3\cdot p^{\alpha-1}$. Since any orbit contains three triples $[x, y, z]$ with $x=2$ we have $p^{\alpha-1}$ orbits being mapped by ψ^* onto B. □

Theorem 3.1. *If the orbits B_1, B_2 consisting of vertices of* $\mathrm{GS}_2(2p)$ *form an edge of* $\mathrm{OGS}_2(2p)$ *then there is a bijective function Φ: $\mathfrak{F}(B_1)\to\mathfrak{F}(B_2)$ so that for all $D\in\mathfrak{h}(B_1)$ the set $\{D, \Phi(D)\}$ is an edge of* $\mathrm{RO\bar{G}S}_2(2p^\alpha)$.

Proof. (i) Let B_1 be represented by $\{1, y_i, z_i\}_r$ and B_2 by $\{1, u_i, w_i\}_r$, $i=1, 2, 3$. Since we have assumed B_1, B_2 to be connected there are, according to the corollary of (3.3), two neighbours of elements of B_1 contained in B_2. Without loss of generality we can choose $u_1=y_1+1$, $u_2=y_2+1$ otherwise we would only alter the notation. Now u_3, w_3 can be expressed by y_3 and z_3. Since the representing triples of B_1 resp. B_2 can be written as

$$\{1, y_1, -(1+y_1)\}_r,\quad \left\{1, -\frac{y_1}{1+y_1}, -\frac{1}{1+y_1}\right\}_r,\quad \left\{1, -\frac{1+y_1}{y_1}, \frac{1}{y_1}\right\}_r$$

resp. as

$$\{1, y_1+1, -(2+y_1)\}_r,\quad \left\{1, \frac{1}{y_1+1}, -\frac{2+y_1}{y_1+1}\right\}_r,\quad \left\{1, -\frac{1+y_1}{2+y_1}, -\frac{1}{2+y_1}\right\}_r$$

with

$$y_2:=\frac{y_1}{1+y_1},\quad y_3:=-\frac{1+y_1}{y_1},\quad u_2:=\frac{1}{y_1+1},\quad u_3:=\frac{1+y_1}{2+y_1}$$

and by eliminating the parameter y_1 we obtain

$$u_3=-\frac{y_3}{1+2y_3}\quad\text{and}\quad w_3=-\frac{z_3}{1+2z_3}.$$

So B_2 can be represented by

$$\{1, y_1+1, z_1-1\}_r,\quad \{1, y_2+1, z_2-1\}_r,\quad \left\{1, -\frac{y_3}{1+2y_3}, -\frac{z_3}{1+2z_3}\right\}_r.$$

(ii) If $\overline{\{1, Y, Z\}_r}$ is a vertex of $\mathrm{RO\bar{G}S}_2(2p^\alpha)$ with $\overline{\{1, Y, Z\}}_r^{\psi^*}=\overline{\{1, y_1, z_1\}_r}$ and $\{1, y_l, z_l\}_r\in\overline{\{1, y_1, z_1\}_r}$, $l=1, 2, 3$ then the following six possibilities $Y\equiv y_l(p)$, $Y\equiv z_l(p)$, $l=1, 2, 3$ have to be considered. Accordingly we define Φ: $\mathfrak{F}(\mathrm{B}_1)+\mathfrak{F}(\mathrm{B}_2)$ by

$$(\Phi)\quad \Phi(\overline{\{1, Y, Z\}_r})=\begin{cases}\overline{\{1, Y+1, Z-1\}_r}, & \text{if } Y\equiv y_1(p) \text{ or } Y\equiv y_2(p)\\ \overline{\{1, Y-1, Z+1\}_r}, & \text{if } Y\equiv z_1(p) \text{ or } Y\equiv z_2(p)\\ \overline{\left\{1, -\frac{Y}{1+2Y}, -\frac{Z}{1+2Z}\right\}_r}, & \text{if } Y\equiv y_3(p) \text{ or } Y\equiv z_3(p).\end{cases}$$

From (i) it follows immediately that $(\Phi(\overline{\{1, Y, Z\}_r}))^{\psi^*}=B_2$ and that $\{\overline{\{1, Y, Z\}_r},$

$\Phi(\{\overline{1, Y, Z}\}_r)\}$ is an edge. Next we observe that Φ is surjective and hence, because of Propositions 3.1, bijective. □

Theorem 3.2. *If the graph* $\mathrm{OGS}_2(2p)$ *has a 1-factor then* $\mathrm{O\bar{G}S}_2(2p^{\alpha})$ *has one.*

Proof. Let $\mathrm{OGS}_2(2p)$ have a 1-factor. In the beginning of this section we have mentioned that the set of vertices of $\mathrm{O\bar{G}S}_2(2p^{\alpha})$ can be decomposed by $\mathfrak{A} \cup \mathfrak{B} \cup \mathrm{RO}(2p^{\alpha})$. From Section 3.1 we know that $\{A, k(A)\}$ for all $A \in \mathfrak{A}$ are candidates for the elements of a 1-factor of $\mathrm{O\bar{G}S}_2(2p^{\alpha})$. Let now $\{B_1, B_2\}$ be an edge of a 1-factor of $\mathrm{OGS}_2(2p)$, then for all $D \in \mathfrak{F}(B_1)$ the set $\{D, \Phi(D)\}$ is an edge of a 1-factor of $\mathrm{RO\bar{G}S}_2(2p^{\alpha})$ and so $\mathrm{RO\bar{G}S}_2(2p^{\alpha})$ and hence $\mathrm{O\bar{G}S}_2(2p^{\alpha})$ have a 1-factor. We deduce $\mathrm{\bar{G}S}_2(2p^{\alpha})$ has a 1-factor (Proposition 2.4). □

Theorem 3.3. *If the graph* $\mathrm{OGS}_2(2p) - (p-5)/6$ *vertices – has a 1-factor then* $\mathrm{sSQS}(2p^{\alpha})$ *exists for all* $\alpha \in \mathbb{N}^*$.

Proof. The theorem follows directly from Theorem 3.2, Proposition 2.4, Proposition 2.5. □

References

[1] H. Hanani, On Quadruple Systems, Can. J. of Math. 12 (1960) 145–147.
[2] A. Hartman, Tripling Quadruple Systems, Ars Combin. 12 (1980) 255–309.
[3] A. Hartman, A general recursive construction for Quadruple Systems, J. Combin. Theory A 33 (1982) 121–134.
[4] E. Köhler, Zyklische Quadrupelsysteme, Abh. Sem. Univ. Hamburg XLVIII (1978) 1–24.
[5] H. Lenz, Tripling Steiner Quadruple Systems, Ars. Combin. 20 (1985), 193–202.
[6] W. Piotrowski, Untersuchungen über S-zyklische Quadrupelsysteme, Diss. Univ. Hamburg 1985, 1–104.
[7] H. Siemon, Some remarks on the construction of cyclic Steiner Quadruple Systems, Arch. der Math. 49 (1987) 166–178.

Discrete Mathematics 77 (1989) 317–321
North-Holland

MINIMAL PAIRWISE BALANCED DESIGNS

R. G. STANTON
Department of Computer Science, University of Manitoba, Winnipeg, Canada, R3T 2N2

An expression involving a "remainder term" is given for the number of blocks in a minimal pairwise balanced design in which the length of the longest block is specified. The allows a simple presentation and unification of a number of earlier results derived by various authors.

1. Introduction

Suppose that we are given a set V made up of v elements $1, 2, 3, \ldots, v$. A *pairwise balanced design* is a collection F of blocks with the property that every pair of elements from V occurs exactly λ times among the blocks of F. In the rest of this paper, we shall restrict attention to the particular case $\lambda = 1$. We shall also introduce the parameter k to designate the length of the longest block in the family F (this block may not be unique; usually, there will be several blocks of length k).

As a simple example, let us look at the case $v = 7$, $k = 4$. There are six non-isomorphic pairwise blanced designs with these parameters, and it is instructive to list them.

(a) Blocks 1234, 1567, 9 pairs; total of 11 blocks.
(b) Blocks 1234, 567, 12 pairs; total of 14 blocks.
(c) Blocks 1234, 156, 257, 367, 6 pairs; total of 10 blocks.
(d) Blocks 1234, 156, 257, 9 pairs; total of 12 blocks.
(e) Blocks 1234, 156, 12 pairs; total of 14 blocks.
(f) Blocks 1234, 15 pairs; total of 16 blocks.

It is clear that the *minimal pairwise balance design* with $v = 7$, $k = 4$, is the design labelled (c).

In general, we use the symbol $g^{(k)}(1, 2; v)$ to designate the minimum cardinality of any pairwise balanced design on a set of v elements with longest block having length k. Thus, we have shown, by exhaustive search, that $g^{(4)}(1, 2; v) = 10$. Of course, the minimal design may not be unique; it is perfectly possible for two non-isomorphic designs to possess the same minimal cardinality.

We shall frequently abbreviate $g^{(k)}(1, 2; v)$ to $g^{(k)}(v)$ or simply, in this paper, to g.

2. Elementary relations

In the minimal design, we let b_i represent the number of blocks of length i, where $i<k$. If $i=k$, we designate one particular block of length k to be the "longest block", and we use b_k to designate the number of *other* blocks of length k. Thus, the total number of blocks of length k is b_k+1. We often refer to the designated "longest block" as the *base block*; it plays a very specialized role in the theory.

By counting blocks, and then by counting appearances of pairs within blocks, we immediately obtain two relations.

$$b_2+b_3+b_4+b_5+\cdots+b_k=g-1 \tag{1}$$

$$\begin{aligned}2b_2+6b_3+12b_4+210b_5+\cdots+k(k-1)b_k&=v(v-1)-k(k-1)\\&=(v-k)(v+k-1).\end{aligned} \tag{2}$$

To obtain a third relation, we define b_{ij} to be the number of blocks of length i that pass through point j on the base block $(j=1,2,3,\ldots,k)$. Since every pair containing j must appear in the set of blocks, we immediately have

$$\Sigma_i(i-1)b_{ij}=v-k, \tag{3}$$

and this result holds for every point j. Hence we may sum over j and obtain

$$\Sigma_i\Sigma_j(i-1)b_{ij}=k(v-k). \tag{4}$$

This summation is over all blocks of length i that meet the base block. However, there may be some blocks of length i that are disjoint from the base block; suppose that the number of these is b_{i0}. Then we may form the sum

$$\Sigma_i(i-1)b_{i0}=E, \tag{5}$$

where the quantity E (for excess) is certainly nonnegative. Since we know that

$$b_i=b_{i0}+b_{i1}+b_{12}+b_{13}+\cdots+b_{ik}, \tag{6}$$

we can add equations **(4)** and **(5)** to end up with

$$b_2+2b_3+3b_4+4b_5+\cdots+(k-1)b_k=k(v-k)+E. \tag{7}$$

We now combine equations **(1)**, **(2)**, and **(7)** in such a way as to eliminate adjacent columns in the equations. For instance, using multipliers 2, 1, −4, would eliminate the terms in b_2 and b_3 to leave

$$2(b_4+3b_5+6b_6+\cdots).$$

We shall multiply the three equations by $s(s+1)$, 1, $-2(s+1)$, respectively, in order to eliminate those terms involving b_{s+1} and b_{s+2}. The resulting expression involves the quantity

$$P=(b_s+b_{s+3})+3(b_{s-1}+b_{s+4})+6(b_{s-2}+b_{s+5})+10(b_{s-3}+b_{s+6})+\cdots \tag{8}$$

It is clear that P is nonnegative.

The result of combining

$$s(s+1)\mathbf{(1)} + \mathbf{(2)} - 2(s+1)\mathbf{(7)}$$

is the relation

$$s(s+1)(g-1) + (v-k)(v+k-1) - 2(s+1)k(v-k) = 2E(s+1) + 2P. \tag{9}$$

If we solve for g from Eq. **(9)**, the result is

$$g = 1 + (v-k)(2sk - v + k + 1)/s(s+1) + 2E/s + 2P/s(s+1), \tag{10}$$

where the quantities E and P are non-negative. If we drop the terms in E and P, we obtain a lower bound that was established by Stinson [5] in 1982, using generalized variance techniques.

Theorem 1 (Stinson). $g \geq 1 + (v-k)(2sk - v + k + 1)/s(s+1)$.

This result is true for all values of s; we can easily determine the most effective value for s by writing $F(s) = 1 + (v-k)(2sk - v + k + 1)/s(s+1)$; then we find

$$F(s) - F(s-1) = 2(v-k)(v-1-sk)/s(s-1)(s+1).$$

This equation shows that $F(s)$ is increasing so long as sk lies below $(v-1)$. Hence, to obtain the strongest result from **(10)**, we should assign to s the value $\lfloor (v-1)/k \rfloor$; of course, if the quantity $(v-1)/k$ should happen to be an integer, then both $F(s)$ and $F(s-1)$ are equal.

Now, let us consider the case of a very long block whose length k lies between $v/2$ and v. For k in this region, we select $s = 1$, and thus obtain a result due to Woodall [6].

Theorem 2 (Woodall). *If k lies between $v/2$ and v, then* $g \geq 1 + (v-k)(3k - v + 1)/2$.

We note that the Woodall bound is always an integer. Consequently, Eq. **(9)** can be applied to give

Corollary 2.1. *The Woodall bound can only be achieved if $E = P = 0$, that is, all blocks meet the long base block, and their lengths are either* 2 *or* 3.

This bound can actually be met by using an easy construction based on 1-factors of the $(v-k)$ points not in the long block; see [4] for details.

However, Eq. **(9)** gives us more information than simply the Woodall bound and its converse. Suppose that we now let k lie between $v/3$ and $v/2$; then we take $s = 2$. (We should remark that special techniques may have to be applied when one is at the exact boundary of this region, that is, where s is changing from 1 to 2 or from 2 to 3.) In this case, the term $2E/s$ in **(9)** becomes E; because E is a non-negative integer, we see that E must be zero if the Stinson bound is met. If we write S for the Stinson bound, and require that it be "met" (that is, $g = \lceil S \rceil$), then we have

$$g = S + 2P/s(s+1) = S + (b_2 + b_5)/3,$$

where the second term is less than unity. Consequently, we have

Theorem 3. *If k lies between $v/3$ and $v/2$, and the Stinson bound is met (in the nearest-integer sense), then $E = 0$, that is, all blocks meet the base block. Furthermore, all of the blocks have lengths 3 or 4, except that there may possibly be one or two rogue blocks (this corresponds to the case $P = 1$ or $P = 2$), and the number of these is given by the relation*

$$\lceil S \rceil - S = (b_2 + b_5)/3.$$

There is curently a great deal of work being done for k lying in this region; see, for example [3], the very important work of Rees in [1] and [2], and the various works cited in [1] and [2]. The use of "frames" (cf. [1]) has been of particular significance in discussing the question.

Actually, Theorem 3 is only a special case of a more general result. Suppose that the Stinson bound is actually met, that is, $g = \lceil S \rceil$. Then we prove, without any restriction on k, that is, for all values of $s \geqslant 2$,

Theorem 4. *The Stinson bound can only be met, that is, $g = \lceil S \rceil$, if all of the blocks meet the long block.*

Proof. We suppose that, if possible, the Stinson bound is met, but that there is a block of length $(s+1) - z$ that does not meet the base block. This block will contribute an amount $(s - z)$ to E; however, it also contributes an amount $z(z+1)/2$ to P. There is a certain balancing effect in action here, since small z values make E large and P small, whereas large z values make P large and E small. More precisely, we may write

$$g = S + 2E/s + 2P/s(s+1),$$

where the contribution of the disjoint block to the "remainder terms" is given by

$$2(s-z)/s + z(z+1)/s(s+1) = \{z^2 - z(2s+1) + 2s(s+1)\}/s(s+1). \tag{11}$$

Now the discrete variable z may range from the value 1, if there is a disjoint block of length s, to the value $(s-1)$, if there is a disjoint block of length 2. The expression **(11)** is decreasing and reaches its minimum value (in the permissible range for z) at $s - 1$; this minimum value is

$$(s^2 + s + 2)/(s^2 + s),$$

and it is greater than unity. Consequently, it is not possible to have $g = \lceil S \rceil$ unless there is no disjoint block, that is, $E = 0$, as stated in Theorem 4.

It is an obvious corollary that, if the Stinson bound is met (that is, $g = \lceil S \rceil$), then

$$g = S + 2P/s(s+1).$$

All blocks have lengths $s + 1$ and $s + 2$, with the exception of a small number that can be determined from the relation

$$\lceil S \rceil - S = 2P/s(s+1),$$

where P is given by **(8)**. This relation guarantees that the number of rogue blocks is very small, and that their lengths are close to those of blocks of lengths $s + 1$ and $s + 2$. □

References

[1] R. Rees, The existence of restricted resolvable designs I: (1,2)-factorizations of K_{2n}, Research Report CORR 87-16, Department of Combinatorics and Optimization, University of Waterloo, 1987.
[2] R. Rees, The existence of restricted resolvable designs II: (1,2)-factorizations of K_{2n+1}, Research Report CORR 87-21, Department of Combinatorics and Optimization, University of Waterloo, 1987.
[3] R.G. Stanton and J.L. Allston, A census of values for $g^{(k)}(1, 2; v)$, Ars Combinatoria **21** (1985) 203-216.
[4] R.G. Stanton, J.L. Allston, and D.D. Cowan, Pair coverings with restricted largest block length, Ars Combinatoria **11** (1981) 85-98.
[5] D.R. Stinson, Applications and generalizations of the variance method in combinatorial designs, Utilitas Mathematica **22** (1982) 323-333.
[6] D.R. Woodall, The λ-μ problem, J. London Mathematical Society **2** (1968) 505-519.

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 323–343
North-Holland

COMBINATORIAL PROBLEMS IN REPEATED MEASUREMENTS DESIGNS

Deborah J. STREET
Waite Agricultural Research Institute, The University of Adelaide, Adelaide, SA, Australia

A number of papers in the statistical literature in recent years have considered the structure of designs with certain desirable statistical properties. Some constructions for these designs have been presented but a number of open problems remains. In this paper a survey of the designs required, and a summary of the known results, is presented.

1. Introduction

In a *repeated measurements design* there are t treatments, n experimental units and the experiment lasts for p periods. Each experimental unit receives one treatment during each period. Thus the design may be represented as a $p \times n$ array containing entries from $\{1, 2, \ldots, t\}$. Some examples are given in *Table 1.*

Table 1.

(a) $t = 3$, $n = 9$, $p = 6$

0	0	0	1	1	1	2	2	2
0	1	2	0	1	2	0	1	2
1	1	1	2	2	2	0	0	0
1	2	0	1	2	0	1	2	0
2	2	2	0	0	0	1	1	1
2	0	1	2	0	1	2	0	1

(b) $t = 6$, $n = 6$, $p = 6$

1	2	3	4	5	6
2	3	4	5	6	1
6	1	2	3	4	5
3	4	5	6	1	2
5	6	1	2	3	4
4	5	6	1	2	3

(c) $t = 5$, $n = 10$, $p = 5$

1	2	3	4	5	1	2	3	4	5
2	3	4	5	1	5	1	2	3	4
5	1	2	3	4	2	3	4	5	1
3	4	5	1	2	4	5	1	2	3
4	5	1	2	3	3	4	5	1	2

The term "repeated measurements design" is also used to describe experiments in which at most one treatment is applied to an experimental unit and successive readings are taken over time. The interest then is in modelling the growth, or change, over time. We will not consider this area further.

As it stands, any $p \times n$ array containing entries from $\{1, 2, \ldots, t\}$ can be used as a design. However, some arrays are better than others and the arrays that are 'best' depend on the model that is being proposed to analyse the results of the experiment and the terms in that model that one is interested in estimating.

We will consider two linear models which have been proposed for analysing results from a repeated measurements experiment. We use $d(k, u)$ to represent the treatment applied, in design d, to unit u during period k.

The first linear model assumes that the observation, Y_{ku}, made on unit u during period k is the sum of a period effect (α_k), a unit effect (β_u), a direct treatment effect ($\tau_{d(k,u)}$), a (first-order) residual treatment effect ($\rho_{d(k-1,u)}$) (for any period other than the first) and an error term (E_{ku}). The observations are assumed to be independent of each other, so $\mathrm{Corr}(E_{ku}, E_{gw}) = 0$ for all pairs $(k, u) \neq (g, w)$. The variance of the error terms is assumed to be constant, so $\mathrm{var}(E_{ku}) = \sigma^2$. Thus we may write this model as

$$Y_{ku} = \alpha_k + \beta_u + \tau_{d(k,u)} + \rho_{d(k-1,u)} + E_{ku},$$
$$k = 1, \ldots, p; \quad u = 1, \ldots, n; \quad \mathrm{Var}(E_{ku}) = \sigma^2; \quad \rho_{d(0,u)} = 0.$$

This model may be varied by assuming that the last period precedes the first (so-called *circular* repeated measurements designs) or by deleting the period effect, or the unit effect, or both.

The second linear model assumes that the observation, Y_{ku}, made on unit u during period k is the sum of a period effect (α_k), a unit effect (β_u), a direct treatment effect ($\tau_{d(k,u)}$) and an error term (E_{ku}). Observations on different units are assumed to be independent but observations on the same unit are assumed to be correlated with the correlation depending on how 'close together' the observations are. We write $\mathrm{Var}(E_{ku}) = \sigma^2/(1-\lambda^2)$ and $\mathrm{Corr}(E_{ku}, E_{gu'}) = \lambda^{|k-g|}\delta_{uu'}$ where $\delta_{uu'}$ is the Kronecker δ. We may write this model as

$$Y_{ku} = \alpha_k + \beta_u + \tau_{d(k,u)} + E_{ku}, \quad k = 1, \ldots, p; \quad u = 1, \ldots, n.$$

To facilitate further discussion of ways of comparing designs, we will express the linear models above in matrix notation.

For the first model, following Cheng and Wu [7], we let

$$\theta = (\tau_1, \ldots, \tau_t, \rho_1, \ldots, \rho_t, \alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_n)^{\mathrm{T}},$$
$$\boldsymbol{Y} = (Y_{11}, Y_{21}, \ldots, Y_{p1}, \ldots, Y_{1n}, Y_{2n}, \ldots, Y_{pn})^{\mathrm{T}},$$
$$\boldsymbol{E} = (E_{11}, E_{21}, \ldots, E_{p1}, \ldots, E_{1n}, \ldots, E_{pn})^{\mathrm{T}}$$

and write $\boldsymbol{Y} = \boldsymbol{X}_d\theta + \boldsymbol{E}$. X_d is a (0, 1) matrix and is called the *design matrix*.

We can write $\boldsymbol{Y} = X_d\theta + \boldsymbol{E} = \eta + \boldsymbol{E}$, say. Our eventual aim is to estimate the elements in θ, but we begin by estimating the elements in η. To do this we have available the data vector $\boldsymbol{Y}$ which differs from η by $\boldsymbol{E}$. Note that $\boldsymbol{Y}, \eta$ and $\boldsymbol{E}$ are all vectors in R^{np}, $\boldsymbol{E}$ has no preferred direction in R^{np} since its elements are independent of each other and have constant variance. Hence the most natural estimate of η is that vector in the range of X_d which is closest to $\boldsymbol{Y}$ in the usual Euclidean sense. Thus our estimate of η, $\hat{\eta}$ say, minimises $(\boldsymbol{Y}-\eta)^{\mathrm{T}}(\boldsymbol{Y}-\eta)$.

Suppose we choose $\boldsymbol{b}$ such that $X_d^{\mathrm{T}}(\boldsymbol{Y} - \boldsymbol{X}_d\boldsymbol{b}) = 0$, that is $X_d^{\mathrm{T}}X_d b = X_d^{\mathrm{T}}\boldsymbol{Y}$. Clearly $X_d\boldsymbol{b}$ is in the range of X_d, $\boldsymbol{Y} - \boldsymbol{X}_d\boldsymbol{b}$ is in the orthogonal complement of the range of X_d and $\boldsymbol{Y} = X_d\boldsymbol{b} + \boldsymbol{Y} - X_d\boldsymbol{b}$. These facts, together with the fact that η is in the range of X_d, give

$$\begin{aligned}(\boldsymbol{Y}-\eta)^{\mathrm{T}}(\boldsymbol{Y}-\eta) &= (\boldsymbol{Y} - X_d\mathbf{b} + X_d\boldsymbol{b} - \eta)^{\mathrm{T}}(\boldsymbol{Y} - X_d\mathbf{b} + X_d\boldsymbol{b} - \eta)\\ &= (\boldsymbol{Y} - \boldsymbol{X}_d\boldsymbol{b})^{\mathrm{T}}(\boldsymbol{Y} - X_d\boldsymbol{b}) + (X_d\boldsymbol{b} - \eta)^{\mathrm{T}}(X_d\boldsymbol{b} - \eta).\end{aligned}$$

Since $(Y - X_d b)^T(Y - X_d \mathbf{b})$ is constant we see that $(Y - \eta)^T(Y - \eta)$ is minimised if $\hat{\eta} = X_d b$. Any vector $\hat{\theta}$ such that

$$X_d\hat{\theta} = \hat{\eta} = X_d b$$

produces the same vector $\hat{\eta}$ and is a least squares estimator of θ. Thus we have

$$X_d^T X_d \hat{\theta} = X_d^T X_d b = X_d^T Y,$$

and

$$\hat{\theta} = (X_d^T X_d)^- X_d^T Y$$

where $(X_d^T X_d)^-$ is the Moore–Penrose generalised inverse of $X_d^T X_d$ (see Searle [23]). $X_d^T X_d$ is called the *information matrix* (of the design d) for estimating θ.

Sometimes not all elements in θ are of equal interest to us. The terms are included in the model for correctness, but we are not interested in estimating, say, the period effect. In a RMD the interest usually centres on estimating the direct treatment effects and/or the residual treatment effects. Hence we want the information matrices for estimating the direct treatment effects and the residual treatment effects. To do this we again consider the equation $X_d^T X_d \hat{\theta} = X_d^T Y$. Let $\gamma = (\tau_1, \ldots, \tau_t, \rho_1, \ldots, \rho_t)^T$, $\delta = (\alpha_1, \ldots, \alpha_p, \beta_1, \ldots, \beta_n)^T$ and write

$$X_d^T X_d \hat{\theta} = X_d^T X_d \begin{bmatrix} \hat{\gamma} \\ \hat{\delta} \end{bmatrix} = \begin{bmatrix} S & T \\ U & V \end{bmatrix} \begin{bmatrix} \hat{\gamma} \\ \hat{\delta} \end{bmatrix} = X_d^T Y = \begin{bmatrix} Z_1 \\ Z_2 \end{bmatrix}, \quad \text{say.}$$

This gives

$$S\hat{\gamma} + T\hat{\delta} = Z_1 \quad \text{and} \quad U\hat{\gamma} + V\hat{\delta} = Z_2.$$

From the second equation we get that $\hat{\delta} = V^-(Z_2 - U\hat{\gamma})$. Substituting we get

$$(S - TV^-U)\hat{\gamma} = Z_1 - TV^-Z_2$$

and $S - TV^-U$ is the information matrix for estimating direct and residual treatment effects simultaneously. Similar results hold for the calculation of the information matrices for estimating either direct or residual treatment effects.

We now define various matrices associated with a RMD so that we can give an explicit expression for the information matrices for estimating direct, and residual, treatment effects. As we are interested in the layout of both the direct and residual effects, the constants are defined in pairs, the first referring to the layout of the τ's, the second to the layout of the ρ's.

Let

h_{is} be the number of times that treatment i occurs in period s,

$\tilde{h}_{i1} = 0$,

$\tilde{h}_{is} = h_{i,s-1}$, $s = 2, \ldots, p$,

n_{iu} be the number of times treatment i occurs on unit u,

$\tilde{n}_{iu}$ be the number of times that treatment i occurs on unit u in the first $p-1$ periods,

m_{ij} be the number of times that treatment i is preceded by treatment j,

$r_i = \sum_u n_{iu}$

and

$\tilde{r}_i = \sum_u \tilde{n}_{iu}$.

We now collect these constants into matrices and let $D = \operatorname{diag}(r_1, \ldots, r_t)$, $\tilde{D} = \operatorname{diag}(\tilde{r}_1, \ldots, \tilde{r}_t)$, $M = (m_{ij})$, $N_p = (h_{is})$, $\tilde{N}_p = (\tilde{h}_{is})$, $N_u = (n_{iu})$, $\tilde{N}_u = (\tilde{n}_{iu})$.

Hence for the first model above

$$X_d^{\mathrm{T}} X_d = \begin{bmatrix} D & M & N_p & N_u \\ M^{\mathrm{T}} & \tilde{D} & \tilde{N}_p & \tilde{N}_u \\ N_p^{\mathrm{T}} & \tilde{N}_p^{\mathrm{T}} & nI_p & J_{p,n} \\ N_u^{\mathrm{T}} & \tilde{N}_u^{\mathrm{T}} & J_{n,p} & pI_n \end{bmatrix},$$

where I_p is the identity matrix of order p and $J_{p,n}$ is the $p \times n$ matrix of 1s. Then the information matrix for estimating direct and residual treatment effects (τ's and ρ's) jointly is

$$\begin{bmatrix} D & M \\ M^{\mathrm{T}} & \tilde{D} \end{bmatrix} - \begin{bmatrix} N_p & N_u \\ \tilde{N}_p & \tilde{N}_u \end{bmatrix} \begin{bmatrix} nI_p & J_{p,n} \\ J_{n,p} & pI_n \end{bmatrix}^{-} \begin{bmatrix} N_p & N_u \\ \tilde{N}_p & \tilde{N}_u \end{bmatrix}^{\mathrm{T}} = \begin{bmatrix} C_{11} & C_{12} \\ C_{21} & C_{22} \end{bmatrix}.$$

Thus we see that

$$C_{11} = D - n^{-1} N_p N_p^{\mathrm{T}} - p^{-1} N_u N_u^{\mathrm{T}} + (np)^{-1} N_u J_{n,n} N_u^{\mathrm{T}},$$

$$C_{12} = C_{21}^{\mathrm{T}} = M - n^{-1} N_p \tilde{N}_p^{\mathrm{T}} - p^{-1} N_u \tilde{N}_u^{\mathrm{T}} + (np)^{-1} N_u J_{n,n} \tilde{N}_u^{\mathrm{T}},$$

and

$$C_{22} = \tilde{D} - n^{-1} \tilde{N}_p \tilde{N}_p^{\mathrm{T}} - p^{-1} \tilde{N}_u \tilde{N}_u^{\mathrm{T}} + (np)^{-1} \tilde{N}_u J_{n,n} \tilde{N}_u^{\mathrm{T}}.$$

Then the information matrix for estimating direct treatment effects (τ's) is

$$C_D = C_{11} - C_{12} C_{22}^{-} C_{21}$$

and the information matrix for estimating residual treatment effects (ρ's) is

$$C_R = C_{22} - C_{21} C_{11}^{-} C_{12}.$$

Cheng and Wu [7] show that the row and column sums of C_D and C_R are 0.

Example 1. Let $t = p = 2$, $n = 10$ and let the design be

$$\begin{matrix} 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\ 1 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 2 \end{matrix}$$

Then

$$D=\begin{bmatrix}7&0\\0&13\end{bmatrix},\quad \tilde{D}=\begin{bmatrix}3&0\\0&7\end{bmatrix},\quad M=\begin{bmatrix}1&3\\2&4\end{bmatrix},\quad N_p=\begin{bmatrix}3&4\\7&6\end{bmatrix}$$

$$\tilde{N}_p=\begin{bmatrix}0&3\\0&7\end{bmatrix},\quad N_u=\begin{bmatrix}2&1&1&1&1&1&0&0&0&0\\0&1&1&1&1&1&2&2&2&2\end{bmatrix},$$

$$\tilde{N}_u=\begin{bmatrix}1&1&1&0&0&0&0&0&0&0\\0&0&0&1&1&1&1&1&1&1\end{bmatrix}$$

and

$$X_d^{\mathrm{T}}X_d=\begin{bmatrix}7&0&1&3&3&4&2&1&1&1&1&1&0&0&0&0\\0&13&2&4&7&6&0&1&1&1&1&1&2&2&2&2\\1&2&3&0&0&3&1&1&1&0&0&0&0&0&0&0\\3&4&0&7&0&7&0&0&0&1&1&1&1&1&1&1\\3&7&0&0&10&0&1&1&1&1&1&1&1&1&1&1\\4&6&3&7&0&10&1&1&1&1&1&1&1&1&1&1\\2&0&1&0&1&1&2&0&0&0&0&0&0&0&0&0\\1&1&1&0&1&1&0&2&0&0&0&0&0&0&0&0\\1&1&1&0&1&1&0&0&2&0&0&0&0&0&0&0\\1&1&0&1&1&1&0&0&0&2&0&0&0&0&0&0\\1&1&0&1&1&1&0&0&0&0&2&0&0&0&0&0\\1&1&0&1&1&1&0&0&0&0&0&2&0&0&0&0\\0&2&0&1&1&1&0&0&0&0&0&0&2&0&0&0\\0&2&0&1&1&1&0&0&0&0&0&0&0&2&0&0\\0&2&0&1&1&1&0&0&0&0&0&0&0&0&2&0\\0&2&0&1&1&1&0&0&0&0&0&0&0&0&0&2\end{bmatrix}$$

Suppose we say there are $w=1$ units of the form $(1,1)^{\mathrm{T}}$, $x=2$ units of the form $(1,2)^{\mathrm{T}}$, $y=3$ units of the form $(2,1)^{\mathrm{T}}$ and $z=4$ units of the form $(2,2)^{\mathrm{T}}$. Then

$$C_{11}=\frac{n(x+y)-(x-y)^2}{2n}\begin{bmatrix}1&-1\\-1&1\end{bmatrix}=2.45\begin{bmatrix}1&-1\\-1&1\end{bmatrix},$$

$$C_{12}=\frac{-(y(w+x)+x(y+z))}{2n}\begin{bmatrix}1&-1\\-1&1\end{bmatrix}=-1.15\begin{bmatrix}1&-1\\-1&1\end{bmatrix},$$

$$C_{22}=\frac{(w+x)(y+z)}{2n}\begin{bmatrix}1&-1\\-1&1\end{bmatrix}=1.05\begin{bmatrix}1&-1\\-1&1\end{bmatrix}.$$

Thus

$$C_D=\frac{1}{2}\left(\frac{wx}{w+x}+\frac{yz}{y+z}\right)\begin{bmatrix}1&-1\\-1&1\end{bmatrix}=\frac{1}{2}\left(\frac{2}{3}+\frac{12}{7}\right)\begin{bmatrix}1&-1\\-1&1\end{bmatrix},$$

and

$$C_R = \left(\frac{(w+x)(y+z)}{2n} - \frac{(y(w+x)+x(y+z))^2}{2n(n(x+y)-(x-y)^2)}\right)\begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}$$

$$= \left(1.05 - \frac{529}{980}\right) = \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}.$$

The discussion is slightly different for the second model since the E_{ku}'s are no longer independent and so do have preferred positions in R^{np}. The usual solution is to apply a transformation to the E_{ku}'s to make them independent and then proceed as before. Let W be a $p \times p$ matrix where $W = (W_{ij}) = (\lambda^{|i-j|}/(1-\lambda^2))$. Then the entries in W are, except for a factor of σ^2, the covariances of the error terms of the readings on any unit. Since the errors on different units are assumed to be independent, the covariance matrix of $\boldsymbol{E}$ is given by $V = \sigma^2 I_n \otimes W$. There is a matrix Z such that $ZWZ^{\mathrm{T}} = I_p$. Then $(I_n \otimes Z)V(I_n \otimes Z^{\mathrm{T}}) = \sigma^2 I_n \otimes I_p$ and so we can write

$$(I_n \otimes Z)\boldsymbol{Y} = (I_n \otimes \boldsymbol{Z})\boldsymbol{X}_d\theta + (I_n \otimes Z)\boldsymbol{E},$$

where the new error terms are now independent. We can then proceed as in the first model. The estimate $\hat{\tau}$ is called a weighted least squares estimator of τ.

For either model one further question we might ask is how accurate are the estimates we have obtained. This is measured by the variance of the estimate and for the first model the variance of $\hat{\gamma}_i$ is proportional to the ith diagonal entry of the matrix

$$(S - TV^-U)^-(S - TV^-U)(S - TV^-U)^- = (S - TV^-U)^-.$$

The smaller the variance the more accurate is the corresponding estimate. Clearly we would like the estimates to be as accurate as possible, hence we consider designs which minimise some function of the variances of the parameters we are interested in.

An *optimality criterion* is a function Φ from a set of square, nonnegative definite matrices with zero row and column sums to the real numbers. A design is said to be *Φ-optimal* if it minimises $\Phi(C_D)$ (if we are estimating direct treatment effects, or $\Phi(C_R)$, if we are estimating residual treatment effects) over a class of designs. This class of designs is often referred to as the class of competing designs. Sometimes a design has been shown to be "best" only when competing against a subset of the class of all RMDs.

We will refer to four optimality criteria in this paper. A design in a class of designs is said to be *A-optimal* if the trace of C_D^- (or C_R^-) is a minimum, to be *E-optimal* if C_D^- (or C_R^-) has minimum eigenvalue and to be *$\tilde{E}$-optimal* if it has the minimum value of the maximum variance of $\hat{\tau}_i - \hat{\tau}_j$ for all i and j.

Kiefer [11] introduced the concept of universal optimality. A design is said to be *universally optimal* if it is Φ-optimal for all Φ satisfying:

(1) Φ is convex;

(2) $\Phi(bC)$ is non-increasing in the scalar b, $b \geqslant 0$;

(3) Φ is invariant under any simultaneous permutation of the rows and columns of C. If a design is universally optimal it is A- and E-optimal.

Kiefer [11] showed that a design is universally optimal provided that the information matrix is of the form $aI + bJ$ (that is, completely symmetric), the information matrix has maximum trace (over the class of competing designs) and that the information matrix of every design in the class has zero row and column sums.

Several classes of designs have been considered and it is convenient to have a notation for them. Let $\Omega_{t,n,p}$ be the set of all repeated measurements designs (RMDs) with t treatments, n experimental units and p periods and let $\Omega^{c}_{t,n,p}$ be the set of all circular RMDs with t treatments, n experimental units and p periods. A *preperiod* is a period applied prior to the commencement of the experiment so that all observations have a residual treatment effect. Let $\bar{\Omega}_{t,n,p}$ be the set of RMDs with preperiod. Let $\Lambda_{t,n,p}$ be the set of all RMDs in which each treatment appears equally often in each period, at most once in each column and any pair of distinct treatments appear in $np(p-1)/t(t-1)$ columns. Thus $\Lambda_{t,n,p}$ is a subset of the set of generalised Youden designs (see Ash [3] for a definition). Let $\bar{\Omega}^{*}_{t,n,p}$ be the equi-replicate RMDs and let $\bar{\Omega}^{**}_{t,n,p}$ be the RMDs which are equi-replicate in the first $(p-1)$ periods. Let $\Gamma_{t,n,p}$ be the RMDs in which no treatment is applied, in successive periods, to any unit; that is, $m_{ii} = 0$.

A design is said to be *uniform on the units* if $n_{iu} = p/t$ for all $1 \leqslant i \leqslant t$, $1 \leqslant u \leqslant n$, *uniform on the periods* if $h_{is} = n/t$ for all $1 \leqslant i \leqslant t$, $1 \leqslant s \leqslant p$, *uniform* if it is uniform on both units and periods, *balanced* if $m_{ij} = (1-\delta_{ij})n(p-1)/t(t-1)$ for all $1 \leqslant i$, $j \leqslant t$ and *strongly balanced* if $m_{ij} = (p-1)n/t^2$ for all $1 \leqslant i$, $j \leqslant t$. Thus, for example, a uniform RMD with $t = n = p$ is a Latin square and a balanced, uniform RMD with $t = n = p$ is a column-complete Latin square (such as design (b) in *Table 1*).

In the remainder of this paper we summarise results about the structure of optimal RMDs, over classes of competing designs, for the two linear models given above, and the construction methods available for these designs. We do not consider the structure of optimal designs when the treatments to be applied have a factorial structure. The interested reader is referred to the papers by Fletcher and John [9] and Fletcher [8]. For a general survey of RMDs and related designs see Bishop and Jones [5]. Tables of generalised Youden designs with $t \leqslant 25$, $p,n \leqslant 50$ have been published (Ash [3]).

2. Optimal designs for RMDs with independent errors

The first class of designs we consider are strongly balanced, uniform RMDs. These designs have been shown to be optimal for the estimation of direct, and of residual, treatment effects over $\Omega_{t,n,p}$ and to minimise the variance of the best linear unbiased estimator of any contrast among direct effects (in $\Omega^{*}_{t,n,p}$) and among residual effects (in $\Omega^{**}_{t,n,p}$) (Theorems 3.1, 3.4 and 3.5, Cheng and Wu [7]).

The necessary conditions for the existence of a strongly balanced, uniform RMD are that $t \mid p$, $t \mid n$, $t^2 \mid (p-1)n$ and $p \geqslant 2t$ (since pairs of the form (i, i) can only occur if a treatment can occur at least twice on a unit). Hence

$$p = \lambda_p t, \qquad \lambda_p \geqslant 2, \qquad n = \lambda_n t^2, \quad \lambda_n \geqslant 1, \quad \lambda_p, \lambda_n \in N.$$

Construction 2 (Cheng and Wu [7]). *There is a strongly balanced, uniform* RMD *with $n = t^2$ and $p = 2t$.*

Proof. Denote the t treatments by the numbers $0, 1, 2, \ldots, t-1$. Form a $2 \times t^2$ array, A say, containing all the ordered pairs (i, j), $0 \leqslant i, j \leqslant t-1$, arranged so that the array is uniform on the rows. Let $A_i = A + i \pmod t$. The required RMD is

$$(A^{\mathrm{T}}, A_1^{\mathrm{T}}, \ldots, A_{t-1}^{\mathrm{T}})^{\mathrm{T}}.$$

Design (a) in *Table 1* was constructed in this way. The designs in construction 2 can be extended both vertically and horizontally so there is a strongly balanced, uniform RMD for $n = \lambda_n t^2$, $p = 2\lambda t$, λ_n, $\lambda \in N$. Other designs with these parameters have been constructed by Berenblut [4] and Patterson [20, 21]. Subsets of these designs with additional desirable properties for treatments with a factorial structure are described in Kok and Patterson [12]. The next construction gives a strongly balanced, uniform RMD for $3t$ periods.

Construction 3 (Sen and Mukerjee [22]). *Let L and N be two mutually orthogonal Latin squares* (MOLS) *of order t. Let the ith column of L be l_i; the ith column of N be $\boldsymbol{n}_i$, $\boldsymbol{j} = (11 \cdots 1)^{\mathrm{T}}$, $G_h = [l_h\, \boldsymbol{n}_h\, h\boldsymbol{j}]$, $1 \leqslant h \leqslant t$. Let $G = [G_1, G_2, \ldots, G_t]$ and $H_i = G + i \pmod t$. The required design is*

$$[H_1^{\mathrm{T}}, H_2^{\mathrm{T}}, \ldots, H_t^{\mathrm{T}}].$$

Example 4. Let $t = 4$ and

$$L = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, \qquad N = \begin{bmatrix} 1 & 3 & 4 & 2 \\ 2 & 4 & 3 & 1 \\ 3 & 1 & 2 & 4 \\ 4 & 2 & 1 & 3 \end{bmatrix}.$$

Then

$$G = H_4 = \begin{bmatrix} 1 & 1 & 1 & 2 & 3 & 2 & 3 & 4 & 3 & 4 & 2 & 4 \\ 2 & 2 & 1 & 1 & 4 & 2 & 4 & 3 & 3 & 3 & 1 & 4 \\ 3 & 3 & 1 & 4 & 1 & 2 & 1 & 2 & 3 & 2 & 4 & 4 \\ 4 & 4 & 1 & 3 & 2 & 2 & 2 & 1 & 3 & 1 & 3 & 4 \end{bmatrix}.$$

Arrays from Constructions 2 and 3 can be juxtaposed to give designs with $n = t^2$ and $p = \lambda_p t$, $\lambda_p \geq 2$, $\lambda_p \in N$.

An RMD with $n = \lambda_n t$, $p = \lambda_p t + 1$, λ_n, $\lambda_p \in N$ which is strongly balanced, uniform on the periods, and uniform on the units in the first $(p-1)$ periods, is universally optimal for the estimation of direct, and of residual, effects over $\Omega_{t,n,p}$ (Theorem 3.3, Cheng and Wu [7]). They point out that one way of obtaining such a design is to repeat the last period in a balanced, uniform RMD with $n = \lambda_n t$ and $p = t$. These designs exist for smaller values of n and p than do strongly balanced, uniform RMDs.

Another useful subset of RMDs are the balanced, uniform designs. These designs are universally optimal for the estimation of residual effects over $\Gamma_{t,\lambda_n t,t}$, for the estimation of residual effects over the designs in $\Gamma_{t,\lambda_n t,\lambda_p t}$ with treatments equi-replicated in the first $(p-1)$ periods, for the estimation of direct effects over the designs in $\Gamma_{t,\lambda_n t,\lambda_p t}$ uniform on units and the last period (Theorems 4.2, 4.1 and 4.3, Cheng and Wu [7]) and for the estimation of direct effects over $\Omega_{t,t,t}$ $(t \geq 3)$ and $\Omega_{t,2t,t}$ $(t \geq 6)$ (Theorems 2.1 and 2.2, Kunert [14]).

Construction 5 (E.J. Williams [29]). *There is a balanced, uniform* RMD *with* $t = n = p = 2m$.

Proof. Let the first column be $(1\;2\;2m\;3\;2m-1\;4 \cdots m\;m+2\;m+1)^{\mathrm{T}}$. Obtain subsequent columns by adding, in turn, each of the non-zero numbers modulo t to the first column. We say that the first column has been developed mod t. The design is obviously uniform. To see that the design is balanced we note that each non-zero number modulo t appears as a difference between adjacent positions precisely once.

Design (b) in *Table 1* is an example of this construction with $m = 3$ (and so $t = 6$).

For odd values of t a general construction for balanced, uniform RMDs with $t = n = p$ (that is, column-complete Latin squares) has not been found. Such designs do not exist for $t = 3$, 5 or 7. Designs for $t = 9$ and 15 have been given by Mertz and Sonnemann, quoted in Hedayat and Afsarinejad [10]. Archdeacon et al. [2] give a method of construction for squares of order pq.

Construction 6 (Williams [29]). *There is a balanced, uniform* RMD *with* $t = 2m + 1$, $t = p$, $n = 2t$.

Proof. Obtain the first set of t columns by developing the column $(1\;\;2\;\;2m+1\;\;3\;\;2m\;\;\cdots\;\;m+1\;\;m+2)^{\mathrm{T}}$ mod t and the second set of t columns by developing the column $(1\;\;2m+1\;\;2\;\;2m\;\;3 \cdots m+2\;\;m+1)^{\mathrm{T}}$ mod t. The verification of balance and uniformity is straightforward.

Design (c) in *Table 1* is an example of this construction with $m=2$ (and so $t=5$).

By juxtaposing the arrays given in constructions 2 and 3 we get balanced uniform RMDs with $t=p=2m$, $n=\lambda_n t$, $\lambda_n \geqslant 1$ and $t=p=2m+1$, $n=2\lambda t$, $\lambda \geqslant 1$.

The proofs of the next two constructions are straight-forward.

Construction 7 (Street [26]). *Let C be the array obtained by developing the column* $(1\ 2m\ 2\ 2m-1 \cdots m\ m+1)^{\mathrm{T}} \bmod 2m$ *and let*

$$C_i = \begin{cases} C+j & i=2j+1, \\ C+m-j, & i=2j, \end{cases}$$

where the addition is mod $2m$. *Then the array*

$$(C_1^{\mathrm{T}}, C_2^{\mathrm{T}}, \ldots, C_m^{\mathrm{T}})^{\mathrm{T}}$$

is a balanced, uniform RMD *with $n=t=2m$ and $p=t+t(t-1)$.*

Construction 8 (Street [26]). *Let* $r_e=(1, 2m+1, 2, 2m, 3, \ldots, m+3, m, m+2, m+1)$, $r_0=(1, 2, 2m+1, 3, 2m, \cdots m, m+3, m+1, m+2)$ *and let "$r_e(+i)r_0$" mean "write down r_e, add i to the final element of r_e and use this as the first element of r_0". Then the array obtained by developing the first column*

$$(r_e(+1)r_0(+3)r_e(+5)\cdots(+2m-1)r_e(+1)r_0(+3)r_e(+5)\cdots(+2m-1)r_e), \quad 2m+1 \equiv 1 \pmod 4,$$

$$(r_e(+1)r_0(+3)r_e(+5)\cdots(+2m-1)r_0(+1)r_e(+3)r_0(+5)\cdots(+2m-1)r_0), \quad 2m+1 \equiv 3 \pmod 4,$$

is a balanced, uniform RMD *with $n=t=2m+1$, $p=t+t(t-1)$.*

Example 9. Let $m=2$. Then $r_e=(1\ 5\ 2\ 4\ 3)$, $r_0=(1\ 2\ 5\ 3\ 4)$ and the first column is $r_e(+1)r_0(+3)r_e(+1)r_0(+3)r_e$ which is $(1\ 5\ 2\ 4\ 3\ 4\ 5\ 3\ 1\ 2\ 5\ 4\ 1\ 3\ 2\ 3\ 4\ 2\ 5\ 1\ 4\ 3\ 5\ 2\ 1)$.

Clearly the number of units can be extended to any multiple of t, and the number of periods can be any number of the form $t+t(t-1)a$, $a \geqslant 1$.

The next result shows that if $t=n=p$ then balanced, uniform RMDs are not universally optimal for the estimation of residual effects over $\Omega_{t,t,t}$.

Theorem 10 (Proposition 3.1, Kunert [14]). *Assume $t=n=p$ and there exists $f \in \Omega_{t,t,t}$ such that*

(i) *by exchanging the last period we can transform f to be uniform*;

(ii) *the last and second last periods are the same*;

(iii) *for every treatment i there exists a unique treatment j_i such that treatment i is never preceded by treatment j_i (thus i is preceded exactly once by every other treatment including i)*;

(iv) *in the unit in which treatment i appears in each of the last two periods, treatment j_i does not appear at all.*

Then no balanced uniform design in $\Omega_{t,t,t}$ can be universally optimal for the estimation of residual effects over $\Omega_{t,t,t}$.

Street [27] gives initial columns for designs satisfying the conditions of the theorem for all $t \geqslant 5$.

Let $n = t(t-1)$ and suppose there is a balanced, uniform design d in $\Omega_{t,t(t-1),t}$ with the property that every ordered pair of distinct treatments appears exactly once between the last two periods of d. Construct the design f from d by replacing the tth period in d with the $(t-1)$th period. Then f is called an *orthogonal residual effects design* and has the property that $C_{12} = 0$. Kunert ([14], Proposition 3.3) has shown that orthogonal residual effects designs are universally optimal for the estimation of residual effects over $\Omega_{t,t(t-1),t}$.

Construction 11 (Sonnemann, quoted in Kunert [16]). *Let L be a balanced, uniform* RMD *with $t = n = p = 2m$. Adjoin to L a first row containing the treatment $2m+1$. Use each column of this augmented square to construct a cyclic square of order $2m+1$. Juxtaposing these squares gives a balanced, uniform RMD with $t = p = 2m+1$, $n = t(t-1)$ and with every ordered pair of distinct treatments appearing exactly once between the last two periods.*

Proof. Since L is a balanced, uniform design, the augmented square is uniform on units, and the final array is obtained by juxtaposing cyclic squares obtained one from each unit, we see that the final array is uniform. Since L is uniform, treatment $2m+1$ is adjacent to each treatment equally often and, since L is balanced, so is every other treatment. The ordered pairs in the last two rows of the array are the pairs of treatments adjacent in L together with $(2m+1, i)$, i in the first row of L and $(j, 2m+1)$, j in the final row of L. Since L is uniform and balanced, the result follows.

Example 12. Let $m = 2$, $t = 4$. Then

$$L = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 4 & 1 & 2 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}, \qquad L\text{ (adjoined)} = \begin{bmatrix} 5 & 5 & 5 & 5 \\ 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 4 & 1 & 2 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}$$

and the RMD is

$$\begin{array}{cccccccccccccccccccc}
5 & 3 & 4 & 2 & 1 & 5 & 4 & 1 & 3 & 2 & 5 & 1 & 2 & 4 & 3 & 5 & 2 & 3 & 1 & 4 \\
1 & 5 & 3 & 4 & 2 & 2 & 5 & 4 & 1 & 3 & 3 & 5 & 1 & 2 & 4 & 4 & 5 & 2 & 3 & 1 \\
2 & 1 & 5 & 3 & 4 & 3 & 2 & 5 & 4 & 1 & 4 & 3 & 5 & 1 & 2 & 1 & 4 & 5 & 2 & 3 \\
4 & 2 & 1 & 5 & 3 & 1 & 3 & 2 & 5 & 4 & 2 & 4 & 3 & 5 & 1 & 3 & 1 & 4 & 5 & 2 \\
3 & 4 & 2 & 1 & 5 & 4 & 1 & 3 & 2 & 5 & 1 & 2 & 4 & 3 & 5 & 2 & 3 & 1 & 4 & 5
\end{array}$$

There do not appear to be any construction methods for orthogonal residual effects designs for even t.

Suppose that $t=p>2$ and that $n=\lambda t$, where $\lambda>t(t-1)^2/2$ and $\lambda\in Z$. Let $g\in\Omega_{t,n,t}$ be such that the first $t(t-1)$ units of g form an orthogonal residual effects design and the remaining $n-t(t-1)$ units of g form a balanced uniform design. Then g is universally better than any balanced uniform design in $\Omega_{t,n,t}$ for the estimation of direct effects (Proposition 2.4, Kunert [14]).

Suppose that the class of designs is $\Omega_{t,n,p}\cup\bar{\Omega}_{t,n,p}$ and that the direct effects are to be estimated. Then the universally optimal designs are generalised Youden designs with $m_{ij}=r_j/t$ if $t\mid n$ and $t\mid p$, $m_{ij}=\sum_k h_{ik}\bar{h}_{jk}/n$ if $t\nmid n$ and $t\mid p$ and $m_{ij}=\sum_u n_{iu}\bar{n}_{ju}/p$ if $t\mid n$ and $t\nmid p$ (Theorems 4.1, 4.4, 4.8 Kunert [13]). General construction methods for these designs do not seem to be available. Indeed generalised Youden designs have mainly been constructed by complete search techniques and tables for generalised Youden designs with $t\leqslant 25$, n, $p\leqslant 50$ have been given by Ash [3]. These tables do not give the values of m_{ij}.

The final results we shall mention in this section concern nearly strongly balanced generalised Youden designs. A design is said to be *nearly strongly balanced* if MM^{T} is completely symmetric and if, for all $1\leqslant i$, $j\leqslant t$, $m_{ij}\in\{[n(p-1)t^{-2}], [n(p-1)t^{-2}]+1\}$. When $n=at^2+bt$, $1\leqslant b\leqslant t-1$, $p=\lambda t$ then the nearly strongly balanced generalised Youden designs are universally optimal for the estimation of direct effects over the class of designs in $\Omega_{t,n,p}$ which are uniform on units and in the last period, for the estimation of residual effects over the class of designs in $\Omega_{t,n,p}$ which are uniform on the units and on each of the first and last periods and for the estimation of direct effects over $\Omega_{t,n,p}$ if $a\geqslant b(t-b-1)/t$ and $\lambda\geqslant\max\{2, b(t-b)/4+2/t\}$ (Theorems 5.3, 5.4 and 5.8, Kunert [13]). Again there do not appear to be any construction methods available for these designs.

3. Optimal designs for circular RMDs with independent errors

The results of this section are similar to those of the previous section.

The universally optimal designs for the estimation of direct, as well as of residual, effects over $\Omega^{c}_{t,n,p}$ are the strongly balanced, uniform designs (Theorem 3.1, Magda [19]). If $t=p$ then the universally optimal designs for the estimation of direct, as well as of residual, effects are the uniform, balanced designs (Theorem 2.2, Kunert [15]). If we restrict the class of designs to the equi-replicated $\Omega^{c}_{t,n,p}$ then the strongly balanced, uniform designs minimise the variance of the best linear unbiased estimator of any contrast of direct effects, and of any contrast of residual effects (Theorem 3.3, Magda [19]). The universally optimal designs for the estimation of direct, as well as residual, effects over $\Gamma_{t,n,p}$ are the balanced, uniform designs (Theorem 3.4, Magda [19]).

Magda [19] also establishes that if the term for the period effect is removed from the model then so is the requirement of uniformity on periods. Similar results are true for removing the unit effect and both the period and unit effects.

The necessary conditions for the existence of a strongly balanced, uniform circular RMD are that $t \mid p$, $t \mid n$ and $t^2 \mid pn$. Thus $p = \lambda_p t$ and $n = \lambda_n t$, say, λ_p, $\lambda_n \in N$. Note that the designs obtained from construction 2 are also circular, strongly balanced, uniform designs with $p = 2t$ and $n = t^2$.

Another family of circular, strongly balanced, uniform designs can be obtained from the type 1 serially balanced sequences of R.M. Williams [30].

A type 1 serially balanced sequence of order t and index λ is a sequence of length $\lambda t^2 + 1$, which has the following properties:

(i) the first and last elements are the same;

(ii) the first element appears $\lambda t + 1$ times;

(iii) the remaining $t - 1$ elements appear λt times each;

(iv) each of the t^2 ordered pairs of elements appears λ times among the λt^2 pairs of consecutive elements;

(v) aside from the first element, each element appears precisely once in each of the λt successive sets of t elements.

We denote such a sequence by SBS1(t, λ).

Clearly instead of repeating the last element we just view the sequence as being circular so the sequence is uniform. We develop the sequence mod t to obtain a circular, strongly balanced, uniform RMD with $p = \lambda t^2$ and $n = t$.

Construction 13 (R.M. Williams [30]; see also Street and Street [25]). *An* SBS1$(t, 2)$ *exists for all* $t \geq 4$.

Proof. If $t = 2m$ let $L = (l_{ij})$ be the Latin square with first row and column given by $(1\ 2\ 2m\ 3\ 2m-1\ 4 \cdots m\ m+2\ m+1)$ and with $l_{ij} = l_{i1} + l_{1j} - 1 \pmod{2m}$, $i > 1$, $j > 1$. Let N be the Latin square obtained from L by applying the permutation $\pi = (1\ 2\ 3 \cdots m)$ to the elements of L. The sequence is obtained by writing down the first row of L, then the row of N beginning with the element $m + 1$, followed by the row of L beginning with the element at the end of the row of N, and so on, until m rows of both L and N have been used. The $(2m + 1)$st row to be used is taken from N and then the alternation continues until all the rows of both squares have been used. Since both L and N are balanced in rows, all ordered pairs of distinct elements appear twice. If we can show that each row of L and N is used precisely once, then pairs of the form (i, i) will appear twice in the final sequence. Let us index the rows in L and N by their first elements. In L, if the first element in a row is i, then the last element is $i + m \pmod{2m}$ whereas in N, it is

$$\pi^{-1}(i) + m \pmod{2m}, \quad \text{if } 1 \leq i \leq m,$$

or

$$\pi(i + m), \quad \text{if } m + 1 < i < 2m.$$

Hence the rows used from L and N are

$$\begin{array}{lllllllll} L\colon & 1 & 2 & 3 & \cdots m & 2m & 2m-1 & \cdots & m+1 \\ N\colon & m+1 & m+2 & m+3 \cdots & 2m\ 1 & m & m-1 & \cdots & 2 \end{array}$$

and we see that each row is used once, as required.

If $t = 2m + 1$, let L be the Latin square with first row and column $(1\,2\,2m+1\,3\,2m\,4 \cdots m\,m+3\,m+1\,m+2)$ and with $l_{ij} = l_{i1} + l_{1j} - 1 (\text{mod}\,2m+1)$, $i > 1$, $j > 1$. Let N be the Latin square obtained from L by adding m to each element (mod $2m + 1$) and reversing each row. The construction is similar to that for t even, except that now all the rows in L are used and then all the rows in N. Verification is straightforward.

Example 14. Let $m = 2$, $t = 4$. Then

$$L = \begin{bmatrix} 1 & 2 & 4 & 3 \\ 2 & 3 & 1 & 4 \\ 4 & 1 & 3 & 2 \\ 3 & 4 & 2 & 1 \end{bmatrix}, \qquad N = \begin{bmatrix} 2 & 1 & 4 & 3 \\ 1 & 3 & 2 & 4 \\ 4 & 2 & 3 & 1 \\ 3 & 4 & 1 & 2 \end{bmatrix}$$

and the first column is

$$1\,2\,4\,3 \quad 3\,4\,1\,2 \quad 2\,3\,1\,4 \quad 4\,2\,3\,1 \quad 1\,3\,2\,4 \quad 4\,1\,3\,2 \quad 2\,1\,4\,3 \quad 3\,4\,2\,1.$$

The proof of the next result is also straightforward.

Construction 15 (Sharma [24]). *Develop the first column*

$$(t\,t-1\,1\,t-2\,2\,t-3 \cdots t-2\,1\,t-1\,t)^{\mathrm{T}}$$

modulo t. This gives a circular, strongly balanced, uniform RMD *with $n = t$ and $p = 2t$. The first column can be extended in multiples of $2t$ as required.*

There are two known families of circular, balanced, uniform RMDs.

Construction 16 (Sonnemann, quoted in Kunert [16]). *Let $t = 2m$ and obtain the first set of t columns by developing the column*

$$(2m\ 1\ 2m-1\ 2\ 2m-2\ 3 \cdots m+1\ m)$$

and call this set L. Let $\pi = (1\,2 \cdots m-1\,2m-1 \cdots m)$ and let $L_i = \pi^i L$ so $L = L_0$. The required RMD *is $(L_0, L_1, \ldots, L_{t-2})$ and has $p = t = 2m$, $n = t(t-1)$.*

Proof. Each L_i is a balanced, uniform RMD. Hence we need only consider the pairs formed by viewing the array as circular. The set of pairs so obtained from L are $\{(m, 2m), (m+1, 1), (m+2, 2), \ldots, (m-1, 2m-1)\} = S$, say. The pairs obtained from L_i are found by applying π^i to the elements of the pairs in S. The result follows.

Example 17. Let $m = 3$, $t = 6$. Then $\pi = (1\,2\,5\,4\,3)$ and

$$L = L_0 = \begin{bmatrix} 6 & 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 & 6 & 1 \\ 4 & 5 & 6 & 1 & 2 & 3 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{bmatrix} \qquad L_1 = \pi L = \begin{bmatrix} 6 & 2 & 5 & 1 & 3 & 4 \\ 2 & 5 & 1 & 3 & 4 & 6 \\ 4 & 6 & 2 & 5 & 1 & 3 \\ 5 & 1 & 3 & 4 & 6 & 2 \\ 3 & 4 & 6 & 2 & 5 & 1 \\ 1 & 3 & 4 & 6 & 2 & 5 \end{bmatrix}$$

$$L_2 = \begin{bmatrix} 6 & 5 & 4 & 2 & 1 & 3 \\ 5 & 4 & 2 & 1 & 3 & 6 \\ 3 & 6 & 5 & 4 & 2 & 1 \\ 4 & 2 & 1 & 3 & 6 & 5 \\ 1 & 3 & 6 & 5 & 4 & 2 \\ 2 & 1 & 3 & 6 & 5 & 4 \end{bmatrix} \qquad L_3 = \begin{bmatrix} 6 & 4 & 3 & 5 & 2 & 1 \\ 4 & 3 & 5 & 2 & 1 & 6 \\ 1 & 6 & 4 & 3 & 5 & 2 \\ 3 & 5 & 2 & 1 & 6 & 4 \\ 2 & 1 & 6 & 4 & 3 & 5 \\ 5 & 2 & 1 & 6 & 4 & 3 \end{bmatrix}$$

$$L_4 = \begin{bmatrix} 6 & 3 & 1 & 4 & 5 & 2 \\ 3 & 1 & 4 & 5 & 2 & 6 \\ 2 & 6 & 3 & 1 & 4 & 5 \\ 1 & 4 & 5 & 2 & 6 & 3 \\ 5 & 2 & 6 & 3 & 1 & 4 \\ 4 & 5 & 2 & 6 & 3 & 1 \end{bmatrix}$$

The other family is obtained from the type 2 sequences of R.M. Williams [30]. A type 2 serially balanced sequence of order t and index λ is a sequence of length $\lambda t(t-1)+1$, which has the following properties:

(i) the first and last elements are the same;

(ii) the first element appears $\lambda(t-1)+1$ times;

(iii) the remaining $t-1$ elements appear $\lambda(t-1)$ times each;

(iv) each of the $t(t-1)$ ordered pairs of elements appears λ times among the $\lambda t(t-1)$ pairs of consecutive elements;

(v) aside from the first element, each element appears precisely once in each of the $\lambda(t-1)$ successive sets of t elements.

We denote such a sequence by SBS2(t, λ).

Again rather than repeat the last element we view the sequence as circular, so it is uniform. We develop the sequence modulo t to obtain a circular, balanced, uniform RMD with $p = \lambda t(t-1)$ and $n = t$. The verification of the next result is straightforward.

Construction 18 (R.M. Williams [30]; see also Street and Street [25]). *An* SBS2$(t, 1)$ *exists for all* $t \geq 4$ *and is obtained by developing a column of size* *t and concatenating the columns in the natural order. The initial columns are*:

$$1, 2, 2m, 3, 2m-1, \ldots, m, m+2, m+1, \infty, \quad \textit{if } t-1=2m,$$

$$1, \infty, 2, 4m+1, 3, 4m, 4, \ldots m, 3m+3, m+1, m+2, 3m+2,$$
$$m+3, 3m+1, \ldots, 2m+1, 2m+3, 2m+2,$$

if $t-1=4m+1$;

$$1, \infty, 2, 4m+3, 3, 4m+2, 4, \ldots, m+1, 3m+4, m+2, m+3,$$
$$3m+3, m+4, 3m+2, \ldots, 2m+2, 2m+4, 2m+3,$$

if $t-1=4m+3$;

where the blocks are developed modulo $t-1$ *and* $\infty+i=\infty$ *for all* i.

Example 19. Let $m=1$, $t-1=5$, $t=6$. The required column is $1\infty23542\infty34153\infty45214\infty51325\infty1243$.

4. Optimal designs for RMDs with correlated errors

In this situation the optimal designs usually prove to be variants of the designs constructed by E.J. Williams [29] and called Williams designs by Kunert [16]. Let $w_{ij}=m_{ij}+m_{ji}$ and let d be a uniform RMD with $t=p$ and in which the w_{ij} $(i \neq j)$ are equal. Then d is said to be a *Williams design*. Let $d=(d_{ij})$ be a Williams design and let B be the block design with blocks (d_{1j}, d_{pj}), $j=1, 2, \ldots, n$. B is called the *end-pair design*. A design is said to be *connected* if, given any two treatments, it is possible to form a list of treatments, starting with one and ending with the other, such that any two adjacent treatments in the list appear in some block of the design. If $t=n$ and if the end-pair design is connected then the original design is said to be a *Williams design with circular structure*. If the end-pair design is a balanced incomplete block design then the original design is said to be a *Williams design with balanced end-pairs*. We will let $\Delta_{t,n,t}$ be the set of all Williams designs on n units and using t treatments.

Recall that $\mathrm{Corr}(E_{ku}, E_{gu})=\lambda^{|k-g|}\delta_{uu'}$. The optimal designs depend on the value of λ. For example, a Williams design with balanced end-pairs is universally optimal for the estimation of treatment effects over the class of uniform RMDs with $t=p$ and is universally optimal over $\Omega_{t,n,j}$ whenever

$$\lambda \geq \{t-2-\sqrt{t^2-8}\}/\{2(t-3)\}$$

and $t \geq 4$ and for all λ when $t=3$ (Theorem 1, Kunert [16]).

Suppose that $n \leq \binom{t}{2}$. Then a Williams design is E-optimal over the class of uniform RMDs which are not Williams designs and this is true for all λ $(-1<\lambda<1)$. If $n=t \geq 4$ and $-1/(t-1) \leq \lambda \leq \frac{1}{2}$ then a Williams design is E-optimal over the class of RMDs which are not Williams designs. If $n=t \geq 5$ and $-1/(t-1) \leq \lambda \leq \frac{1}{2}$, then a Williams design with circular structure is E-optimal over $\Omega_{t,t,t}$ (Theorems 2 and 3 and comments on p. 384, Kunert [16]). If $\lambda > \frac{1}{2}$ or $\lambda < -1/(t-1)$ the optimality, or otherwise, of Williams designs has not been established.

The designs given in Construction 5 are Williams designs and the first t columns of the designs given in Construction 6 are Williams designs with circular structure. The designs given in Constructions 11 and 16 are Williams designs with balanced end-pairs. Indeed one needs only juxtapose the first m squares in Construction 11 to get a Williams design with balanced end-pairs. The next result is straightforward to prove and gives Williams designs with circular structure for $t = 4m + 2$. The existence of Williams designs with circular structure for $t = 4m$ is still unresolved.

Construction 20 (Street [27]). *Developing the column*

$(1\; 2m\; 2\; 2m-1 \cdots m\; m+1\; 3m+1\; 3m+2\; 3m\; 3m+3 \cdots 2m+2\; 4m+1\; 2m+1\; 4m+2)$

modulo $t = 4m + 2$ *gives a Williams design with circular structure.*

Example 21. Let $m = 1$ and $t = 6$. Then the Williams design is

1	2	3	4	5	6
2	3	4	5	6	1
4	5	6	1	2	3
5	6	1	2	3	4
3	4	5	6	1	2
6	1	2	3	4	5

and the end-pair design is $(1, 6)$, $(2, 1)$, $(3, 2)$, $(4, 3)$, $(5, 4)$, $(6, 5)$.

Any design in $\Lambda_{t,n,p}$ performs equally well under the A-optimality criterion but not under the $\tilde{E}$-optimality criterion. For $d \in \Lambda_{t,n,p}$, let $M_{ij}(k)$ be the number of columns in which treatments i and j appear with exactly $k-1$ rows between them, let $l_{ik}(j)$ be the number of columns where treatment i appears in row k and treatment j does not appear at all and let $h_{ij}(k) = l_{ik}(j) + l_{jk}(i)$.

Theorem 22 (Result 2, Kunert [17]). *Assume that* $t \mid n$ *and* $\binom{t}{2} \mid n$ *and that* $d \in \Lambda_{t,n,p}$ *exists with*

(i) $M_{ij}(k) = 2(p-k)n/(t(t-1))$, $k = 1, 2, \ldots, p-1$,

(ii) $h_{ij}(k') = 2n(t-p)/(t(t-1))$, $k' = 1, 2, \ldots, p$,

for all $1 \leq i,j \leq t$. *Then d is $\tilde{E}$-optimal over* $\Lambda_{t,n,p}$ *for all* $-1 < \lambda < 1$.

A perpendicular array is a $p \times \binom{t}{2}$ array, t odd, containing the symbols $1, 2, \ldots, t$, arranged so that, considering the set of pairs coming from any two rows of the array, each unordered pair appears precisely once in the set. Any perpendicular array satisfies the conditions of the theorem (Street [28]). The proof of the next result is straightforward.

Construction 23 (Street [28]). *Assume that a set of m idempotent* MOLS *of order t exists. Construct an array* $A = [a_{ij}]$ *of size* $(m+2) \times t^2$ *as follows. Let a_i be the* ith *row of A. Then* $a_{m+1} = [1, 2, \ldots, t] \otimes \boldsymbol{j}_t$ *and* $\boldsymbol{a}_{m+2} = \boldsymbol{j}_t \otimes [1, 2, \ldots, t]$. *Then, for* $i \neq m+1, m+2$, *the entry in row i and column j is the entry in the* $(a_{m+1,j}, a_{m+2,j})$ *position of square i. Now remove from A the t columns containing only one symbol. The resulting array is a design with* $n = t(t-1)$ *and* $p = m+2$ *satisfying the conditions of Theorem 22.*

Example 24. Let $m = 2$ and $t = 4$. Let the two idempotent MOLS be

$$\begin{array}{cccc} 1 & 3 & 4 & 2 \\ 4 & 2 & 1 & 3 \\ 2 & 4 & 3 & 1 \\ 3 & 1 & 2 & 4 \end{array} \quad \text{and} \quad \begin{array}{cccc} 1 & 4 & 2 & 3 \\ 3 & 2 & 4 & 1 \\ 4 & 1 & 3 & 2 \\ 2 & 3 & 1 & 4 \end{array}$$

The required design is

1	1	1	2	2	2	3	3	3	4	4	4
2	3	4	1	3	4	1	2	4	1	2	3
3	4	2	4	1	3	2	4	1	3	1	2
4	2	3	3	4	1	4	1	2	2	3	1

5. Miscellaneous designs

Some other families of RMDs have been constructed. We mention some below.

Construction 25 (Afsarinejad [1]). *If t is even,* $t = \lambda(p-1)+1$ *and* $n = \lambda t$, $\lambda \in N$, *then a balanced* RMD *can be obtained by developing, in turn,* mod t, *each of the* λ *columns*

$$(c_1, c_2, \ldots, c_p),\ (c_p, c_{p+1}, \ldots, c_{2p-1}),\ \ldots,\ (c_{(\lambda-1)p-(\lambda-2)}, \ldots, c_t),$$

where

$$(c_1, c_2, \ldots, c_t) = (1, t, 2, t-1, 3, t-2, \ldots, t/2, (t+2)/2).$$

Proof. The set $\bigcup_{i=2}^{t} \{c_i - c_{i-1}\}$ contains each non-zero number mod t and so each ordered pair of distinct treatments will appear precisely once in the final array.

Example 26. Let $p = 4$, $\lambda = 3$ so $t = 10$. Then $(c_1, c_2, c_3, \ldots, c_{10}) = (1, 10, 2, 9, 3, 8, 4, 7, 5, 6)$ and the design is

1	2	3	4	5	6	7	8	9	10	9	10	1	2	3	4	5	6	7	8	4	5	6	7	8	9	10	1	2	3
10	1	2	3	4	5	6	7	8	9	3	4	5	6	7	8	9	10	1	2	7	8	9	10	1	2	3	4	5	6
2	3	4	5	6	7	8	9	10	1	8	9	10	1	2	3	4	5	6	7	5	6	7	8	9	10	1	2	3	4
9	10	1	2	3	4	5	6	7	8	4	5	6	7	8	9	10	1	2	3	6	7	8	9	10	1	2	3	4	5

If $\lambda(p-1) = t$ and $n = \lambda t$ then a strongly balanced RMD can be obtained in the same way using the sequence $(c_1, c_2, \ldots, c_t, c_t)$.

A similar construction works for odd t.

Construction 27 (Afsarinejad [1]). *If t is odd, $t = \lambda(p-1)+1$ and $n = \lambda t$, $\lambda \in N$, then a balanced* RMD *can be obtained by developing, in turn, each of the λ columns*

$$(c_1, c_2, \ldots, c_p), (c_p, c_{p+1}, \ldots, c_{2p-1}), \ldots, (c_{(\lambda-1)p-(\lambda-2)}, \ldots, c_t)$$

where

$$(c_1, c_2, \ldots, c_t) = (1, t, 3, t-2, 5, t-4, \ldots, (t-3)/2, (t+5)/2, (t+1)/2, (t+5)/2(t-3)/2, \ldots, t, 1).$$

Again if $\lambda(p-1) = t$ and $n = \lambda t$ then a strongly balanced RMD can be obtained in the same way using the sequence $(c_1, c_2, \ldots, c_{(t+1)/2}, c_{(t+1)/2}, c_{(t+3)/2}, \ldots, c_t)$.

Chakravarti [6] gives some sequences, based on polynomials, which give rise to RMDs which are uniform on the periods, have $p = t$ and in which every ordered triple of distinct treatments appears equally often.

Example 28. Let $t = 8$ and let ϑ be a primitive element of GF(8), with primitive polynomial $x^3 + x + 1$. Let $\mathrm{GF}(8) = \{\alpha_0 = 0, \alpha_1 = 1, \alpha_2 = \vartheta, \ldots, \alpha_7 = \vartheta^6\}$ and define the polynomial $f(.)$ by

x	α_0	α_1	α_2	α_3	α_4	α_5	α_6	α_7
$f(x)$	α_0	α_1	α_2	α_3	α_4	α_5	α_6	α_7

.

Let $P_i(x) = w^{i-1}f(x)$, $i = 1, 2, \ldots, 7$ and let $L_i = (\alpha_j + P_i(x))$, j, $x = 0, 1, \ldots, 7$; $i = 1, 2, \ldots, 6$. Then $A^{\mathrm{T}} = (L_1^{\mathrm{T}}, L_2^{\mathrm{T}}, \ldots, L_7^{\mathrm{T}})$ is the required design.

6. Conclusion

We conclude with a summary of some of the open problems.

Strongly balanced, uniform RMDs can only exist if $p = \lambda_p t$, $\lambda_p \geq 2$, $n = \lambda_n t^2$ and λ_p, $\lambda_n \in N$. Constructions 2 and 3 give such designs but non-isomorphic designs with these parameters are of interest; see, for example, Kok and Patterson [12].

Balanced, uniform RMDs can only exist if $p = \lambda_p t$, $n = \lambda_n t$ and $t(t-1) \mid n(p-1)$. The known families have $t = p = 2m$, $n = \lambda_n t$; $t = 2m$, $p = t + t(t-1)a$, $a \geq 1$, $n = \lambda_n t$; $t = p = 2m+1$, $n = 2\lambda_n t$; $t = 2m+1$, $p = t + t(t-1)a$, $a \geq 1$, $n = \lambda_n t$ and $t = p = 2m+1$, $n = t(t-1)$.

Generalised Youden designs with $M = t^{-1}J_{t,t}D$, if $t \mid n$ and $t \mid p$, with $M = n^{-1}n_p\bar{N}_p^{\mathrm{T}}$, if $t \nmid n$ and $t \mid p$ and with $M = p^{-1}N_u\bar{N}_u^{\mathrm{T}}$, if $t \mid n$ and $t \nmid p$, as well as nearly strongly balanced, generalised Youden designs are required.

Circular, strongly balanced, uniform RMDs can only exist if $p = \lambda_p t$, $n = \lambda_n t$ and λ_p, $\lambda_n \in N$. The smallest combination of p and n known is $p = 2t$ and $n = t$. Do such designs exist for $p = 3t$ and $n = t$?

Circular, balanced, uniform RMDs can only exist if $p = \lambda_p t$, $n = \lambda_n t$ and

$t(t-1) \mid np$. Known designs have either $p=t=2m$, $n=t(t-1)$ or $p=\lambda(t-1)$, $\lambda \geqslant 1$, $n=t$.

No general construction methods for Williams designs with circular structure with $t=4m$ are known. Such a design cannot exist for $t=4$. Examples are known for $t=8$, but have only been found by exhaustive search. It is also easy to show that a single column, to be developed mod $4m$, cannot exist.

Designs satisfying the conditions of Theorem 22 are known for $p=3$, 4 and 5 for all odd t (except possibly $p=5$ and $t=39$) (Lindner [18]) but results for larger p are much sparser.

Acknowledgement

I thank the referees for critically reading the paper and offering a number of constructive suggestions.

References

[1] K. Afsarinejad, Balanced repeated measurements designs, Biometrika 70 (1983) 199–204.

[2] D.S. Archdeacon, J.H. Dinitz, D.R. Stinson and T.W. Tillson, Some new row-complete Latin squares, J. Combin. Theory A29 (1980) 395–398.

[3] A. Ash, Generalized Youden designs: Construction and tables, J Statistical Planning and Inference 5 (1981) 1–25.

[4] I.I. Berenblut, Change-over designs with complete balance for first residual effects, Biometrics 20 (1964) 707–712.

[5] S.H. Bishop and B. Jones, A review of higher order crossover designs, J. Applied Statistics 11 (1984) 29–50.

[6] I.M. Chakravarti, On Williams' balanced designs from Latin squares admitting certain sets of serial symmetries, in Contributions to Statistics: Essays in Honour of Norman L. Johnson, P.K. Sen. (ed.) (North-Holland Publishing Company, 1983), 97–105.

[7] C.S. Cheng and C.F. Wu, Balanced repeated measurements designs, Annals of Statistics 8 (1986) 1272–1283.

[8] D.J. Fletcher, A new class of change-over designs for factorial experiments, Biometrika 74 (1987), 649–654.

[9] D.J. Fletcher and J.A. John, Changeover designs and factorial structure, J. Royal Statistical Society B 47 (1985), 117–124.

[10] A. Hedayat and K. Afsarinejad, Repeated measurement design, II, Annals of Statistics 6 (1978) 619–628.

[11] J. Kiefer, Construction and optimality of generalized Youden designs, in A Survey of Statistical Design and Linear Models, J.N. Srivastava (ed.) (North-Holland 1975) 333–353.

[12] K.-L. Kok and H.D. Patterson, Algebraic results in the theory of serial factorial design, Biometrika 63 (1976) 559–565.

[13] J. Kunert, Optimal design and refinement of the linear model with applications to repeated measurements designs, Annals of Statistics 11 (1983), 247–257.

[14] J. Kunert, Optimality of balanced uniform repeated measurements designs, Annals of Statistics 12 (1984) 1006–1017.

[15] J. Kunert, Designs balanced for circular residual effects, Communications in Statistics—Theory and Methods 13(21) (1984) 2665–2671.

[16] J. Kunert, Optimal repeated measurements designs for correlated observations and analysis by weighted least squares, Biometrika 72 (1985) 375–389.

[17] J. Kunert, Optimal experimental design when the errors are assumed to be correlated, Statistics and Decisions, Supplement Issue No. 2 (1985) 287–298.

[18] C.C. Lindner, Perpendicular arrays and graph decompositions Ars Combin. 26B (1988) 67–92.

[19] C.G. Magda, Circular balanced repeated measurements designs, Communications in Statistics—Theory and Methods A9 (1980) 1901–1918.

[20] H.D. Patterson, Nonadditivity in change-over designs for a quantitative factor at four levels, Biometrika 57 (1970), 537–549.

[21] H.D. Patterson, Quenouille's changeover designs, Biometrika 60 (1973) 33–45.

[22] M. Sen and R. Mukerjee, Optimal repeated measurements designs under interaction, J. Statistical Planning and Inference 17 (1987) 81–91.

[23] S.R. Searle, Linear Models (John Wiley, New York, 1971).

[24] V.K. Sharma, Extra-period balanced change-over designs, Sankhya B44 (1982) 167–173.

[25] A.P. Street and D.J. Street, Combinatorics of Experimental Designs (Clarendon Press, Oxford, 1987).

[26] D.J. Street, Unbordered two-dimensional nearest neighbour designs, Ars Combinatoria 22 (1986) 51–57.

[27] D.J. Street, Some repeated measurements designs, Communications in Statistics—Theory and Methods, 17 (1988) 87–104.

[28] D.J. Street, Some construction methods for optimal designs when the errors are assumed correlated, Ars Combin. 26A (1988) 193–196.

[29] E.J. Williams, Experimental designs balanced for the estimation of residual effects of treatments, Australian J. Scientific Research A2 (1949) 149–168.

[30] R.M. Williams, Experimental designs for serially correlated observations, Biometrics 39 (1952), 151–167.

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 345–356
North-Holland

LOCALLY TRIVIAL t-DESIGNS AND t-DESIGNS WITHOUT REPEATED BLOCKS

Luc TEIRLINCK*
Division of Mathematics (Algebra, Combinatorics and Analysis), Auburn University, Auburn, AL 36849, U.S.A.

To Haim Hanani on his seventy-fifth birthday.

We simplify our construction [12] of non-trivial t-designs without repeated blocks for arbitrary t. We survey known results on partitions of the set of all $(t+1)$-subsets of a v-set into $S(\lambda; t, t+1, v)$ for the smallest λ allowed by the obvious necessary conditions. We also obtain some new results on this problem. In particular, we construct such partitions for $t = 4$ and $\lambda = 60$ whenever $v = 60u + 4$, u a positive integer with $\gcd(u, 60) = 1$ or 2. Sixty is the smallest possible λ for such v.

1. Introduction

It has been known for a long time that there are a lot of t-designs for all t. However, it was not until relatively recently that the first examples of non-trivial 6-designs without repeated blocks were found [7]. In [12], we constructed non-trivial t-designs without repeated blocks for all t. More precisely, we showed that if $v \equiv t \pmod{(t+1)!^{(2t+1)}}$, $v \geq t+1$, then the set of all $(t+1)$-subsets of a v-set can be partitioned into $S((t+1)!^{(2t+1)}; t, t+1, v)$.

In Section 2, we give a simpler proof of the main result, mentioned above, of [12]. Actually, we will prove a somewhat stronger theorem, but this is only due to the fact that we did not try to minimize the $\lambda = (t+1)!^{(2t+1)}$ in [12]. The main construction of Section 2 (Proposition 6) is actually a special case of the constructions of [12].

In Section 3, we survey known results on partitions of the set of all $(t+1)$-subsets of a v-set into $S(\lambda; t, t+1, v)$ for the smallest value of λ allowed by the obvious necessary conditions. We also obtain some new results on this problem. For instance, we prove that the set of all 5-subsets of a $(60u+4)$-set can be partitioned into $S(60; 4, 5, 60u+4)$ for all positive integers u such that $\gcd(u, 60) = 1$ or 2. (Sixty is the smallest value of λ for which an $S(\lambda; 4, 5, 60u+4)$ can exist.)

The new results in Section 3 use a theorem, which is implicit in [12]. However, unless one has a very good understanding of the techniques of [12], this is by no means obvious. Therefore, we give, in Section 4, a completely self-contained proof of this theorem.

* Research supported in part by NSA grant MDA904-88-H-2005.

0012-365X/89/$3.50

2. The existence of locally trivial t-designs without repeated blocks for arbitrary t

In this paper, we will assume all sets that are not obviously infinite, to be finite. If X is a set, then $P(X)$ is the set of all subsets of X, $P_k(X)$ the set of all k-subsets and $P_{k_1,k_2}(X)$ the set of all $B \in P(X)$ with $k_1 \leqslant |B| \leqslant k_2$. A *$t$-$X$-multiset* will be a function μ: $X \to \mathbb{N}$ such that $|\mu| = \sum_{x \in X} \mu(x) = t$. We call $\mu(x)$ the *multiplicity* of x. We call x an element of μ if $\mu(x) \neq 0$ and a repeated element if $\mu(x) \geqslant 2$. By the number of elements of μ having a given property, we will always mean the sum of the multiplicities of the elements having that property. A multiset without repeated elements will be identified with its set of elements. For instance, if X is a set and λ is a nonnegative integer, $\lambda \cdot X$ will denote the X-multiset defined by $(\lambda \cdot X)(x) = \lambda$ for all $x \in X$. If $Y \subset X$ and μ is an X-multiset, with $\mu \mid (X - Y) = 0$, we identify μ and $\mu \mid Y$. If μ is a $P(X)$-multiset, we will often call the elements of X *points* and the elements of μ *blocks*. An *isomorphism* between a $P(X_1)$-multiset μ_1 and a $P(X_2)$-multiset μ_2 will be a bijection $\sigma: X_1 \to X_2$ such that $\mu_1 = \mu_2 \circ \sigma$. (We identify σ with its canonical extension to $P(X_1)$.) If μ is a $P(X)$-multiset, we will denote the automorphism group of μ by $\mathrm{Aut}(\mu)$. If $Y \subset X$, we call a $P(X)$-multiset μ *Y-trivial* if $\mathcal{S}_Y \subset \mathrm{Aut}(\mu)$. We call μ *r-trivial* if μ is Y-trivial for some $Y \in P_r(X)$.

A *t-design* $S(\lambda; t, k, v)$, where λ, t, k and v are nonnegative integers with $t \leqslant k$, is a $P_k(S)$-multiset μ, $|S| = v$, such that every t-subset of S is contained in exactly λ elements of μ. For t-designs and related notions, we use the convention that if λ is not specified, we have $\lambda = 1$. Thus, we often write $S(t, k, v)$ instead of $S(1; t, k, v)$. A well known necessary condition for the existence of an $S(\lambda; t, k, v)$, $v \geqslant k$, $t > 0$, is that

$$\lambda \cdot \binom{v-i}{t-i} \Big/ \binom{k-i}{t-i}$$

should be an integer for all $i = 0, 1, \ldots, t-1$. If $k = t+1$, this simplifies to the condition that λ should be divisible by $\lambda(t, t+1, v) = \gcd(v - t, lcm\{1, \ldots, t+1\})$. The function $\lambda(t, t+1, v)$ will play an important role in the sequel.

A $t - S(\lambda; t, t+1, v)$, λ, t, $v \in \mathbb{N}$, $v \geqslant t+1$, will be a $P_{1,t+1}(X)$-multiset μ, $|X| = v - t$, such that, for every $A \in P_{0,t}(X)$, we have $(t + 1 - |A|)\mu(A) + \sum_{x \in X - A} \mu(A \cup \{x\}) = \lambda \cdot \binom{t}{|A|}$. (We put $\mu(\emptyset) = 0$.) If X is a set, if μ is a $P(X)$-multiset and if $X_1 \subset X$, then $\mu \parallel X_1$ will be the $P(X_1)$-multiset obtained by intersecting all elements of μ with X_1. If μ is an $S(\lambda; t, t+1, v)$, $v \geqslant t+1$, on a set S and if $X \in P_{v-t}(S)$, then $\mu \parallel X$ is a $t - S(\lambda; t, t+1, v)$. (Indeed, let $A \in P_{0,t}(X)$. Let ν be the submultiset of μ consisting of all B such that either $B \cap X = A$ or $B \cap X = A \cup \{x\}$, $x \in X - A$. Let ϵ be the $P_{t-|A|}(S - X)$-multiset obtained by replacing each B in ν by the elements of $P_{t-|A|}(B - X)$. If $B \cap X = A$, we have $|P_{t-|A|}(B - X)| = t + 1 - |A|$ and if $B \cap X = A \cup \{x\}$, $x \in X - A$, we have $|P_{t-|A|}(B - X)| = 1$. Thus $|\varepsilon| = (t + 1 - |A|)((\mu \parallel X)(A)) +$

$\sum_{x \in X-A} (\mu \parallel X)(A \cup \{x\})$. On the other hand, as μ is an $S(\lambda; t, t+1, v)$, we have $\varepsilon = \lambda \cdot P_{t-|A|}(S-X)$. Thus $|\varepsilon| = \lambda \cdot \binom{t}{t-|A|} = \lambda \cdot \binom{t}{|A|}$.)

An $\mathcal{S}_t - S(\lambda; t, t+1, v)$, λ, t, $v \in \mathbb{N}$, $v \geq t+1$, will be a $P_{1,t+1}(X)$-multiset ν, $|X| = v - t$, such that, for every $A \in P_{0,t}(X)$, we have $|A|\, \nu(A) + \sum_{x \in X-A} \nu(A \cup \{x\}) = \lambda$. (Again, we put $\nu(\emptyset) = 0$.) If μ is a Y-trivial $S(\lambda; t, t+1, v)$, $v \geq t+1$, on a set S, $|Y| = t$, then $\mu \parallel (S - Y)$ is a $t - S(\lambda; t, t+1, v)$ such that, for all $B \in P_{1,t+1}(S-Y)$, $(\mu \parallel (S-Y))(B)$ is divisible by

$$\binom{t}{t+1-|B|} = \binom{t}{|B|-1}.$$

If ε is a $t - S(\lambda; t, t+1, v)$ on a set X such that, for all $B \in P_{1,t+1}(X)$, $\varepsilon(B)$ is divisible by $\binom{t}{|B|-1}$, then the $P_{1,t+1}(X)$-multiset γ defined by $\gamma(B) = \varepsilon(B)/\binom{t}{|B|-1}$, is an $\mathcal{S}_t - S(\lambda; t, t+1, v)$. Finally, if ν is an $\mathcal{S}_t - S(\lambda; t, t+1, v)$ on a set X and if $Y \cap X = \emptyset$, $|Y| = t$, then the $P_{t+1}(X \cup Y)$-multiset μ defined by $\mu(B) = \nu(B \cap X)$ is a Y-trivial $S(\lambda; t, t+1, v)$. Thus, t-trivial $S(\lambda; t, t+1, v)$ and $\mathcal{S}_t - S(\lambda; t, t+1, v)$ are just two different ways of looking at the same structure and we will use the two completely interchangeably throughout this paper.

If t is positive integer, put $\lambda(t) = lcm\{\binom{t}{i};\ i = 1, \ldots, t\}$. The following proposition is an immediate consequence of the above remarks.

Proposition 1. *If μ is a $t - S(\lambda; t, t+1, v)$, $t \geq 1$, on a set X, then the $P_{1,t+1}(X)$-multiset μ^* defined by*

$$\mu^*(B) = \frac{\mu(B) \cdot \lambda(t)}{\binom{t}{|B|-1}}$$

is an $\mathcal{S}_t - S(\lambda \cdot \lambda(t);\ t,\ t+1,\ v)$.

If S and J are sets, S^J denotes the set of all functions from J to S. A (J, S)-array is an S^J-multiset. The elements of the array are called *rows* and the elements of J are called *columns*. The elements of S are called *entries*. A (J, S)-array is called *totally symmetric* if it is invariant under all permutations of J. An $\mathrm{RA}(\lambda; t, t+1, v)$, λ, t, $v \in \mathbb{N}$, will be a (J, S)-array μ, $|J| = t+1$, $|S| = v$, such that, for every $J_1 \in P_{0,t}(J)$ and $B \in S^{J_1}$, there are exactly λ rows R of μ with $R \mid J_1 = B$ and $|R(J - J_1)| = 1$. In [11, 12] an $\mathrm{RA}(\lambda; t, t+1, v)$ is called a regular $\mathrm{OA}(\lambda; t, t+1, v)$. A totally symmetric $\mathrm{RA}(\lambda; t, t+1, v)$ will be denoted by $\mathcal{S}_{\mathrm{RA}}(\lambda; t, t+1, v)$. The following proposition is straightforward (A proof can be found in [11], where a slightly different notation and terminology are used.)

Proposition 2. *Let J be a set, $|J| = t+1 \geq 2$. Let u be a positive integer. Put $\lambda = \lambda(t, t+1, u+t) = \gcd(u, lcm\{1, \ldots, t+1\})$. Put $\gamma_a = \{C \in \mathbb{Z}_u^J;\ \sum_{j \in J} C(j) \in \{\lambda a, \lambda a + 1, \ldots, \lambda a + \lambda - 1\}\}$, $a \in \{0, 1, \ldots, (u/\lambda) - 1\}$. Then, for all $a \in \{0, 1, \ldots, (u/\lambda) - 1\}$, γ_a is an $\mathcal{S}_{\mathrm{RA}}(\lambda; t, t+1, u)$ and $\sum_{a=0}^{(u/\lambda)-1} \gamma_a = \mathbb{Z}_u^J$.*

If $R \in S^J$, we can define a $|J| - S$-multiset R' by putting, for each $x \in S$, $R'(x) = |R^{-1}(x)|$. Let $M_t(S)$ be the set of all $t - S$-multisets. If μ is a totally symmetric (J, S)-array, then we can define an $M_{|J|}(S)$-multiset μ' by putting $\mu'(B) = \mu(R)$, where $R \in S^J$ and $R' = B$. (As μ is totally symmetric, $\mu(R)$ does not depend on the choice of R.) We can then go on and replace each multiset in μ' by its underlying set. This yields a $P_{1,|J|}(S)$-multiset μ''.

Proposition 3. *If μ is an $\mathcal{S}_{\mathrm{RA}}(\lambda; t, t+1, u)$, $u \geq 1$, then μ'' is a $t - S(\lambda; t, t+1, u+t)$.*

Proof. Let $A \in P_{0,t}(X)$, where X is the set of entries of μ. Let $b \notin X$. Intuitively, we think of b as a symbol meaning ⟪blank⟫ It is well known that the number of $(t - |A|) - (A \cup \{b\})$-multisets equals $\binom{t}{|A|}$. For every $(t - |A|) - (A \cup \{b\})$-multiset C there are exactly λ multisets in μ' that can be obtained by adding together A, all elements of C distinct from b and $C(b) + 1$ copies of some element x of X. Every element of μ' having $A \cup \{x\}$, $x \notin A$, as its underlying set can be obtained in this way from exactly one $(t - |A|) - (A \cup \{b\})$-multiset. On the other hand, an element of μ' having A as its underlying set is obtained from $t + 1 - |A|$ different $(t - |A|) - (A \cup \{b\})$-multisets. It follows that

$$(t + 1 - |A|)\mu''(A) + \sum_{x \in X - A} \mu''(A \cup \{x\}) = \lambda \cdot \binom{t}{|A|}.$$

Thus, μ'' is a $t - S(\lambda; t, t+1, u+t)$. □

Proposition 4. *For all positive integers u and t, there is a collection $(\mu_r)_{r \in R}$ of $\mathcal{S}_t - S(\lambda(t, t+1, u+t) \cdot \lambda(t); t, t+1, u+t)$ on a u-set X such that $\sum_{r \in R} \mu_r = \lambda(t) \cdot P_{1,t+1}(X)$ and such that, for every $B \in P_{1,t+1}(X)$, $\mu_r(B)$ is divisible by $\lambda(t)/\binom{t}{|B|-1}$.*

Proof. Let J be a $(t+1)$-set. By Proposition 2, there is a collection $(\gamma_r)_{r \in R}$, $R = \{0, 1, \ldots, (u/\lambda(t, t+1, u+t)) - 1\}$ of $\mathcal{S}_{\mathrm{RA}}(\lambda(t, t+1, u+t); t, t+1, u)$ such that $\sum_{r \in R} \gamma_r = \mathbb{Z}_u^J$. Put $X = \mathbb{Z}_u$ and $\mu_r = \gamma_r''^*$, where $*$ is defined as in Proposition 1. Then $(\mu_r)_{r \in R}$ satisfies all required properties. We only prove $\sum_{r \in R} \mu_r = \lambda(t) \cdot P_{1,t+1}(X)$, all other properties being easy consequences of Propositions 1 and 3. Let $B \in P_{1,t+1}(X)$. We have

$$\sum_{r \in R} \mu_r(B) = \sum_{r \in R} \gamma_r''^*(B) = \sum_{r \in R} \frac{\gamma_r''(B) \cdot \lambda(t)}{\binom{t}{|B|-1}} = \frac{\lambda(t)}{\binom{t}{|B|-1}} \sum_{r \in R} \gamma_r''(B).$$

As $\sum_{r \in R} \gamma_r = X^J$, we have $\sum_{r \in R} \gamma_r' = M_{t+1}(X)$. Thus $\sum_{r \in R} \gamma_r''(B)$ equals the number of $(t+1)$-B-multisets containing every element of B at least once, which equals the number of $(t + 1 - |B|) - B$-multisets, i.e. $\binom{t}{|B|-1}$. Thus $\sum_{r \in R} \mu_r(B) = \lambda(t)$. □

Putting $\varepsilon_r = \lambda_0 \cdot \mu_r$, where $(\mu_r)_{r\in R}$ satisfies the conditions of Proposition 4, yields

Proposition 5. *For all positive integers u, t and* λ_0, *there is a collection* $(\varepsilon_r)_{r\in R}$ *of* $\mathcal{S}_t - S(\lambda_0 \cdot \lambda(t, t+1, u+t)\cdot\lambda(t); t, t+1, u+t)$ *on a u-set X such that* $\sum_{r\in R}\varepsilon_r = \lambda_0\cdot\lambda(t)\cdot P_{1,t+1}(X)$ *and such that, for every* $B\in P_{1,t+1}(X)$, $\varepsilon_r(B)$ *is divisible by* $\lambda_0\cdot\lambda(t)/\binom{t}{|B|-1}$.

If v is a $P(X)$-multiset and $A\in P(X)$, then $|A|\, v(A) + \sum_{x\in X-A} v(A\cup\{x\}) = \sum_{x\in X} v(A\cup\{x\})$. We will often use this simple, but useful, observation implicitly when dealing with $\mathcal{S}_t - S(\lambda; t, t+1, v)$.

Proposition 6. *Let* $(\varepsilon_r)_{r\in R}$ *be a collection of* $\mathcal{S}_t - S(\lambda_r; t, t+1, u+t)$ *on a u-set X such that* $\sum_{r\in R}\varepsilon_r = wP_{1,t+1}(X)$, $w\geqslant 1$. *Assume that, for each* $B\in P_{1,t+1}(X)$ *a positive integer* $\lambda(B)$ *is given such that* $\lambda(B)$ *divides* $\varepsilon_r(B)$ *for all* $r\in R$. *Assume moreover that, for each* $B\in P_{1,t+1}(X)$, *there is a family* $(\gamma_l[B])_{l\in\mathbb{Z}_{w/\lambda(B)}}$ *of* $\mathcal{S}_{t+1-|B|} - S(\lambda(B); t+1-|B|, t+2-|B|, w+t+1-|B|)$ *on* $\mathbb{Z}_w$ *such that* $\sum_{l\in\mathbb{Z}_{w/\lambda(B)}}\gamma_l[B] = P_{1,t+2-|B|}(\mathbb{Z}_w)$.

Then there is a collection $(\mu_r)_{r\in R}$ *of* $\mathcal{S}_t - S(\lambda_r; t, t+1, uw+t)$ *on* $X\times\mathbb{Z}_w$ *such that* $\sum_{r\in R}\mu_r = P_{1,t+1}(X\times\mathbb{Z}_w)$. *Consequently, if Y is a t-set with* $Y\cap(X\times\mathbb{Z}_w)=\emptyset$, *then there is a collection* $(\nu_r)_{r\in R}$ *of Y-trivial* $S(\lambda_r; t, t+1, uw+t)$ *on* $(X\times\mathbb{Z}_w)\cup Y$ *whose blocks partition* $P_{t+1}((X\times\mathbb{Z}_w)\cup Y)$.

Proof. Choose, for each $B\in P_{1,t+1}(X)$, a family $(\delta_r[B])_{r\in R}$ of pairwise disjoint $(\varepsilon_r(B)/\lambda(B))$-subsets of $\mathbb{Z}_{w/\lambda(B)}$ whose union is $\mathbb{Z}_{w/\lambda(B)}$. If $C\in P(X\times\mathbb{Z}_w)$, let $B(C)$ be the set of all $x\in X$ such that there is an element i of $\mathbb{Z}_w$ with $(x,i)\in C$. For every $x\in X$, let C_x be the set of all $i\in\mathbb{Z}_w$ with $(x,i)\in C$. If $C\in P_{1,t+1}(X\times\mathbb{Z}_w)$ and $x\in B(C)$, then, as $\sum_{l\in\mathbb{Z}_{w/\lambda(B(C))}}\gamma_l[B(C)] = P_{1,t+2-|B(C)|}(\mathbb{Z}_w)$ and $C_x\in P_{1,t+2-|B(C)|}(\mathbb{Z}_w)$, there is a unique element $l(C,x)$ of $\mathbb{Z}_{w/\lambda(B(C))}$ such that $C_x\in\gamma_{l(C,x)}[B(C)]$. Let μ_r be the set of all $C\in P_{1,t+1}(X\times\mathbb{Z}_w)$ such that $\sum_{x\in B(C)} l(C,x)\in\delta_r[B(C)]$.

For each $C\in P_{1,t+1}(X\times\mathbb{Z}_w)$, there is exactly one $r\in R$ such that $\sum_{x\in B(C)} l(C,x)\in\delta_r[B(C)]$ and thus, exactly one $r\in R$ such that $C\in\mu_r$. Thus $\sum_{r\in R}\mu_r = P_{1,t+1}(X\times\mathbb{Z}_w)$.

It remains to be proved that each μ_r is an $\mathcal{S}_t - S(\lambda_r;\ t,\ t+1,\ uw+t)$. Let $A\in P_{0,t}(X\times\mathbb{Z}_w)$. Obviously, $B(A)\in P_{0,t}(X)$ and we have $\sum_{x\in X}\varepsilon_r(B(A)\cup\{x\}) = \lambda_r$. Let $x\in X$. We want to count the number of $i\in\mathbb{Z}_w$ such that $A\cup\{(x,i)\}\in\mu_r$. If $i\in\mathbb{Z}_w$, then $B(A\cup\{(x,i)\}) = B(A)\cup\{x\}$, $(A\cup\{(x,i)\})_x = A_x\cup\{i\}$ and $(A\cup\{(x,i)\})_y = A_y$ for all $y\in B(A)-\{x\}$. The first and third equalities show that $\sum_{y\in B(A)-\{x\}} l(A\cup\{(x,i)\}, y)$ is independent of i. Put $\sum_{y\in B(A)-\{x\}} l(A\cup\{(x,i)\}, y) = l_0(x)$. We have $A\cup\{(x,i)\}\in\mu_r$ iff $l(A\cup\{(x,i)\}, x) + l_0(x)\in\delta_r[B(A)\cup\{x\}]$. There are $|\delta_r[B(A)\cup\{x\}]| = \varepsilon_r(B(A)\cup\{x\})/\lambda(B(A)\cup\{x\})$ elements l of $\mathbb{Z}_{w/\lambda(B(A)\cup\{x\})}$ such that $l + l_0(x)\in\delta_r[B(A)\cup\{x\}]$. For each such l, we have $\sum_{i\in\mathbb{Z}_w}(\gamma_l[B(A)\cup\{x\}])(A_x\cap\{i\}) = \lambda(B(a)\cup\{x\})$.

Remember that $\gamma_l[B(A)\cup\{x\}]$ is a set. (This follows from $\sum_{l\in\mathbb{Z}_{w/\lambda(B(A)\cup\{x\})}}\gamma_l[B(A)\cup\{x\}]=P_{1,t+2-|B(A)\cup\{x\}|}(\mathbb{Z}_w)$.) Thus, for each of the obtained l, there are exactly $\lambda(B(A)\cup\{x\})$ elements i of $\mathbb{Z}_w$ such that $A_x\cup\{i\}\in\gamma_l[B(A)\cup\{x\}]$, i.e. such that $l(A\cup\{(x,i)\},x)=l$. It follows that, for each $x\in X$, there are exactly $\varepsilon_r(B(A)\cup\{x\})$ elements i of $\mathbb{Z}_w$ such that $A\cup\{(x,i)\}\in\mu_r$. Thus $\sum_{(x,i)\in X\times\mathbb{Z}_w}\mu_r(A\cup\{(x,i)\})=\sum_{x\in X}\varepsilon_r(B(A)\cup\{x\})=\lambda_r$. □

A *large set of disjoint* $S(\lambda;t,k,v)$, briefly LS$(\lambda;t,k,v)$, is a collection $(\mu_l)_{l\in L}$ of $S(\lambda;t,k,v)$ on a v-set S, $v\geq k$, such that $\sum_{l\in L}\mu_l=P_k(S)$. An LS$(\lambda;t,k,v)$ is called Y-trivial if all its members are Y-trivial. Because of the remarks preceding Proposition 1, it is obvious that t-trivial LS$(\lambda;t,t+1,v)$ and collections $(\mu_r)_{r\in R}$ of $\mathcal{S}_t-S(\lambda;t,t+1,v)$ on a $(v-t)$-set X satisfying $\sum_{r\in R}\mu_r=P_{1,t+1}(X)$, are just two different ways of looking at the same structure.

Put $\lambda^*(t)=lcm\{1,\ldots,t+1\}$ and, for $t\geq 1$, $l(t)=\prod_{i\in\{1,\ldots,t\}}\lambda(i)\cdot\lambda^*(i)$. By convention, we put $l(0)=1$.

Proposition 7. *If* $v\equiv t\pmod{l(t)}$, $v\geq t+1$, *then there is a t-trivial* LS$(l(t);t,t+1,v)$.

Proof. For every v-set S, $v\geq 1$, there is exactly one LS$(0,1,v)$ on S, namely $\{\{s\};s\in S\}$. Thus, the proposition is true for $t=0$. Assume that $t\geq 1$ and that the proposition is true for all t_1, $0\leq t_1<t$. Put $u=(v-t)/(l(t-1)\cdot\lambda(t))$. As $u\equiv 0\pmod{\lambda^*(t)}$, we have $\lambda(t,t+1,u+t)=\lambda^*(t)$. Applying Proposition 5 with $\lambda_0=l(t-1)$ yields a collection $(\varepsilon_r)_{r\in R}$ of $\mathcal{S}_t-S(l(t);t,t+1,u+t)$ on a u-set X such that $\sum_{r\in R}\varepsilon_r=l(t-1)\cdot\lambda(t)\cdot P_{1,t+1}(X)$ and such that for every $B\in P_{1,t+1}(X)$, $\varepsilon_r(B)$ is divisible by $l(t-1)\cdot\lambda(t)/\binom{t}{|B|-1}$. Applying Proposition 6 with $w=l(t-1)\cdot\lambda(t)$ yields Proposition 7. (If $B\in P_{2,t+1}(X)$, put $\lambda(B)=l(t+1-|B|)$. The existence of the $\gamma_l[B]$ follows by induction. If $B\in P_1(X)$, put $\lambda(B)=w$ and put $\gamma_0[B]=P_{1,t+1}(\mathbb{Z}_w)$.) □

Obviously, $\lambda(t)$ divides $t!$ and $\lambda^*(t)$ divides $(t+1)!$. As $t_1!$ divides $t!$ for all $t\geq t_1$, as $l(0)=1$, $l(1)=2$ and, for $t\geq 1$, $l(t)=\lambda(t)\cdot\lambda^*(t)\cdot l(t-1)$, it is easy to see that $l(t)$ divides $(t+1)!^{(2t-1)}$ for all t. Thus Proposition 7 implies Proposition 4.3 of [12].

3. Smaller values of λ and $(t,t+1,v)$-decompositions

If we want to find smaller values of λ, the following is a better tool than Proposition 6.

Proposition 8. *Let* $(\varepsilon_r)_{r\in R}$ *be a collection of* $\mathcal{S}_t-S(\lambda;t,t+1,u+t)$ *on a u-set X such that* $\sum_{r\in R}\varepsilon_r=w\cdot P_{1,t+1}(X)$, $w\geq 1$. *Assume that, for each* $B\in P_{1,t+1}(X)$, *a* *positive integer $\lambda(B)$ is given such that $\lambda(B)$ divides $\varepsilon_r(B)$ for all $r \in R$. Assume that, for each $B \in P_{1,t+1}(X)$, there is an* $\mathrm{LS}(\lambda(B); t+1-|B|, t+2-|B|, w+t+1-|B|)$. *Then there is an* $\mathrm{LS}(\lambda; t, t+1, uw+t)$.

Proposition 8 is implicit in [12]. However, unless one has a very good understanding of the techniques of [12], this is by no means obvious. Therefore we will give, in Section 4, a completely self-contained proof of Proposition 8. Actually, we will prove a slightly more general result. The difference between Proposition 6 and Proposition 8 is that, in Proposition 8, the $\mathrm{LS}(\lambda(B); t+1-|B|, t+2-|B|, w+t+1-|B|)$ do not have to be $(t+1-|B|)$-trivial. We pay for this by the fact that the obtained $\mathrm{LS}(\lambda; t, t+1, uw+t)$ will not necessarily be t-trivial. We are, however, more interested in getting reasonably small λ than in t-triviality. Although we defer the proof of Proposition 8 to Section 4, we will give some examples of its usefulness in the present section.

If μ is a $P(X)$-multiset and $A \subset X$, we will denote by μ_A the $P(X-A)$-multiset whose blocks are the intersections with $X-A$ of the blocks of μ containing A. We say that μ_A is *derived* from μ. Let $A \in P_{0,t}(X)$. If μ is an $S(\lambda; t, k, v)$ on X, then μ_A is an $S(\lambda; t-|A|, k-|A|, v-|A|)$ on $X-A$. If $(\mu_r)_{r\in R}$ is an $\mathrm{LS}(\lambda; t, k, v)$ on X, then $(\mu_{rA})_{r\in R}$ is an $\mathrm{LS}(\lambda; t-|A|, k-|A|, v-|A|)$ on $X-A$.

Proposition 8 has the following corollary.

Proposition 9. *If an* $\mathrm{LS}(\lambda; t, t+1, w+t)$ *exists, then an* $\mathrm{LS}(\lambda u; t, t+1, uw+t)$ *exists for all positive integers u.*

Proof. Let X be a u-set. Let R be a (w/λ)-set. Put $\varepsilon_r = \lambda \cdot P_{1,t+1}(X)$ for all $r \in R$. Then $(\varepsilon_r)_{r\in R}$ is a collection of $\mathcal{S}_t - S(\lambda u; t, t+1, u+t)$ and $\sum_{r\in R} \varepsilon_r = w \cdot P_{1,t+1}(X)$. For each $B \in P_{1,t+1}(X)$, choose $\lambda(B) = \lambda$. The existence of an $\mathrm{LS}(\lambda; t, t+1, w+t)$ implies, as noted above, the existence of an $\mathrm{LS}(\lambda(B); t+1-|B|, t+2-|B|, w+t+1-|B|)$. Thus, Proposition 9 follows from Proposition 8. □

A $(t, t+1, v)$-decomposition, $v \geq t+1$, will be an $\mathrm{LS}(\lambda(t, t+1, v); t, t+1, v)$. *Trivial* $(t, t+1, v)$-decompositions consisting of a single $S(v-t; t, t+1, v)$ exist for all $v = t + \lambda_0$, where λ_0 divides $\lambda^*(t) = lcm\{1, \ldots, t+1\}$. It is well known that $(1, 2, v)$-decompositions exist for all v. Indeed, if v is even (odd, respectively), a $(1, 2, v)$-decomposition is the same thing as a 1-factorization (2-factorization, respectively), of the complete graph on v vertices. In [9, 10, 11] $(2, 3, v)$-decompositions are constructed for all $v \equiv 0$, 2, 4 or 5 (mod 6). A $(2, 3, 7)$-decomposition does not exist [1]. For $v = 141$, 283, 501, 789, 1501 and 2365, the existence of a $(2, 3, v)$-decomposition is still open. For all other $v \equiv 1$ or 3 (mod 6), $(2, 3, v)$-decompositions are known [5, 6, 8]. There are no $(3, 4, v)$-decompositions for $v = 8$ or 10 [3]. On the other hand, $(3, 4, v)$-decompositions exist for all $v \equiv 0 \pmod 3$, $v > 3$ [11]. To the author's best knowledge, the only

$v \equiv 1$ or $2 \pmod 3$ for which a $(3,4,v)$-decomposition is known are $v = 4$, 5, 7 (these are all trivial decompositions) and 11 (see below).

With the aid of a computer, Kreher and Radziszowski [4] constructed a $(6,7,14)$-decomposition. By Proposition 9, this yields $(6, 7, v)$-decompositions for $v = 30$, 46, 62, 126, 174, 286 and 846. The derived designs yield $(5, 6, v)$-decompositions for $v = 13$, 29, 45 and 125. They give $(4,5,v)$-decompositions for $v = 12$, 28, 44 and 124. (A $(4,5,12)$-decomposition was also constructed earlier, in a simpler way, without use of a computer, by Denniston [2]. The values $v = 28$, 44 and 124 can also be obtained by applying Proposition 9 to Denniston's decomposition.) Further derivation yields $(3,4,v)$-decompositions for $v = 11$ and 27. (Note that 27 can also be obtained from [11], but 11 cannot.)

Using the above mentioned results about $(1,2,v)$-, $(2,3,v)$- and $(3,4,v)$-decompositions, it is easy to check that applying Proposition 8 to Proposition 5 with $\lambda_0 = 12$ and $t = 4$, yields, for all positive integers u, an LS$(144\lambda(4, 5, u+4)$; 4, 5, $144u + 4)$. As $\lambda^*(4) = 60$, this never gives a $(4,5,v)$-decomposition. Using this result, we can now see that applying Proposition 8 to Proposition 5 with $\lambda_0 = 360$ and $t = 5$ gives, for all positive integers u, an LS$(3600\lambda(5, 6, u+5)$; 5, 6, $3600u + 5)$. As $\lambda^*(5) = 60$, this again never yields a $(5, 6, v)$-decomposition. Of course, we can continue this indefinitely. This will yield smaller values of λ than Proposition 7, but nevertheless, the smallest value of λ we obtain in this way, grows extremely quickly as a function of t.

For $t = 4$, we can do better. Applying Proposition 5 with $t = 5$ yields, for all positive integers λ_0 and u, a collection $(\varepsilon_r)_{r\in R}$ of $\mathcal{S}_5 - S(\lambda_0 \cdot \lambda(5, 6, u+5) \cdot 10;\ 5,\ 6,\ u+5)$ such that $\sum_{r\in R} \varepsilon_r = \lambda_0 \cdot 10 \cdot P_{1,6}(X)$ and such that, for every $B \in P_{1,6}(X)$, $\varepsilon_r(B)$ is divisible by $\lambda_0 \cdot 10/\binom{5}{|B|-1}$. Then $(\varepsilon_r \mid P_{1,5}(X))_{r\in R}$ is a collection of $\mathcal{S}_4 - S(\lambda_0 \cdot \lambda(5, 6, u+5) \cdot 10;\ 4,\ 5,\ u+4)$ such that $\sum_{r\in R} \varepsilon_r = \lambda_0 \cdot 10 \cdot P_{1,5}(X)$. Notice that, as $\lambda^*(5) = \lambda^*(4) = 60$, we have $\lambda(5, 6, u+5) = \lambda(4, 5, u+4)$. Choosing $\lambda_0 = 6$ and applying Proposition 8 to $(\varepsilon_r \mid P_{1,5}(X))_{r\in R}$ yields an LS$(60 \cdot \lambda(4, 5, u+4)$; 4, 5, $60u + 4)$ for all positive integers u. This shows that a $(4, 5, 60u + 4)$-decomposition exists for all positive integers u such that $\lambda(4, 5, u+4) = 1$, i.e. such that $\gcd(u, 30) = 1$. (Note that if, as is likely, a $(3,4,23)$-decomposition exists, then we can choose, in the above, $\lambda_0 = 2$ and obtain an LS$(20 \cdot \lambda(4, 5, u+4)$; 4, 5, $20u + 4)$ for all positive integers u. This would yield $(4,5,20u + 4)$-decompositions for all positive integers u such that $\lambda(4, 5, u+4) = 1$. The existence of a $(3,4,23)$-decomposition is, however, still open.) Using the previous result, we can now see that applying Proposition 8 to Proposition 5 with $\lambda_0 = 300$ and $t = 5$ yields for all positive integers u, an LS$(3000\lambda(5, 6, u+5)$; 5, 6, $3000u + 5)$. This again never gives a $(5,6,v)$-decomposition.

We can, in the above, take two copies of $\varepsilon_r \mid P_{1,5}(X)$ for each $r \in R$. This yields a collection of $\mathcal{S}_4 - S(10\lambda_0\lambda(4, 5, u+4);\ 4, 5, u+4)$ such that $\sum_{r\in R} \varepsilon_r = 20\lambda_0 P_{1,5}(X)$ and such that, for every $B \in P_{1,5}(X)$, $\varepsilon_r(B)$ is divisible by $10\lambda_0/\binom{5}{|B|-1}$. Choosing $\lambda_0 = 6$ and applying Proposition 8, yields, using the existence, deduced above, of a $(4, 5, 124)$-decomposition, an $\mathrm{LS}(60\lambda(4, 5, u+4); 4, 5, 120u+4)$ for all $u \in \mathbb{N} - \{0\}$. Combined with the above, this shows that a $(4, 5, 60u+4)$-decomposition exists for all positive integers u such that $\gcd(u, 60) = 1$ or 2. (Again, if a $(3, 4, 43)$-decomposition exists, we can choose $\lambda_0 = 2$ and get, using the existence of a $(4, 5, 44)$-decomposition, $\mathrm{LS}(20\lambda(4, 5, u+4); 4, 5, 40u+4)$ for all $u \in \mathbb{N} - \{0\}$. These would yield $(4, 5, 40u+4)$-decompositions for all positive integers u such that $\gcd(u, 30) = 1$. The existence of a $(3, 4, 43)$-decomposition is still in doubt.)

To our best knowledge, the only known infinite family of non-trivial $(t, t+1, v)$-decompositions with $t \geq 4$ are the $(4, 5, 60u+4)$-decompositions constructed above for all positive integers u with $\gcd(u, 60) = 1$ or 2. A finite amount of further non-trivial $(t, t+1, v)$-decompositions with $4 \leq t \leq 6$ can be obtained, as explained above, by combining [4] with Proposition 9. We do not know any other non-trivial $(t, t+1, v)$-decompositions for $t \geq 4$. In particular, we do not know any single non-trivial $(t, t+1, v)$-decomposition for $t \geq 7$.

4. A proof of Proposition 8

If μ is a multiset, then $s(\mu)$ will denote the underlying set of μ, i.e. $s(\mu) = \{x; x \in \mu\}$.

Let S be a set and let δ be a $k - P(S)$-multiset such that $s(\delta)$ is a partition of S. An $S(\lambda; t, k, \delta)$, $t \leq k$, will be a $P_k(S)$-multiset μ such that, for every $B \in \mu$ and $A \in \delta$, we have $|A \cap B| = \delta(A)$ and such that, for every $T \in P_t(S)$ satisfying $|A \cap T| \leq \delta(A)$ for all $A \in \delta$, there are exactly λ blocks of μ containing T. A *large set of disjoint* $S(\lambda; t, k, \delta)$, briefly $\mathrm{LS}(\lambda; t, k, \delta)$, is a collection $(\mu_r)_{r \in R}$ of $S(\lambda; t, k, \delta)$ such that $\sum_{r \in R} \mu_r$ equals the set of all k-subsets B of S with $|B \cap A| = \delta(A)$ for all $A \in \delta$. If δ consists of k copies of S, then the $(L)S(\lambda; t, k, \delta)$ are exactly the $(L)S(\lambda; t, k, |S|)$ on S.

If S is a set, then a (w, t, S)-partition, or more briefly (w, t)-partition, $w \geq 1$, will be a $(t+1) - P(S)$-multiset δ such that $s(\delta)$ is a partition of S and such that, for every $A \in \delta$, we have $|A| = w + \delta(A) - 1$. For instance, if δ consists of $t+1$ copies of S, $|S| \geq t+1$, then δ is a $(|S| - t, t, S)$-partition. (For readers familiar with [12], note that what we call here a (w, t, S)-partition is equivalent with what is called a (w, J, S)-partition in [12], where J is a $(t+1)$-set. An $\mathrm{LS}(\lambda; t, t+1, \delta)$, δ a (w, t, S)-partition, is equivalent with a $Z(\lambda; J, F)(\mu_l)_{l \in L}$, F a (w, J, S)-partition, $|J| = t+1$, satisfying $H(\mu_l) = H(F)$ for all $l \in L$. When we say that two types of structures are equivalent, we mean that they are formally different, but that there is an obvious way to identify a structure of one type with a structure of the other type.)

Much more can be proved about $S(\lambda; t, k, \delta)$ than we will do here. We will study $S(\lambda; t, k, \delta)$ and $\mathrm{LS}(\lambda; t, k, \delta)$ in more detail in a subsequent publication. In this paper, we will essentially only prove those results about $S(\lambda; t, k, \delta)$ that we will actually use.

First, note that if $(\mu_r)_{r\in R}$ is an $\mathrm{LS}(\lambda; t, t+1, \delta)$, δ a (w, t, S)-partition, then $|R| = w/\lambda$. (Indeed, let T be a t-subset of S with $|A_0 \cap T| = \delta(A_0) - 1$ for a given $A_0 \in s(\delta)$ and $|A \cap T| = \delta(A)$ for all $A \in s(\delta) - \{A_0\}$. There are exactly $|A_0| - (\delta(A_0) - 1) = w + \delta(A_0) - 1 - (\delta(A_0) - 1) = w$ $(t+1)$-subsets B of S with $T \subset B$ and $|A \cap B| = \delta(A)$ for all $A \in \delta$. Each of the μ_r contains λ of these $(t+1)$-sets and each of these $(t+1)$-sets is contained in exactly one μ_r, giving $|R| = w/\lambda$.)

Proposition 10. *Let δ be a (w, t, S)-partition and put $m = \max\{\delta(A); A \in \delta\}$. If an $\mathrm{LS}(\lambda; m-1, m, w+m-1)$ exists, then an $\mathrm{LS}(\lambda; t, t+1, \delta)$ exists.*

Proof. For every $A \in \delta$, put an $\mathrm{LS}(\lambda; \delta(A) - 1, \delta(A), w + \delta(A) - 1)(\mu_{(i,A)})_{i\in\mathbb{Z}_{w/\lambda}}$ on A. (As noticed in Section 3, the existence of an $\mathrm{LS}(\lambda; m-1, m, w+m-1)$ implies the existence of an $\mathrm{LS}(\lambda; \delta(A) - 1, \delta(A), w + \delta(A) - 1)$.) Let γ_r, $r \in \mathbb{Z}_{w/\lambda}$, be the set of all $(t+1)$-subsets B of S such that $|A \cap B| = \delta(A)$ for all $A \in \delta$ and such that $\sum_{A\in s(\delta)} i_{A,B} = r$, where $i_{A,B}$ is the uniquely determined element of $\mathbb{Z}_{w/\lambda}$ with $A \cap B \in \mu_{(i_{A,B}, A)}$. It is immediately clear from the definition of γ_r that $\sum_{r\in\mathbb{Z}_{w/\lambda}} \gamma_r$ is the set of all $(t+1)$-subsets B of S such that $|A \cap B| = \delta(A)$ for all $A \in \delta$. It remains to be proved that each γ_r is an $S(\lambda; t, t+1, \delta)$. Let T be a t-subset of S such that $|T \cap A_0| = \delta(A_0) - 1$ for some given $A_0 \in \delta$ and $|T \cap A| = \delta(A)$ for all $A \in s(\delta) - \{A_0\}$. For each $A \in s(\delta) - \{A_0\}$, let i_A be the uniquely determined element of $\mathbb{Z}_{w/\lambda}$ with $A \cap T \in \mu_{(i_A, A)}$. The blocks of γ_r containing T are the $(t+1)$-sets B containing T and a further point of A_0 such that $B \cap A_0 \in \mu_{(i_0, A_0)}$, where $i_0 = r - \sum_{A\in s(\delta)-\{A_0\}} i_A$. The number of such blocks equals the number of blocks of $\mu_{(i_0, A_0)}$ containing the $(\delta(A_0) - 1)$-set $T \cap A_0$. As $\mu_{(i_0, A_0)}$ is an $S(\lambda; \delta(A_0) - 1, \delta(A_0), w + \delta(A_0) - 1)$, this number equals λ. Thus, $(\gamma_r)_{r\in\mathbb{Z}_{w/\lambda}}$ is an $\mathrm{LS}(\lambda; t, t+1, \delta)$. $\square$

In the following, we will often describe a multiset by a collection of elements between square brackets. For instance, $[x, x, x, y, z, z]$ denotes the $\{x, y, z\}$-multiset μ defined by $\mu(x) = 3$, $\mu(y) = 1$ and $\mu(z) = 2$. The square brackets are used to avoid confusion with ordered or unordered sets.

If X is a set, then, as in Section 2, $M_k(X)$ will denote the set of all $k-X$-multisets. Let $(X, \leq)$ be a totally ordered set, $X \cap \{1, \ldots, t\} = \phi$. If μ is a $(t+1)-X$-multiset, then μ^* will denote the set of all $(t+1)-(X \cup \{1, \ldots, t\})$-multisets obtained by listing all elements of μ in increasing order and then replacing some elements in μ by the position in which they occur, where we never replace the last (i.e. most to the right) occurrence of an element. For instance, if $t = 5$, if $X = \{a, b, c, d\}$, $a < b < c < d$ and if $\mu = [a, a, a, c, d, d]$, then $\mu^* = \{[a, a, a, c, d, d], [1, a, a, c, d, d], [a, 2, a, c, d, d] [1, 2, a, c, d, d], [a, a, a, c, 5, d], [1, a, a, c, 5, d], [a, 2, a, c, 5, d], [1, 2, a, c, 5, d]\}$. Note that, as we must keep the last occurrence of all $x \in \mu$, we have $s(\nu) \cap X = s(\mu)$ for all $\nu \in \mu^*$. We will denote by $N_\mu(x)$ the set of all positions occupied by x in μ except the last position, where we again assume that the elements of μ are listed in increasing order. In our example, $N_\mu(a) = \{1, 2\}$, $N_\mu(b) = \phi$, $N_\mu(c) = \phi$ and $N_\mu(d) = \{5\}$.

Proposition 11. *Let $(X, \leq)$ be a totally ordered set, $X \cap \{1, \ldots, t\} = \phi$. Then for every $(t+1) - (X \cup \{1, \ldots, t\})$-multiset v with $v(i) \leq 1$ for all $i \in \{1, \ldots, t\}$, there is exactly one element μ of $M_{t+1}(X)$ such that $v \in \mu^*$.*

Proof. Put all $i \in \{1, \ldots, t\} \cap s(v)$ in position i. Fill out the remaining positions of v by listing the remaining elements of v in increasing order. It is easy to see that there is one and only one element μ of $M_{t+1}(X)$ with $v \in \mu^*$, namely the μ obtained by replacing each $i \in \{1, \ldots, t\}$ by the first element of X occurring to the right of i in v. □

To illustrate the procedure described in the proof of Proposition 11, let $t = 7$, let $X = \{a, b, c, d, e\}$, $a < b < c < d < e$ and let $v = [a, a, b, d, 1, 3, 6, 7]$. We write $v = [1, a, 3, a, b, 6, 7, d]$ and put $\mu = [a, a, a, a, b, d, d, d]$.

Proposition 12. *Let $(\mathscr{E}_r)_{r \in R}$ be a collection of $\mathscr{S}_t - S(\lambda_r; t, t+1, u+t)$ on a u-set X, $X \cap \{1, \ldots, t\} = \phi$, such that $\sum_{r \in R} \mathscr{E}_r = w \cdot P_{1,t+1}(X)$, $w \geq 1$. Assume that, for each $B \in P_{1,t+1}(X)$, a positive integer $\lambda(B)$ is given such that $\lambda(B)$ divides $\mathscr{E}_r(B)$ for all $r \in R$. Assume moreover that, for each $B \in P_{1,t+1}(X)$, there is an $\mathrm{LS}(\lambda(B); t+1-|B|, t+2-|B|, w+t+1-|B|)$. Then there is a collection $(\gamma_r)_{r \in R}$ of $S(\lambda_r; t, t+1, uw+t)$ without repeated blocks on $(X \times \mathbb{Z}_w) \cup \{1, \ldots, t\}$ such that $\sum_{r \in R} \gamma_r = P_{t+1}((X \times \mathbb{Z}_w) \cup \{1, \ldots, t\})$.*

Proof. Put a total order $(X, \leq)$ on X. Let $S = (X \times \mathbb{Z}_w) \cup \{1, \ldots, t\}$. For each $\mu \in M_{t+1}(X)$, let δ_μ be the (w, t)-partition obtained by replacing each occurrence of x in μ by $(\{x\} \times \mathbb{Z}_w) \cup N_\mu(x)$. Put $B_0 = s(\mu)$. Put $m = \max\{\delta_\mu(A); A \in \delta_\mu\}$. We have $m = \max\{\mu(x); x \in B_0\} \leq t + 2 - |B_0|$. As an $\mathrm{LS}(\lambda(B_0); t+1-|B_0|, t+2-|B_0|, w+t+1-|B_0|)$ exists, this means that an $\mathrm{LS}(\lambda(B_0); m-1, m, w+m-1)$ exists. By Proposition 10, this implies the existence of an $\mathrm{LS}(\lambda(B_0); t, t+1, \delta_\mu)(\alpha_{(\mu,i)})_{i \in \{1,\ldots,w/\lambda(B_0)\}}$. Choose a family $(\Pi_r[B_0])_{r \in R}$ of pairwise disjoint $(\mathscr{E}_r(B_0)/\lambda(B_0))$-subsets of $\{1, \ldots, w/\lambda(B_0)\}$ whose union is $\{1, \ldots, w/\lambda(B_0)\}$. Put $\beta_{(\mu,r)} = \sum_{i \in \Pi_r[B_0]} \alpha_{(\mu,i)}$. Obviously, $(\beta_{(\mu,r)})_{r \in R}$ is a collection of $S(\mathscr{E}_r(B_0); t, t+1, \delta_\mu)$ such that $\sum_{r \in R} \beta_{(\mu,r)}$ equals the set of all $(t+1)$-subsets D of S with $|A \cap D| = \delta_\mu(A)$ for all $A \in \delta_\mu$. Put $\gamma_r = \sum_{\mu \in M_{t+1}(X)} \beta_{(\mu,r)}$.

We first prove that $\sum_{r \in R} \gamma_r = P_{t+1}(S)$. Let $D \in P_{t+1}(S)$. Let $v\langle D \rangle$ be the $(t+1)$-$(X \cup \{1, \ldots, t\})$-multiset obtained from D by replacing each $(x, y) \in D \cap (X \times \mathbb{Z}_w)$ by x. We have seen that, if $\mu \in M_{t+1}(X)$, then $\sum_{r \in R} \beta_{(\mu,r)}$ is a set and it is easy to check that D is in this set iff $v\langle D \rangle \in \mu^*$. By Proposition 11, there is exactly one $\mu \in M_{t+1}(X)$ with $v\langle D \rangle \in \mu^*$. Thus, $(\sum_{r \in R} \gamma_r)(D) = 1$.

It only remains to be proved that each γ_r is an $S(\lambda_r; t, t+1, uw+t)$. (The fact that the γ_r have no repeated blocks is an immediate consequence of $\sum_{r \in R} \gamma_r = P_{t+1}(S)$.)

Let $r \in R$ and let $E \in P_t(S)$. Let ν be the $t-(X \cup \{1, \ldots, t\})$-multiset obtained from E by replacing every element (x, y) of $E \cap (X \times \mathbb{Z}_w)$ by x. For any $\mu \in M_{t+1}(X)$ such that $\beta_{(\mu,r)}$ contains a block D with $E \subset D$, the set μ^* contains some ν_1 with $\nu \leqslant \nu_1$. (For instance, choose $\nu_1 = \nu\langle D\rangle$, where $\nu\langle D\rangle$ is defined as above.) For every $\mu \in M_{t+1}(X)$ such that μ^* contains some ν_1 with $\nu \leqslant \nu_1$, we have $|A \cap E| \leqslant \delta_\mu(A)$ for all $A \in \delta_\mu$ and there are exactly $\mathscr{E}_r(s(\mu))$ elements of $\beta_{(\mu,r)}$ containing E. If $x \in X$, Then, by Proposition 11, there is a unique $(t+1)-X$-multiset $\mu[x]$ with $\nu + \{x\} \in \mu[x]^*$. On the other hand, if $\mu \in M_{t+1}(X)$ and if there is a $\nu_1 \in \mu^*$ with $\nu \leqslant \nu_1$, then there is one and only one $x \in X$ such that $\mu = \mu[x]$, i.e. such that $\nu + \{x\} \in \mu^*$. (If $\nu_1 = \nu + \{i\}$, $i \in \{1, \ldots, t\}$, then x is the unique element of μ with $i \in N_\mu(x)$.) It follows that the elements of γ_r containing E are the elements of $\sum_{x \in X} \beta_{(\mu[x],r)}$ containing E. There are $\sum_{x \in X} \mathscr{E}_r(s(\mu[x])) = \sum_{x \in X} \mathscr{E}_r(B \cup \{x\})$ such elements, where $B = S(\nu) \cap X$. As $\mathscr{E}_r$ is an $\mathscr{S}_t - S(\lambda_r; t, t+1, u+t)$, we have $\sum_{x \in X} \mathscr{E}_r(B \cup \{x\}) = \lambda_r$. $\square$

Proposition 8 can be obtained from Proposition 12 by putting $\lambda_r = \lambda$ for all $r \in R$.

Note added in proof. A $(3, 4, 23)$-decomposition was recently constructed by Chee, Colbourn and Kreker.

References

[1] A. Cayley, On the triadic arrangements of seven and fifteen things, London, Edinburgh and Dublin Philos. Mag. and J. Si. (3) 37 (1850) 50–53.

[2] R.H.F. Denniston, A small 4-design, Annals Discrete Math. 18 (1983) 291–294.

[3] E.S. Kramer and D.M. Mesner, Intersections among Steiner systems, J. Combin. Theory Ser. A 16 (1974) 273–285.

[4] D.L. Kreher and S.P. Radziszowski, The existence of simple 6-(14, 7, 4) designs, J. Combin. Theory Ser. A 43 (1986) 237–243.

[5] J.X. Lu, On large sets of disjoint Steiner triple systems I, II and III, J. Combin. Theory, Ser. A 34 (1983) 140–146, 147–155 and 156–182.

[6] J.X. Lu, On large sets of disjoint Steiner triple systems, IV, V and VI, J. Combin. Theory, Ser. A 37 (1984) 136–163, 164–188, 189–192.

[7] S.S. Magliveras and D.W. Leavitt, Simple six designs exist, Congressus Numerantium 40 (1983) 195–205.

[8] A. Rosa, Intersection properties of Steiner systems, Annals Discrete Mathematics 7 (1980) 115–128.

[9] S. Schreiber, Some balanced complete block designs, Israel J. Math. 18 (1974) 31–37.

[10] L. Teirlinck, On the maximum number of disjoint triple systems, J. Geometry 6 (1975) 93–96.

[11] L. Teirlinck, On large sets of disjoint quadruple systems, Ars Combinatoria 17 (1984) 173–176.

[12] L. Teirlinck, Non-trivial t-designs without repeated blocks exist for all t, Discrete Math. 65 (1987) 301–311.

Discrete Mathematics 77 (1989) 357–365
North-Holland

A NEW FAMILY OF BIBDs AND NON-EMBEDDABLE (16, 24, 9, 6, 3)-DESIGNS

G.H.J. van REES*

Department of Computer Science, University of Manitoba, Winnipeg, Mannitoba, Canada R3T 2N2

We construct a new family of balanced incomplete block designs with parameters $(2n^2+3n+2, ((n+1)/2)(2n^2+3n+2), (n+2)^2, 2n+2, n+1)$ where n and $n+1$ are prime powers. Also we construct 251 non-embeddable (16, 24, 9, 6, 3) designs and thereby increasing the lower bound on the number of pairwise non-isomorphic balanced incomplete block designs (16, 24, 9, 6, 3) to 1542.

1. Introduction

A balanced incomplete block design (BIBD) is a pair (V, B) where V is a v-set and B is a collection of b k-subsets of V called blocks such that each element of V is contained in exactly r blocks and any 2-subset of V is contained in exactly λ blocks. The numbers v, b, r, k, λ are parameters of the BIBD. Trivial necessary conditions for the existence of a BIBD (v, b, r, k, λ) are

(1) $vr = bk$,
(2) $r(k-1) = \lambda(v-1)$.

A parameter set that satisfies (1) and (2) is said to be admissible.

Two BIBDs (V_1, B_1) and (V_2, B_2) are isomorphic if there exists a bijection α: $V_1 \to V_2$ such that $B_1\alpha = B_2$. Given a symmetric BIBD (one with $v = b$, $r = k$), one obtains from it the residual design by deleting all elements of one block, and the derived design by deleting all elements of the complement of one block. The parameters of a derived design are $(k, v-1, k-1, \lambda, \lambda-1)$, whereas the parameters of a residual design are $(v-k, v-1, k, k-\lambda, \lambda)$.

Any BIBD that has parameters $(k, v-1, k-1, \lambda, \lambda-1)$ or $(v-k, v-1, k, k-\lambda, \lambda)$ is called a quasi-derived or quasi-residual, respectively. A quasi-residual design which is residual is said to be embeddable in the corresponding symmetric design.

A resolvable BIBD (v, b, r, k, λ), denoted by RBIBD is a balanced incomplete block design in which the blocks of the design may be partitioned into r sets of v/k blocks such that every element of the design occurs in a block exactly once in each partition. The partitions are called resolution classes.

In the following section we describe a construction for a new family of BIBDs.

* Supported by NSERC grant OGP0003558.

In later sections this construction for $n = 2$ is used to produce 278 non-isomorphic (16, 24, 9, 6, 3) BIBDs of which 251 are non-embeddable.

2. General construction

Theorem 1. *If a* SBIBD $(n^2+n+1, n+1, n)$ *and a* RBIBD $((n+1)^2, (n+1)(n+2), n+2, n+1, 1)$ *both exist, then a* BIBD $(2n^2+3n+2, (n+1)(2n^2+3n+2)/2, (n+1)^2, 2n+2, n+1)$, *exists.*

Proof. Let the SBIBD elements be the set $\{1, 2, 3, \ldots, n^2+n+1\} = I$. Let the RBIBD elements be the set $\{n^2+n+2, n^2+n+3, \ldots, 2n^2+3n+2\} = J$. Then to construct the new design, duplicate each block of the SBIBD $n+1$ times and duplicate each block of the RBIBD n times. The new blocks of the design consist of two types. The first type is formed by adjoining to every set of n duplicated blocks a resolution class of the RBIBD. For example, if $n = 2$ then the block $\{1, 2, 3\}$ of the SBIBD is duplicated 3 times and the resolution class $\{8, 9, 10\}$, $\{11, 12, 13\}$ and $\{14, 15, 16\}$ of the RBIBD is adjoined to it to produce the following three blocks of the new design $\{1, 2, 3, 8, 9, 10\}$, $\{1, 2, 3, 11, 12, 13\}$ and $\{1, 2, 3, 14, 15, 16\}$. The choice of which resolution class is adjoined to which set of n duplicated blocks is completely arbitrary except that the $n-1$ resolution classes left over must be identical. Let the blocks of this resolution class be denoted by $B_1, B_2, \ldots, B_n$. Then the second type of blocks for the new design are $B_i \cap B_j$ for all $i \neq j$. This is the design.

It is quite easy to check if the new design has $2n^2+3n+2$ elements and $(n^2+n+1)(n+1) + ((n+1)/2) = (n+1)(2n^2+3n+2)/2$ blocks of size $2n+2$. An element $i \in I$ occurs $(n+1)(n+1)$ times and an element $j \in J$ occurs $(n+2)n - (n-1) + n = (n+1)^2$ times also. A pair of elements $i_1, i_2 \in I$ occurs $1 \times (n+1) = n+1$ times. A pair i, j where $i \in I$ and $j \in J$ occurs $n+1$ (the r of the SBIBD) times. A pair $j_1, j_2 \in J$, where j_1, j_2 are both elements in some B_i of the left over resolution class, occurs once in the first type of blocks and n times in the second type of block whereas if j_1, j_2 do not occur in some B_i, then they occur n times in the first type of block and 1 time in the second type of block. Hence all pairs occur $n+1$ times. $\square$

An SBIBD $(n^2+n+1, n+1, 1)$ is equivalent to a projective plane of order n. An RBIBD $((n+1)^2, (n+1)(n+2), n+2, n+1, 1)$ is equivalent to an affine plane of order $n+1$. Therefore, the construction works if both n and $n+1$ are prime. Another way to state the condition is to specify that either n is a Fermat prime or $n+1$ is a Mersenne prime. Since there are 35 such numbers known [2], the construction works at least 35 times. We record this in the following corollary.

Corollary. *If n is a Fermat prime or $n+1$ is a Mersenne prime then there exists a* BIBD $(2n^2+3n+2, (n+1)(2n^2+3n+2)/2, (n+1)^2, 2n+2, n+1)$.

The construction can be slightly generalized if one uses a RBIBD $((n+1)^2, n(n+1)(n+2), n(n+2), n+1, n)$ which has $n-1$ identical copies of one resolution class instead of n copies of a RBIBD $((n+2)^2, (n+1)(n+2), n+2, n+1, n)$. Thus, we can state the following theorem:

Theorem 2. *If a* SBIBD $(n^2+n+1, n+1, 1)$ *exists and a* RBIBD $((n+1)^2, n(n+1)(n+2), n(n+2), n+1, n)$ *which has* $n-1$ *identical copies of one resolution class exists then a* BIBD $(2n^2+3n+2, (n+1)(2n^2+3n+2)/2, (n+1)^2, 2n+2, (n+1))$ *exists.*

Proof. Same as Theorem 1 but ensure that the $n-1$ identical copies are used for the blocks of type 2. □

In order to tell if the construction produces any new designs, we consult the helpful list of BIBD parameters and known lower bounds of Mathon and Rosa [7]. For $n=3$, the construction produces a (29, 58, 16, 8, 4) BIBD which is non-isomorphic to the only other known such design produced by Sprott [10]. They are non-isomorphic because they have different block intersection numbers. For $n=4$, the construction produces the first known (46, 115, 25, 10, 5) BIBD.

3. Non-isomorphic (16, 24, 9, 6, 3) BIBDs

For $n=2$, the construction produces a design with the same parameters (16, 24, 9, 6, 3), as Bhattacharaya's [1] famous counterexample. The counterexample was non-embeddable as two blocks intersected in four varieties. Brown [3] produced such a design which was non-embeddable but had no block intersection of size 4. Lawless [6] produced 8 non-isomorphic non-embeddable designs with various intersection patterns. All three used ad hoc procedures to produce these results. Just recently Van Trung [12] produced one of these non-embeddable designs with a complicated construction.

For $n=2$, we can use Theorem 2 as any RBIBD (9, 24, 8, 3, 2) trivially has one copy of a resolution class. Hence, by using the list of BIBD (9, 24, 8, 3, 2) of Morgan [9] with the correction of Mathon and Rosa [8], we can generate many non-isomorphic designs with many different intersection patterns. Most of the designs produced this way are obviously non-embeddable as they have block intersection size 4.

Indeed, for any specific RBIBD we can assign resolution classes to the duplicated blocks of the SBIBD in every possible way. This creates 8! designs which can be reduced to 6! or 5! by using the automorphism groups of the smaller designs. Then, using Kocay's very fast graph algorithm program (described in [5]), we can get a canonical form for each design in about one and a half seconds on an Amdahl 580. These are then sorted and duplicates eliminated. These can then be compared to the known non-embeddable (16, 24, 9, 6, 3) BIBDs. Furthermore, designs can be compared to Van Rees' [11] list of all residual (16, 24, 9, 6, 3) BIBDs to see if they are residual or not. The results are summarized in the following theorems.

Theorem 3. *There are* 278 *pairwise non-isomorphic* (16, 24, 9, 6, 3) BIBD*s which contain three identical disjoint copies of the* SBIBD (7, 3, 1).

Proof. Any (16, 24, 9, 6, 3) BIBD which contains three identical copies of the SBIBD (7, 3, 1) must have a structure as described in the beginning of Section 3. To prove this, consider an element of the (16, 24, 9, 6, 3) design which is not one of the seven elements of the SBIBD. If it occurs more than once with the same triplicated block of the SBIBD then it can occur at most 5 times with triplicated blocks and thus at most 8 times in the design. This is a contradiction. It must appear once with each triplet of identical blocks to get the pair count correct. This means every element not in the SBIBD, must occur with a triplet of identical blocks exactly once.

In other words, a resolution class of "other" elements must be attached to each triplet of identical blocks. This determines 7 resolution class which clearly determine the RBIBD (9, 24, 8, 3, 2). Since the construction produces 278 designs, the theorem is true. □

Theorem 4. *There are* 251 *pairwise non-isomorphic, non-embeddable* BIBD (16, 24, 9, 6, 3) BIBDs *which contain three identical disjoint copies of the* SBIBD (7, 3, 1).

Theorem 5. *The number of pairwise non-isormorphic, non-embeddable* BIBD (16, 24, 9, 6, 3) *is* 261.

Proof. The designs of Bhattacharya, Brown and Lawless were non-isomorphic to each other and to any of the 251 produced by our construction. Van Trung's design, which was produced independently and by an entirely different construction, was isomorphic to one of the designs produced by the construction.

In order to produce a listing of all the designs in a minimum of space, we list all resolvable BIBDs (9, 24, 8, 3, 2) using Morgan's numbering. The basic (9, 12, 4, 3, 1) BIBD is as follow:

$$\left.\begin{array}{r}\{8,9,16\}\\ \{10,12,14\}\\ \{11,13,15\}\end{array}\right\} R_0$$

$$\left.\begin{array}{r}\{8,13,14\}\\ \{9,12,15\}\\ \{10,11,16\}\end{array}\right\} R_1$$

$$\left.\begin{array}{r}\{8,10,15\}\\ \{9,11,14\}\\ \{12,13,16\}\end{array}\right\} R_2$$

$$\left.\begin{array}{r}\{8, 11, 12\} \\ \{9, 10, 13\} \\ \{14, 15, 16\}\end{array}\right\} R_3$$

All the resolvable (9, 24, 8, 3, 2) BIBD's have these as their first four resolution classes. The second four resolution classes are these again but with a permutation applied as follows:

Design	*Permutation*
1	I
2	(8, 9)
3	(8, 9)(10, 11)
6	(8, 9, 10)
7	(8, 9, 10, 11)
14	(8, 9)(11, 13)(12, 14)
15	(8, 9, 10, 13)
23	(8, 9, 10, 13, 16)
29	(8, 9, 11, 12, 16)

Therefore, the seventh resolution class, $R6$, in design 29 is (8, 9, 11, 12, 16) $R2$.

Now the blocks of the SBIBD are specified as follows:

$$\{1, 2, 4\} = B_1$$

$$\{2, 3, 5\} = B_2$$

$$\{3, 4, 6\} = B_3$$

$$\{4, 5, 7\} = B_4$$

$$\{5, 6, 1\} = B_5$$

$$\{6, 7, 2\} = B_6$$

$$\{7, 1, 3\} = B_7$$

Now to specify a particular design constructed by Theorem 2, we need only indicate which resolution classes get attached to which tripled blocks of the SBIBD, e.g. 7D02514367 is the design produced from the design number 7 where $R0$ is left over, $R2$ is attached to the tripled block 1 of the SBIBD, $R5$ is attached to tripled block 2, $R1$ is attached to tripled block 3, etc. (*Table 1*).

Table 2 lists those designs which are isomorphic to a (16, 24, 9, 6, 3) BIBD from the Van Rees list and hence these designs are residual and previously known. The left-hand side gives the design number as in the previous list and the middle gives the design number as in Van Rees' list and the right-hand side gives the order of the automorphism group of the design.

The first three designs were produced from Morgan's Design #14, the next 18 were produced from Design #15 and the last 6 were produced from Design #23.

Table 3 shows how many non-isomorphic (16, 24, 9, 6, 3) designs

Table 1. Non-isomorphic (16, 24, 9, 6, 3) BIBDs containing three identical disjoint SBIBDs (7, 3, 1)

#	Design	$\|G\|$	#	Design	$\|G\|$	#	Design	$\|G\|$
1	1D04126357	432	2	1D04152637	54	3	1D04652317	72
4	2D01423567	6	5	2D02453617	2	6	2D03124567	4
7	2D05423617	4	8	2D05432617	12	9	2D10235467	2
10	2D10524367	2	11	2D13024567	4	12	2D14023567	2
13	2D14203567	2	14	2D14250367	4	15	2D14305267	4
16	2D15342067	2	17	2D15420367	2	18	3D01245367	4
19	3D01345267	4	20	3D01352467	2	21	3D01423567	2
22	3D01452367	2	23	3D01534267	2	24	3D02413567	2
25	3D03124567	4	26	3D03145267	2	27	3D03452167	2
28	3D03514267	2	29	3D03524167	4	30	3D04135267	2
31	3D04321567	2	32	3D05241367	4	33	3D05321467	2
34	3D05341267	4	35	3D05432167	2	36	6D01235467	1
37	6D01243567	1	38	6D01254367	1	39	6D02154367	1
40	6D02314567	1	41	6D02315467	1	42	6D02351467	1
43	6D02354167	1	44	6D02413567	1	45	6D02435167	1
46	6D02453167	1	47	6D02513467	1	48	6D02514367	1
49	6D02534167	1	50	6D02543167	1	51	6D03152467	1
52	6D03215467	1	53	6D03421567	1	54	6D03425167	1
55	6D03541267	1	56	6D03542167	1	57	6D04235167	1
58	6D04251367	1	59	6D04321567	1	60	6D04523167	1
61	6D04532167	1	62	6D05132467	1	63	6D05142367	1
64	6D05342167	1	65	6D05431267	1	66	6D12035467	1
67	6D12043567	1	68	6D12304567	3	69	6D12345067	1
70	6D12534067	3	71	6D13204567	1	72	6D13502467	3
73	6D14023567	1	74	6D15043267	3	75	6D15240367	3
76	6D15243067	1	77	6D15324067	3	78	6D15423067	1
79	6D15430267	1	80	7D01243567	1	81	7D01245367	1
82	7D01254367	1	83	7D01342567	1	84	7D01345267	1
85	7D01354267	1	86	7D01432567	1	87	7D01435267	1
88	7D01453267	1	89	7D01534267	1	90	7D02314567	1
91	7D02315467	1	92	7D02453167	1	93	7D02514367	1
94	7D03142567	1	95	7D03412567	1	96	7D03452167	1
97	7D04235167	1	98	7D04251367	1	99	7D04325167	1
100	7D04521367	1	101	7D04531267	1	102	7D05143267	1
103	7D05231467	1	104	7D05241367	1	105	7D05243167	1
106	7D05312467	1	107	7D05321467	1	108	7D05324167	1
109	7D05413267	1	110	7D20143567	2	111	7D20314567	1
112	7D21034567	1	113	7D21043567	2	114	7D21304567	1
115	7D21354067	1	116	7D21403567	2	117	7D23014567	1
118	7D23401567	1	119	7D23415067	1	120	7D23451067	1
121	7D24013567	2	122	7D24103567	2	123	7D24310567	1
124	7D24531067	1	125	7D25143067	2	126	7D25341067	1
127	7D25431067	1	128	7D30214567	1	129	7D30254167	1
130	7D30412567	2	131	7D30512467	2	132	7D31024567	1
133	7D31052467	2	134	7D31054267	1	135	7D31405267	1
136	7D31420567	1	137	7D31542067	2	138	7D32041567	1
139	7D32051467	1	140	7D32501467	1	141	7D34210567	1
142	7D34512067	2	143	7D35012467	2	144	7D35014267	1
145	7D35021467	1	146	14D01453267	6	147	14D02413567	18
148	14D03245167	18	149	14D12034567	6	150	14D12534067	6
151	14D14035267	6	152	14D15432067	3	153	15D01235467	1
154	15D01523467	1	155	15D02345167	1	156	15D02351467	2
157	15D02354167	2	158	15D02431567	1	159	15D02531467	2
160	15D03124567	2	161	15D03142567	2	162	15D03412567	2
163	15D03425167	1	164	15D03514267	1	165	15D04123567	1
166	15D04132567	1	167	15D04513267	1	168	15D04523167	1
169	15D05234167	1	170	15D05321467	1	171	15D10342567	1
172	15D10352467	1	173	15D10423567	1	174	15D10524367	1
175	15D12034567	1	176	15D12035467	1	177	15D12054367	1
178	15D12305467	1	179	15D12430567	1	180	15D13205467	1
181	15D13402567	1	182	15D13450267	1	183	15D14052367	1
184	15D14203567	1	185	15D14205367	1	186	15D14302567	1
187	15D14503267	1	188	15D15024367	1	189	15D15043267	1
190	15D15240367	1	191	15D15302467	1	192	15D15320467	1
193	15D15403267	1	194	15D15420367	1	195	15D20153467	1

Table 1. *Continued*

#	Design	$\lvert G\rvert$	#	Design	$\lvert G\rvert$	#	Design	$\lvert G\rvert$
196	15D20435167	1	197	15D20534167	1	198	15D23504167	1
199	15D25130467	1	200	15D25310467	1	201	15D30142567	2
202	15D30154267	1	203	15D30254167	1	204	15D30412567	2
205	15D30421567	2	206	15D31054267	2	207	15D31540267	1
208	15D32051467	2	209	15D32150467	1	210	15D32410567	1
211	15D34012567	1	212	15D34021567	1	213	15D34102567	1
214	15D34120567	1	215	15D34150267	1	216	15D34201567	1
217	15D35124067	2	218	15D35410267	1	219	23D01425367	1
220	23D03124567	1	221	23D03421567	3	222	23D04153267	3
223	23D04513267	3	224	23D05432167	3	225	23D10235467	1
226	23D10342567	1	227	23D10354267	1	228	23D12304567	1
229	23D12405367	1	230	23D12430567	1	231	23D13420567	1
232	23D14023567	1	233	23D14035267	1	234	23D15430267	1
235	29D01432567	3	236	29D02314567	1	237	29D02435167	1
238	29D03142567	1	239	29D03145267	3	240	29D03214567	1
241	29D03215467	3	242	29D03412567	1	243	29D03421567	3
244	29D03425167	3	245	29D04132567	1	246	29D04312567	1
247	29D04321567	1	248	29D05143267	3	249	29D10234567	1
250	29D10245367	1	251	29D10253467	1	252	29D10325467	1
253	29D10435267	1	254	29D10452367	1	255	29D12304567	1
256	29D12305467	1	257	29D12340567	1	258	29D12403567	1
259	29D12435067	1	260	29D12504367	1	261	29D13024567	1
262	29D13042567	1	263	29D13052467	1	264	29D13402567	1
265	29D13405267	1	266	29D13452067	1	267	29D13502467	1
268	29D13524067	1	269	29D14203567	1	270	29D14250367	1
271	29D14320567	1	272	29D14530267	1	273	29D15024367	1
274	29D15203467	1	275	29D15240367	1	276	29D15243067	1
277	29D15320467	1	278	29D15423067	1			

Table 2. Non-isomorphic, residual (16, 24, 9, 6, 3) BIBDs containing three identical, disjoint SBIBDs (7, 3, 1)

Design number	Isomorphic to	$\lvert G\rvert$	Design number	Isomorphic to	$\lvert G\rvert$
146	1128	6	212	632	1
147	1246	18	213	934	1
148	1247	18	214	630	1
201	1067	2	215	631	1
202	1064	1	216	935	1
203	1065	1	217	1073	2
204	629	2	218	1078	1
205	633	2	219	716	1
206	1069	2	220	718	1
207	626	1	221	719	3
208	1068	2	222	717	3
209	1079	1	223	1066	3
210	627	1	224	1074	3
211	628	1			

Table 3

(9, 24, 8, 3, 2) Design	# of Designs
1	3
2	14
3	18
6	44
7	66
14	7
15	66
23	16
29	14

Table 4

Order of automorphism group	# of Non-isomorphic
1	196
2	43
3	17
4	11
6	5
12	1
18	2
54	1
72	1
432	1

containing 3 identical disjoint SBIBDs $(7, 3, 1)$ were produced from each RBIBD $(9, 24, 8, 3, 2)$.

Table 4 shows the number of non-embeddable $(16, 24, 9, 6, 3)$ BIBDs containing 3 identical disjoint SBIBDs $(7, 3, 1)$ produced with each automorphism group order.

Finally, we state the following theorem.

Theorem 6. *The number of pairwise non-isomorphic* BIBD $(16, 24, 9, 6, 3)$ *is at least* 1542.

Proof. There are 1281 residual ones listed by Van Rees and 261 non-isomorphic, non-embeddable ones by Theorem 6. □

References

[1] K.N. Battacharya, A new balanced incomplete block design, Sci. Culture 9 (1944) 508.

[2] J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman and S.S. Wagstaff, Jr., Factorizations of $b^n \pm 1$, Contemporary Mathematics Ser. AMS Vol. 22 (1983), update 5 (circa June 21, 1987).

[3] R.B. Brown, A new nonextensible (16, 24, 9, 6, 3) design, JCT (a) 19 (1975) 115–116.

[4] R.H.F. Denniston, Enumeration of symmetric designs (25, 9, 3), Annals Discrete Math. 15 (1982) 111–127.

[5] W.L. Kocay, Abstract data types and graph isomorphism, J. Combin. Info. and S.S., 9, 4 (1984) 247–259.

[6] J.F. Lawless, An investigation of Bhattacharya-type designs, J.C.T. 11 (1971) 139–147.

[7] R. Mathon and A. Rosa, Tables of parameters of BIBDs with $r \leqslant 41$ including existence, enumeration and resolvability results, Annals Discrete Math. 265 (1985) 275–308.

[8] R. Mathon and A. Rosa, A census of Mendelsohn triple systems of order 9, Ars Combinatoria 4 (1977) 309–315.

[9] E.J. Morgan, Some small quasi-multiple designs, Ars Combinatoria 3 (1977) 233–250.

[10] D.A. Sprott, A note on balanced incomplete block designs, Can. J. Math., 6 (1954) 314–321.

[11] G.H.J. Van Rees, All non-isomorphic, residual (16, 24, 9, 6, 3) designs, submitted JCMCC.

[12] Van Trung, Maximal ars and related designs, preprint.

This Page Intentionally Left Blank

Discrete Mathematics 77 (1989) 367–384
North-Holland

MODIFICATIONS OF THE "CENTRAL-METHOD" TO CONSTRUCT STEINER TRIPLE SYSTEMS

H. ZEITLER
Mathematisches Institut, Universität Bayreuth, D-8580 Bayreuth, Postfach 101251, F.R. Germany

0. Introduction

0.1. *Steiner triple systems*

Let V with $|V| = v$ be a finite set and B a set of 3-subsets of V. The elements of V are called points, those of B lines. If any 2-subset of V is contained in exactly one line, then the pair (V, B) is called a Steiner triple system of order v, in short STS(v). Each point lies on exactly $r = \frac{1}{2}(v-1)$ lines and we have $|B| = b = \frac{1}{6}v(v-1)$. The condition $v = 7,\ 9 + 6n,\ n \in \mathbb{N}_0$, is necessary and sufficient for the existence of STS(v) (the trivial cases $v = 1$, $v = 3$ are excluded). The set of these "admissible" numbers, of these "Steiner numbers" is denoted by STS.

0.2. *Ovals in STS*(v)

A non-empty subset $O \subset V$ in a STS(v) is called an oval if each point of O lies on exactly one tangent and each other line of the STS(v) has at most two points in common with O. A line is called a tangent if it meets O in exactly one point. If there are exactly two intersection points or if there is no intersection point then we have a secant or a passant respectively. The points of O are called on-points, the points of the tangents which are not on-points are called ex-points and the remaining points in-points. With respect to an oval O there are exactly r tangents, $\frac{1}{2}r(r-1)$ secants, $\frac{1}{6}r(r-1)$ passants and we have $|O| = r$. The number of tangents through an ex-point is even iff r is even.

0.3. *Special ovals in* STS(v)

An oval O_K is called a knot oval if all tangents have exactly one point Z in common. Z is called the knot of the oval. Each ex-point different from Z lies on exactly one tangent and there are no in-points. It is known that there exist systems STS(v) with a knot oval if and only if $v \in \text{HSTS} := \{7,\ 15 + 12n,\ n \in \mathbb{N}_0\}$. [2]. Sometimes the set $H = O_K \cup \{Z\}$ is called a hyperoval. The complement of H together with the passants of O_K forms a subsystem STS(r). It is possible to prove the converse of this theorem. If we delete one point from a hyperoval we get an oval.

An oval O_R is called regular if any ex-point lies on exactly two tangents. There is exactly one in-point. It is known that there exist systems STS(v) with a regular oval if and only if $v \in \mathrm{RSTS} := \{9, 13 + 12n, n \in \mathbb{N}_0\}$ [5].

With all these notations we have $\mathrm{HSTS} \cap \mathrm{RSTS} = \emptyset$ and $\mathrm{STS} = \mathrm{HSTS} \cup \mathrm{RSTS}$. In this way the sets HSTS and RSTS are characterized geometrically by using special ovals.

Now it is quite natural to ask, whether there exist other types of ovals besides knot ovals and regular ovals. This means ovals with other configurations of the tangents.

0.4. *The aim*

In this paper systems STS(v) with other kinds of ovals – neither O_K nor O_R – are constructed. This is done by modifying the so-called "central-method" in different ways. This central-method is due to T. Skolem (1927). Finally we obtain a geometrical classification of further subsets of HSTS.

1. The central-method [2]

Starting with a given system STS(r) a system STS($v = 1 + 2r$) with a knot oval is constructed recursively.

Ex-points:	the points of STS(r): $1, 2, \ldots, r$,
passants (exterior lines):	the lines of STS(r),
knot:	Z,
tangents:	$\{Z, i, i'\}$ with $i \in \{1, 2, \ldots, r\}$,
on-points:	$1', 2', \ldots, r'$.

In order to visualize the procedure, let Z be the top of a pyramid whose base is the system STS(r). Then – as *Fig. 1* shows – all ex-points i are pulled up in a special way to i'. It is also possible to think of a central projection with center Z. Additionally any line $\{a, b, c\}$ of STS(r) together with Z determines a projective plane $\mathrm{PG}(2, 2) = \mathrm{STS}(7)$. Then the lines $\{a, b', c'\}$, $\{a', b, c'\}$, $\{a', b', c\}$ are secants of the knot oval.

In this way a system STS(v) with a knot oval can be developed – as proved in [2]. This construction is possible exactly in the case $v \in \mathrm{HSTS} \setminus \{7\}$.

2. The perturbation trick

In the system STS(v) constructed with the central-method we now consider a passant $\{a_1, b_1, c\}$ together with the projective plane belonging to it (*Fig. 1*).

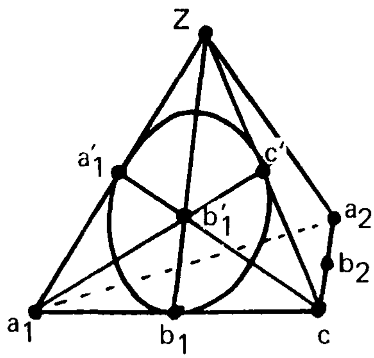


Fig. 1.

The lines $\{Z, a_1, a_1'\}$, $\{Z, b_1, b_1'\}$, $\{c, a_1, b_1\}$, $\{c, a_1', b_1'\}$ may be deleted and replaced by the lines $\{c, a_1, a_1'\}$, $\{c, b_1, b_1'\}$, $\{Z, a_1, b_1\}$, $\{Z, a_1', b_1'\}$. We call this slight modification the perturbation trick. What has happened by doing so? The point set $\{1', 2', \ldots, r'\}$ is still an oval. But through the ex-point Z there are now only $r-2$ tangents (as well as one secant and one passant) and through c there are 3 tangents (as well as $\frac{1}{2}(r-3)$ secants and just as many passants). Nothing else has changed. Using the perturbation trick we therefore obtain a STS(v) with an oval of a completely new type. Now we perform the perturbation trick several times. Doing so we distinguish different cases.

3. A first multiple method (with pencils)

3.1. *The procedure*

We now perform the perturbation trick a second time, using a further passant through c, namely $\{c, a_2, b_2\}$. The lines $\{Z, a_2, a_2'\}$, $\{Z, b_2, b_2'\}$, $\{c, a_2, b_2\}$, $\{c, a_2', b_2'\}$ are deleted and replaced by $\{c, a_2, a_2'\}$, $\{c, b_2, b_2'\}$, $\{Z, a_2, b_2\}$, $\{Z, a_2', b_2'\}$. Now the point Z still has $r-4$ tangents, but the point c is on exactly 5 tangents. A new type of oval has been found. Continuing in this way with further passants through c we always obtain new Steiner triple systems with new types of ovals.

3.2. *Result*

The Table in *Fig. 2* shows the result of our procedure. The letter x_j means the number of ex-points with exactly j tangents. Any column represents one special type of oval. In total there are $z = \frac{1}{2}(r+1)$ rows.

x_r	1	0	0	...	0	...
x_{r-2}	0	1	0		0	
x_{r-4}	0	0	1		0	
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	
x_{r-2p}	0	0	0		1	
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	
x_{1+2p}	0	0	0		1	
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	
x_5	0	0	1		0	
x_3	0	1	0		0	
x_1	r	r-1	r-1		r-1	

Fig. 2.

3.3. *The number of oval types*

Now we ask for the number of different oval types developed by using our procedure. When does the continued execution of the perturbation trick come to an end? To answer this question we distinguish two cases.

3.3.1. *z is odd*

Now it is possible that in one row the number 1 appears twice. This occurs if $r-2p=1+2p$, hence for $p=\frac{1}{4}(r-1)$. It follows that $1+2p=r-2p=\frac{1}{2}(r+1)$. So we have two ex-points with $\frac{1}{2}(r+1)$ tangents each and $r-1$ ex-points with exactly one tangent each. This oval type is denoted by O_1. Performing the perturbation trick once more yields oval types we have already had. Thus – besides the knot oval – we obtain $p=\frac{1}{4}(r-1)$ further oval types in total.

3.3.2. *z is even*

Now it is possible that in one column two numbers 1 are one above the other. This occurs for the first time when $(r-2p)-2=1+2p$, hence for $p=\frac{1}{4}(r-3)$. It follows that $r-2p=\frac{1}{2}(r+3)$ and $1+2p=\frac{1}{2}(r-1)$. So we have one ex-point with exactly $\frac{1}{2}(r+3)$ tangents, one ex-point with exactly $\frac{1}{2}(r-1)$ tangents and $r-1$ ex-points with exactly one tangent each. This oval type is denoted by O_2. Performing the perturbation trick once more does not yield new oval types. Thus – besides the knot oval – we obtain $p=\frac{1}{4}(r-3)$ further oval types in total. *Fig. 3* illustrates 3.3.1 and 3.3.2 for the cases $r=13$ and $r=15$, therefore $z=7$ and $z=8$.

3.3.3. *What about the corresponding Steiner numbers?*

We now investigate the orders $v \in$ HSTS (by using the central-method only numbers of this kind may occur) where the oval types O_1 and O_2 respectively are

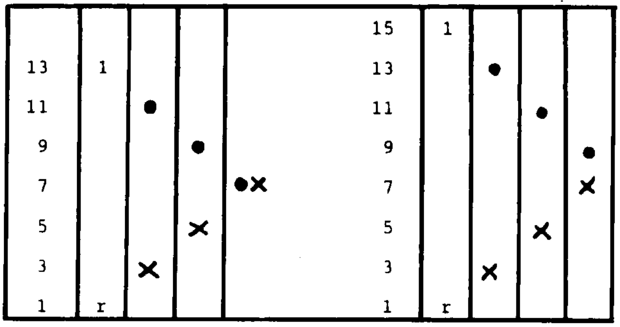


Fig. 3.

obtained. This depends on the parity of z, and the various cases are tabulated in *Fig. 4.* Now we formulate all the results in 3.3 as a theorem.

3.3.4 Theorem. *Exactly for all* $v \in \mathrm{H_1STS}$ *there exist systems* $\mathrm{STS}(v)$ *with an oval* O_1 *and exactly for all the remaining Steiner numbers of* HSTS, *namely for all* $v \in \mathrm{H_2STS}$, *there exist systems* $\mathrm{STS}(v)$ *with an oval* O_2.

$\mathrm{H_1STS}$: $v = 19,\ 27 + 24n$; $\mathrm{H_2STS}$: $v = 15,\ 31 + 24n$; $n \in \mathbb{N}_0$. We have $\mathrm{HSTS} = \mathrm{H_1STS} \cup \mathrm{H_2STS} \cup \{7\}$. Now the disjoint sets $\mathrm{H_1STS}$ and $\mathrm{H_2STS}$ are also geometrically characterized when special ovals are used.

3.3.5. *Visualization*

In *Fig. 5* the configurations of the tangents belonging to the ovals O_1 and O_2 are visualized. Doing so we choose $v = 19$ ($r = 9$, $z = 5$) and $v = 15$ ($r = 7$, $z = 4$). All the ex-points with more than one tangent are represented as quadrangles, all the ex-points with exactly one tangent as "empty" circles and all the on-points as "full" circles. Corresponding pictures may also be drawn in all the other cases $v \in \mathrm{H_1STS}$ and $v \in \mathrm{H_2STS}$ respectively.

$v = 19 + 12n$ $r = 9 + 6n$ $z = 5 + 3n$	$v = 15 + 12n$ $r = 7 + 6n$ $z = 4 + 3n$
$\left.\begin{array}{l} n = 2m \\ z = 5 + 6n, \text{ odd} \\ v = 19 + 24m \end{array}\right\} O_1$	$O_2 \left\{\begin{array}{l} n = 2m \\ z = 4 + 6m, \text{ even} \\ v = 15 + 24m \end{array}\right.$
$\left.\begin{array}{l} n = 2m + 1 \\ z = 8 + 6m, \text{ even} \\ v = 31 + 24m \end{array}\right\} O_2$	$O_1 \left\{\begin{array}{l} n = 2m + 1 \\ z = 7 + 6m, \text{ odd} \\ v = 27 + 24m \end{array}\right.$

Fig. 4.

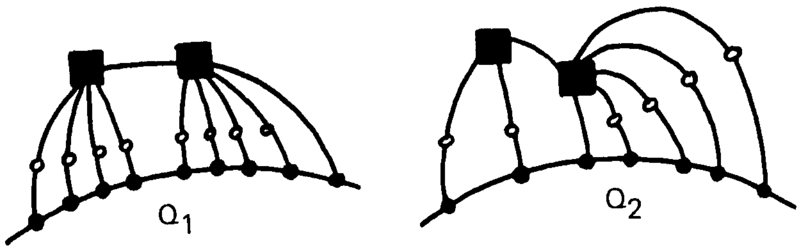


Fig. 5.

Remarks.

(1) Systems STS(v) with the oval types constructed here have been constructed in [6] (by using the polygon-method). It may be shown that

(a) all systems given in [6],

(b) all systems constructed in Section 3.1,

(c) but also all systems of the same order – corresponding to each other – in [6] and Section 3.1 are pairwise non-isomorphic.

(2) The set H_2STS may also be found in [1]. It is proved there, that $v \in H_2\mathrm{STS}$ is a necessary condition for the existence of STS(v) with *two* hyperovals (and therefore also two subsystems of order $\frac{1}{2}(v-1)$).

4. An intermediate chapter: r-chain in STS(v)

4.1. *r-chains – what are they?*

In Steiner triple systems STS(v) we are looking for $r = \frac{1}{2}(v-1)$ lines, which are connected in the form of an r-polygon without any overlapping. A polygon of this kind – also representable as a regular polygon – is called an r-chain. More formally an r-chain in an STS($2r+1$) is a set of r lines $b_0, b_1, \ldots, b_{r-1}$, such that

$$\left|\bigcup_{i=0}^{r-1} b_i\right| = 2r, \qquad |b_i \cap b_{i+1}| = 1 \quad \text{and} \quad |b_{i-1} \cap b_i \cap b_{i+1}| = 0,$$

for all $i = 0, 1, \ldots, r-1$ (subscripts reduced modulo r). If the third point of every polygon edge is put on the circumcircle of this polygon, then we obtain a regular $2r$-gon. The lines may be interpreted as areas ("curved" triangles) and so they form a "garland". In the *Figs. 6* and *7* r-chains of this kind are drawn in the cases $v = 7$ and $v = 9$.

By using trial and error it is possible to discover 6-chains in both Steiner triple systems of order 13 as well. With the notations of [7] we obtain *Fig. 8*. Now we are confronted with the following question: Do there exist systems STS(v) with r-chains for all $v \in$ STS.

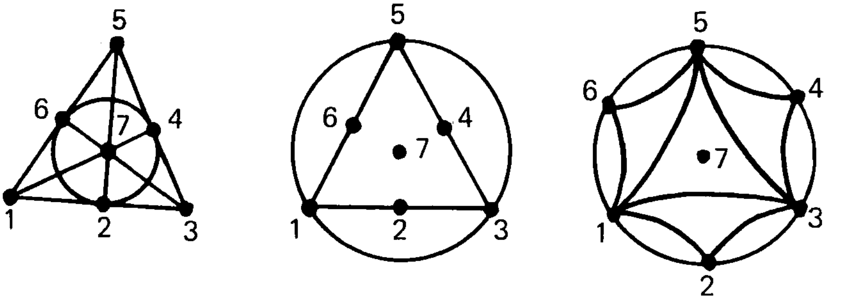


Fig. 6. 3-chains in STS(7).

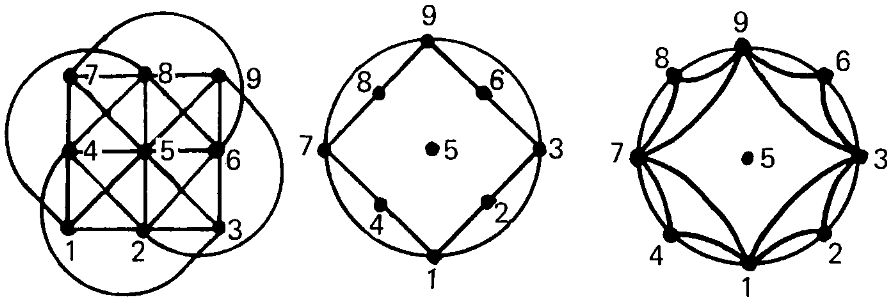


Fig. 7. 4-chains in STS(9).

4.2 Theorem. *For all* $v \in$ STS *there exist* STS(v) *with an* r*-chain.*

The proof of this theorem is in two cases.

$v \in$ HSTS

Starting with a system STS(r) systems STS($v = 1 + 2r$) with $v \in$ HSTS and $v \neq 7$ (this case has already been done by means of *Fig. 6*) may be constructed not only

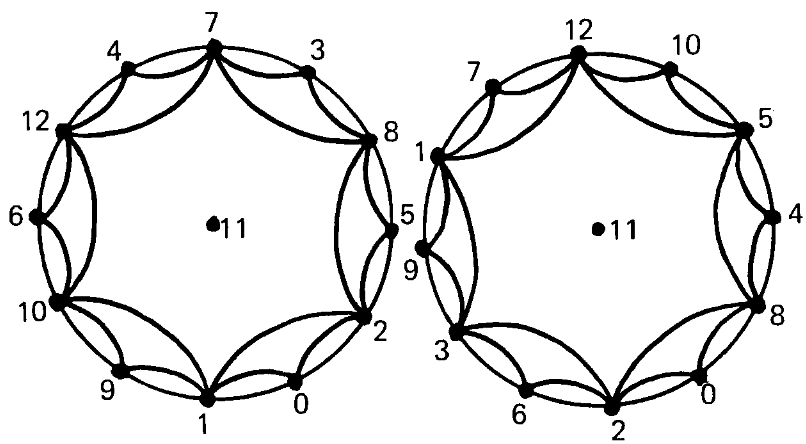


Fig. 8. 6-chains in $STS_1(13)$ (left) and $STS_2(13)$ (right).

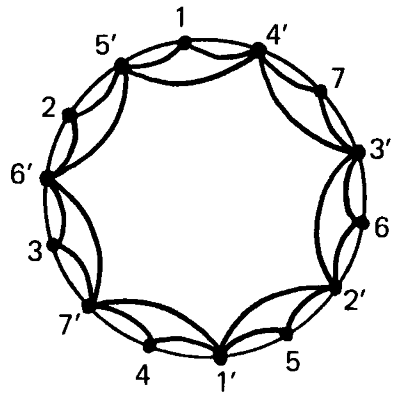


Fig. 9. 7-chains in an STS(15).

by the central- but also by the polygon-method [2]. In any case a knot oval is used.

Ex-points:	the points of STS(r): $1, 2, \ldots, r$,
passants:	the lines of STS(r),
knot:	Z,
tangents:	$\{Z, i, i'\}$ with $i \in \{1, 2, \ldots, r\}$,
on-points:	$1', 2', \ldots, r'$

(up to now all elements are the same as when using the central-method).

The on-points now are put on a circle one after the other such that they form a regular r-gon. Then the oval secant determined by two neighbouring on-points i', $(i+1)'$ is $\{i', (i+1)', \frac{1}{2}(2i+1)\}$. We have always to calculate modulo r. If i runs from 1 to r then the desired r-chain is already found. Putting all the corresponding ex-points on the circle as well, we obtain a $2r$-gon, a "garland". *Fig. 9* shows such a "garland" in the case $v = 15$, hence $r = 7$.

$v \in$ RSTS

Systems STS(v) with $v \in$ RSTS and $v \neq 9$, 13 (these two cases have already been done with the *Figs 7* and *8*) may be constructed with a direct method using regular ovals [5]. Again the ex-points are denoted by $1, 2, \ldots, r$, the on-points by $1', 2', \ldots, r'$ and the only in-point by the letter M. The ex-points as well as the on-points are put on two circles one after the other with the same center M but different radius. They build two regular r-gons turned around about π/r. Then the oval secant determined by two neighbouring on-points i', $(i+r-1)'$ is $\{i', (i+r-1)', i\}$. If i runs from 1 to r then we have already an r-chain (again we calculate modulo r). Putting all the corresponding ex-points on the circle containing the on-points, we have a $2r$-gon with "garland". In *Fig. 10* we see such a "garland" for the case $v = 33$, hence $r = 16$.

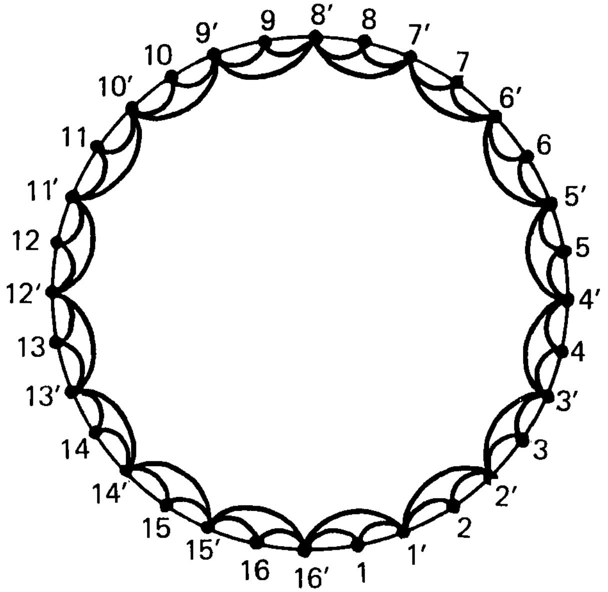


Fig. 10. 16-chain in STS(33).

5. A second multiple method (with chains)

5.1. *The procedure*

Using our central-method we now start with a system STS(r) in which a $\frac{1}{2}(r-1)$-chain is marked. *Fig. 11* shows some lines of this chain. Now we perform the perturbation trick for the first time and start with the passant $\{a_1, b_1, a_2\}$ in *Fig. 11*. The lines $\{K, a_1, a_1'\}$, $\{K, b_1, b_1'\}$, $\{a_2, a_1, b_1\}$, $\{a_2, a_1', b_1'\}$ are deleted and replaced in the usual way by the lines $\{a_2, a_1, a_1'\}$, $\{a_2, b_1, b_1'\}$, $\{K, a_1, b_1\}$, $\{K, a_1', b_1'\}$. In this procedure the points a_1, b_1 are called border points and a_2 central point.

Now we perform the perturbation trick a second time – but not in the way we did in 3.1. Choosing a suitable new passant we have to ensure that with our

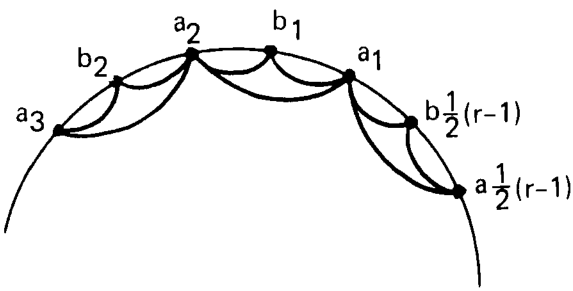


Fig. 11.

x_r	1	0	0	...	0	...
x_{r-2}	0	1	0		0	
x_{r-4}	0	0	1		0	
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	
x_{r-2p}	0	0	0		1	
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	
x_3	0	1	2		p	
x_1	r	r-1	r-2		r-p	

Fig. 12.

construction every ex-point can be at most once a border point, but several times (at most $\frac{1}{2}(r-1)$ times) a central point. It is quite possible that an ex-point is both a border and a central point. Especially favourable for using our trick are the lines of the $\frac{1}{2}(r-1)$-chain.

So we now choose the passant $\{a_2, b_2, a_3\}$ in *Fig. 11*, delete the lines $\{K, a_2, a_2'\}$, $\{K, b_2, b_2'\}$, $\{a_3, a_2, b_2\}$, $\{a_3, a_2', b_2'\}$ and replace these lines by $\{a_3, a_2, a_2'\}$, $\{a_3, b_2, b_2'\}$, $\{K, a_2, b_2\}$, $\{K, a_2', b_2'\}$. The point set $\{1', 2', \ldots, r'\}$ remains an oval. The point Z is still on $r-4$ tangents, the points a_2 and a_3 are on three tangents each. The point a_2 is both a border and a central point. A new type of ovals is found. One of the new tangents contains a_2 and also a_3. Continuing in this way with the connected passants $\{a_3, b_3, a_4\}$, $\{a_4, b_4, a_5\}, \ldots$ in *Fig. 11* we always obtain new Steiner triple systems with new types of ovals.

5.2. *Result*

The table in *Fig. 12* shows the result of our procedure. The notations are the same as in *Fig. 2*.

5.3. *Number of ovals types*

When does the continued execution of the perturbation trick come to an end?

If the number 1 appears on the last but one line, we have $r-2p=3$, therefore $p=\frac{1}{2}(r-3)$. Now we obtain $p+1=\frac{1}{2}(r-1)$ ex-points with exactly 3 tangents and $r-p=\frac{1}{2}(r+3)$ ex-points with exactly one tangent respectively (*Fig. 13* for $v=19$ $(r=9)$).

Our trick may be performed one more time. That is using the last edge of the $\frac{1}{2}(r-1)$-chain. Doing so the number of ex-points with exactly 3 tangents and with exactly one tangent respectively is not changed. But we obtain quite another configuration of the tangents. The tangent in K seems to be in a certain sense isolated. Our system is produced with a $\frac{1}{2}(r-1)$-chain. Therefore in this case a particularly symmetrical representation is possible (*Fig. 14* for $v=19$ $(r=9)$).

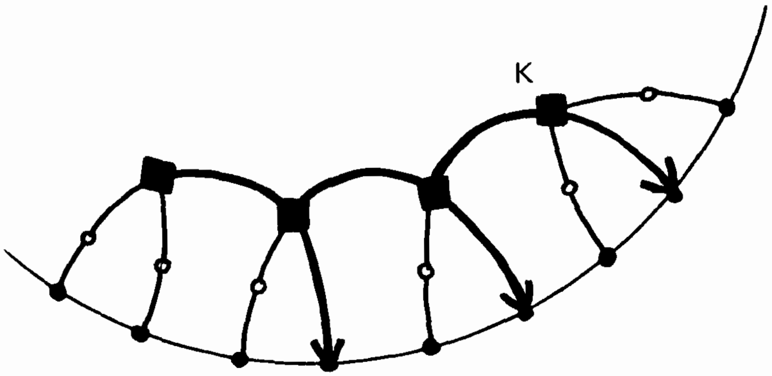


Fig. 13.

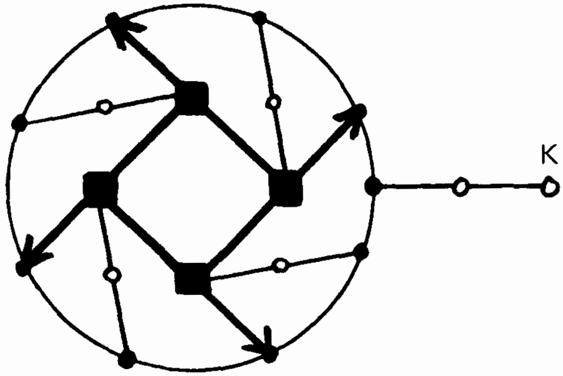


Fig. 14.

Besides the knot oval we obtain $p + 1 = \frac{1}{2}(r - 1)$ further types of ovals. The considerations of this chapter hold for all $v \in$ HSTS. Therefore a partitioning of HSTS as in Section 3 does not result.

6. A further intermediate chapter: parallel classes in STS(v)

6.1. *Parallel classes – what are they?*

Here two lines are called *parallel* if they have no point in common. A set of lines forms a *parallel class* if these lines are pairwise parallel.

6.2 Theorem (Ray-Chauduri, Wilson [3]). *For all $v = 9 + 6n$, $n \in \mathbb{N}_0$, there exist* STS(v) *with a parallelism.*

Systems of this kind are called *resolvable*. In a resolvable STS(v) there are exactly $\frac{1}{2}(v - 1)$ parallel classes each containing exactly $\frac{1}{3}v$ parallel lines.

6.3 Theorem. *For the remaining Steiner number different from 7 – this means for all $v = 13 + 6n$, $n \in \mathbb{N}_0$ – there exist* STS(v) *with a parallel class containing exactly $\frac{1}{3}(v-1)$ parallel lines.*

The projective plane STS(7) must be excepted, because in this system there are no two parallel lines. Using the notation of [7] there exists the parallel class $\{1,3,5\}$, $\{4,7,12\}$, $\{2,9,11\}$, $\{0,8,10\}$ in $\mathrm{STS}_1(13)$ and the parallel class $\{1,2,5\}$, $\{6,7,10\}$, $\{4,9,11\}$, $\{0,3,12\}$ in $\mathrm{STS}_2(13)$. The theorem has been known for a long time [4]. We give here a new proof. In order to do so, write $v = 13 + 12n \in \mathrm{RSTS}$ and $v = 19 + 12n \in \mathrm{HSTS}$ with $n \in \mathbb{N}_0$ respectively instead of $v = 13 + 6n$. We have to distinguish two cases.

$v = 19 + 12n$

As pointed out in Section 4.2 all these systems may be constructed recursively with the polygon-method using STS(r). By 6.2, for $r = 9 + 6n$, $n \in \mathbb{N}_0$ we can start with a resolvable system STS(r). Once more we have to distinguish two cases.

$r = 9 + 12n$

Secants

The secants $\{i', (i+1)', (2i+1)/2\}$ with $i \in \{1, 3, \ldots, r-2\}$ have neither on-points nor ex-points in common. Since $(2i+1)/2 = (2j+1)/2$ we immediately have a contradiction to $i \neq j$. Therefore there are $\frac{1}{2}(r-1)$ secants of this kind.

Tangents

Up to now the on-point $O'(=r')$ and the ex-point $O(=r)$ have not been needed. This fact yields immediately a further line, parallel to the lines already mentioned, namely the tangent $\{Z, O, O'\}$.

Passants

If there exist further parallels then these parallels can be neither secants nor tangents, because all on-points and the point Z are already used. There still remain exactly $r - \frac{1}{2}(r+1) = \frac{1}{2}(r-1)$ ex-points available. We can write $\frac{1}{2}(r-1) = 1 + 3(1+2n)$. So $\frac{1}{2}(r-1) - 1$ is divisible by 3. Now the enumeration of the ex-points is to be done such that all these remaining ex-points form $\frac{1}{3}(\frac{1}{2}(r-1) - 1) = \frac{1}{6}(r-3)$ passants.

Summary

We have found

$$\underbrace{\tfrac{1}{2}(r-1)}_{\text{secants}} + \underbrace{1}_{\text{tangent}} + \underbrace{\tfrac{1}{6}(r-3)}_{\text{passants}} = \tfrac{2}{3}r = \tfrac{1}{3}(v-1)$$

mutually parallel lines in total.

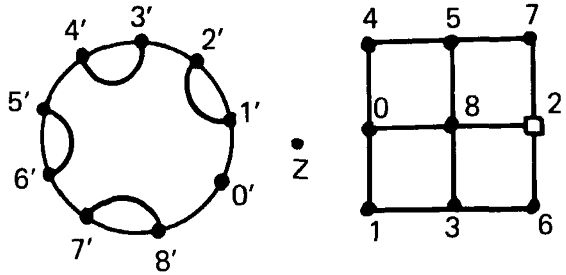


Fig. 15.

Example

In the case $v = 19$ ($r = 9$) we take from *Fig. 15* the parallel class found in this way.

Secants: $\{1', 2', 6\}$, $\{3', 4', 8\}$, $\{5', 6', 1\}$, $\{7', 8', 3\}$;
Tangent: $\{Z, O, O'\}$; Passant: $\{4, 5, 7\}$.

$r = 15 + 12n$

The construction of parallel secants we used in the last case does not work here. The reason is that $\frac{1}{2}(r-1) = 7 + 6n$ now is odd. Therefore we modify the construction a little bit.

Secants

The secants $\{i', (i+1)', (2i+1)/2\}$ with $i \in \{2, 4, \ldots, r-5\}$, $\{1', (r-2)', (r-1)/2\}$, $\{(r-1)', (r-3)', r-2\}$ have no on-points in common. The on-point O' does not occur. It has to be shown that all the ex-points we used are different to one another and to O. This can be shown by contradiction. So for instance with $(2i+1)/2 = (r-1)/2$ we immediately obtain $i = \frac{1}{2}(r-2) = \frac{1}{2}(13+12n) = \frac{1}{2}(28+24n) = 14 + 12n$. This is already a contradiction because $14 + 12n > r - 5$, therefore there are $\frac{1}{2}(r-1)$ secants of this kind.

Now all the missing parallel lines may be found as in the last case.

Example

In the case $v = 31$ ($r = 15$) we take from *Fig.* 16 the parallel class found in this way.

Secants: $\{2', 3', 10\}$, $\{4', 5', 12\}$, $\{6', 7', 14\}$, $\{8', 9', 1\}$, $\{10', 11', 3\}$, $\{12', 14', 13\}$, $\{1', 13', 7\}$; Tangent: $\{Z, O, O'\}$; Passants: $\{2, 4, 5\}$, $\{6, 8, 9\}$.

$v = 13 + 12n$

Now we work again with the construction given in [5] using a regular oval. It is useful to write $r = 12 + 12n$ and $r = 6 + 12n$ with $n \in \mathbb{N}_0$, instead of $r = 6 + 6n$.

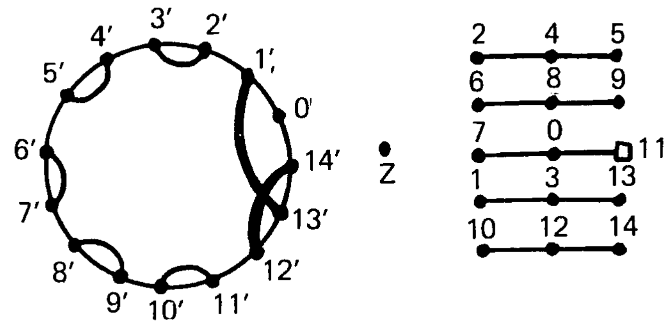


Fig. 16.

$r = 12 + 12n$

Secants

The secants $\{i', (i+1)', i-1\}$ with $i \in \{1, 3, \ldots, r-1\}$ are mutually parallel. Now already $\frac{1}{2}r$ ex-points are used, namely $2, 4, \ldots, O$. The ex-points $1, 3, \ldots, r-1$ as well as the in-point M still remain available. If there exist further parallels then these parallels can be neither secants nor tangents. Because all on-points have already been used.

Passants

Following [5] there exist $\frac{1}{3}r$ passants of the form $\{x, x+\frac{1}{3}r, x+\frac{2}{3}r\}$. These three numbers are either even or they are all odd. We take off all the passants with odd numbers:

$$\{1,\ 1+\tfrac{1}{3}r,\ 1+\tfrac{2}{3}r\},\ \{3,\ 3+\tfrac{1}{3}r,\ 3+\tfrac{2}{3}r\}, \ldots$$

So we obtain $\frac{1}{6}r$ lines parallel to one another and to the lines already chosen. The point M is left over.

Summary

We have found

$$\underset{\text{secants}}{\tfrac{1}{2}r} + \underset{\text{passants}}{\tfrac{1}{6}r} = \tfrac{2}{3}r = \tfrac{1}{3}(v-1)$$

mutually parallel lines in total.

Example

In the case $v = 25$ $(r = 12)$ we take from *Fig. 17* the parallel class found in this way.

Secants: $\{1', 2', 2\}$, $\{3', 4', 4\}$, $\{5', 6', 6\}$, $\{7', 8', 8\}$, $\{9', 10', 10\}$, $\{11', 0', 0\}$;
Passants: $\{1, 5, 9\}$, $\{3, 7, 11\}$.

$r = 6 + 12n$

Following [5] the proof in this case works completely analogously to the last

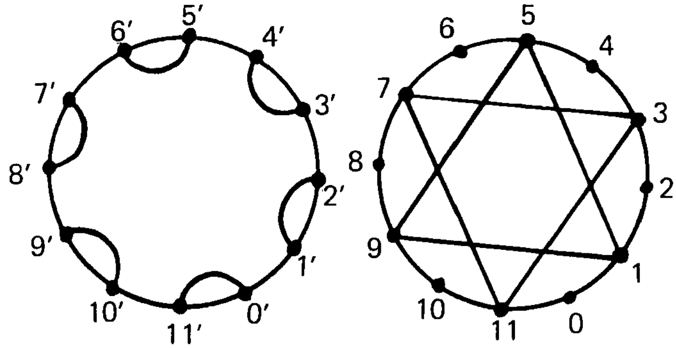


Fig. 17.

one. Here once more a survey of all the cases dealt with in the Theorem 6.2 and 6.3.

$v = 9 + 6n$

$v = 13 + 6n$

$v = 13 + 12n$, $r = 6 + 6n$ $\qquad$ $v = 19 + 12n$, $r = 9 + 6n$

$r = 6 + 12n$ $\qquad$ $r = 12 + 12n$ $\qquad$ $r = 9 + 12n$ $\qquad$ $r = 15 + 12n$

7. A third multiple method (with parallels)

7.1. *The procedure*

In the central construction we now choose a starting system STS(r) with a parallel class $\{a_1, b_1, c_1\}$, $\{a_2, b_2, c_2\}, \ldots, \{a_i, b_i, c_i\}$ as in 6.2 and in 6.3. Then we perform the perturbation to these lines one after the other so that the points $c_1, c_2, \ldots, c_i$ lie on exactly 3 tangents and Z lies on exactly $r - 2i$ tangents. Continuing we always obtain new systems and new ovals.

7.2. *Result*

The table in *Fig.* 12 shows the result of our construction not only using chains but also using parallel lines. It is possible to suppose that nothing has changed. Indeed the number of points with a certain number of tangents is the same. But the configurations of tangents are totally different.

7.3. *Number of ovals types*

When does the continued performing of the perturbation trick come to an end?

$v = 19 + 12n$, *therefore* $r = 9 + 6n$ $(v \neq 7)$.

The parallel class we use contains exactly $\frac{1}{3}r$ lines, therefore after $p = \frac{1}{3}r$ steps the procedure comes to an end. Now we have $p = \frac{1}{3}r$ ex-points with exactly 3 tangents, $r - p = \frac{2}{3}r$ ex-points with exactly one tangent and one ex-point with exactly $r - 2p = \frac{1}{3}r$ tangents (*Fig. 18* for $v = 19$ $(r = 9)$). This type of oval is denoted by O_3. Besides the knot oval we obtain $p = \frac{1}{3}r$ further types of ovals.

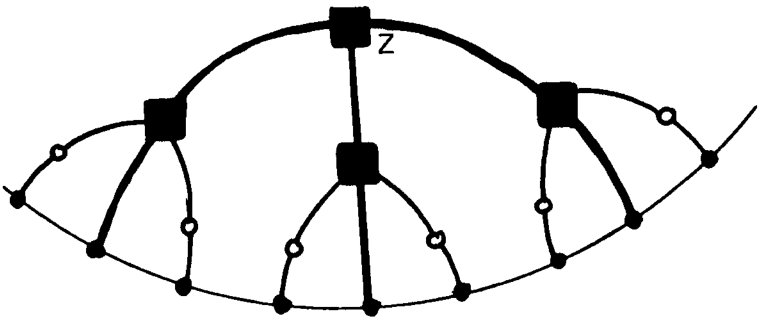


Fig. 18.

$v = 27 + 12n$, *therefore* $r = 13 + 16n$ $(v \neq 15)$.

The parallel class we use contains exactly $\frac{1}{3}(r-1)$ lines, therefore after $p = \frac{1}{3}(r-1)$ steps the procedure comes to an end. Now we have $p = \frac{1}{3}(r-1)$ ex-points with exactly 3 tangents, $r - p = \frac{1}{3}(2r+1)$ ex-points with exactly one tangent and one ex-point with exactly $\frac{1}{3}(r+2)$ tangents (*Fig. 19* for $v = 27$ $(r = 13)$). This type of oval is denoted by O_4. Besides the knot oval we obtain $p = \frac{1}{3}(r-1)$ further types of ovals.

7.4 Theorem.

Exactly as in 3.3.4 we summarize the results of this section in a theorem.

Exactly for all $v \in \mathrm{H_3STS}$ *there exist systems* $\mathrm{STS}(v)$ *with an oval* O_3. *Exactly for all the remaining Steiner number of* HSTS *different from* 7 *and* 15, *namely for all* $v \in \mathrm{H_4STS}$ *there exist systems* $\mathrm{STS}(v)$ *with an oval* O_4.

We have

$\mathrm{H_3STS}$: $v = 19 + 12n$ or $v = 19, 31 + 24n$;
$\mathrm{H_4STS}$: $v = 27 + 12n$ or $v = 27, 39 + 24n$;
$n \in \mathbb{N}_0$; $\mathrm{HSTS} = \mathrm{H_3STS} \cup \mathrm{H_4STS} \cup \{7, 15\}$.

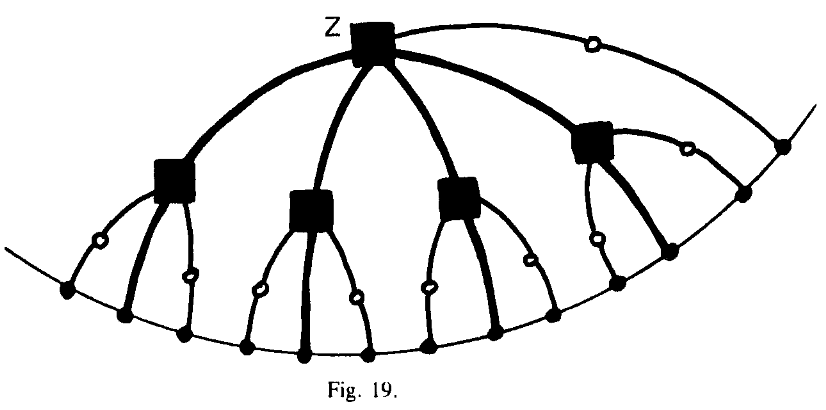


Fig. 19.

So the disjoint sets H_3STS and H_4STS are also characterized in a geometrical way when ovals are used.

8. Theorem.

The Theorems 3.3.4 and 7.4 now are combined in one theorem.

Exactly for all Steiner numbers $v \in H_{st}$ there exist a system STS(v) *with an oval O_s as well as a system* STS(v) *with an oval O_t.*

We have

H_{13}: $v = 19 + 24n$; H_{14}: $v = 27 + 24n$; H_{24}: $v = 39 + 24n$;
H_{23}: $v = 31 + 24n$; $n \in \mathbb{N}_0$; $\mathrm{HSTS} = H_{13} \cup H_{14} \cup H_{23} \cup H_{24} \cup \{7, 15\}$.

Now even the four sets H_{st} are characterized in a geometrical way when ovals are used.

Remarks. (1) *Isomorphism*

It remains to be shown that the systems of the same order v constructed in the Section 3, 5 and 7 are mutually non-isomorphic (except the systems with knot ovals).

(2) *Polygon-construction*

Using the polygon-construction – instead of the central-construction – in [6] the perturbation trick with pencils was already performed. In an analogous way this may also be done with chains and parallels. All the systems of the same order then obtained have to be compared with one another as well as with the systems produced by the central-method and then investigated with respect to isomorphism.

(3) *Combination*

The three treated multiplying methods may be combined in various ways. Thus we obtain an immense number of further Steiner triple systems with new oval types.

(4) *Diophantine equations*

With our constructions we obtain solutions of the system of two linear diophantine equations given in [5]. It should be noticed that one solution may yield quite different kinds of ovals.

References

[1] K. Lang and H. Zeitler, Zur Klassifikation von Steinerzahlen, Resultate der Mathematik 8 (1985) 47–53.

[2] H. Lenz and H. Zeitler, Arcs and ovals in Steiner Triple Systems, Lecture Notes in Mathematics 969 (1982) 229–250.

[3] D.K. Ray-Chauduri and R.M. Wilson, Solution of Kirkmans school-girl problem, Proceedings Symposia in Pure Mathematics 19 (1971) 187–204.

[4] J. Schönheim, On the number of mutually disjoint triples in Steiner systems and related maximal packing and minimal covering systems, Recent Progress in Combinatorics, Proc. 3rd Waterloo Conf. 1968 (Academic Press, New York, 1969) 311–318.
[5] H. Zeitler and H. Lenz, Regular ovals in Steiner Triple Systems, J. Combin., Information and System Sciences, Neu-Delhi 9 (1984) 155–162.
[6] H. Zeitler, Eine Klasse gemischter Ovale in STS(v), J. Geometry 33 (1988) 185–202.
[7] H. Zeitler, Miszellen zum Thema Ovale in Steiner tripelsystemen, Annales Universitatis Scienciarum Budapestiensis de Rolando Eötvös Nominatae sectio Matematica XXXI (1988) 3–17.

Discrete Mathematics 77 (1989) 385–386
North-Holland

AUTHOR INDEX

Volume 77 (1989)