

Design Theory

Second Edition

Thomas Beth
Universität Karlsruhe

Dieter Jungnickel
Universität Augsburg

Hanfried Lenz
Freie Universität Berlin

Volume II

 **CAMBRIDGE**
UNIVERSITY PRESS

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK www.cup.cam.ac.uk
40 West 20th Street, New York, NY 10011-4211, USA www.cup.org
10 Stamford Road, Oakleigh, Melbourne 3166, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain

First edition © Bibliographisches Institut, Zurich, 1985
© Cambridge University Press, 1993
Second edition © Cambridge University Press, 1999

This book is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without
the written permission of Cambridge University Press.

First published 1999

Printed in the United Kingdom at the University Press, Cambridge

Typeset in Times Roman 10/13pt. in L^AT_EX 2_ε [TB]

A catalogue record for this book is available from the British Library

Library of Congress Cataloguing in Publication data

Beth, Thomas, 1949–

Design theory / Thomas Beth, Dieter Jungnickel, Hanfried Lenz. –
2nd ed.

p. cm.

Includes bibliographical references and index.

ISBN 0 521 77231 1 (hardbound)

1. Combinatorial designs and configurations. I. Jungnickel, D.
(Dieter), 1952– . II. Lenz, Hanfried. III. Title.

QA166.25.B47 1999

511'.6 – dc21 98-29508 CIP

ISBN 0 521 77231 1 hardback

Contents

IX. Recursive constructions	608
§1. Product constructions	608
§2. Use of pairwise balanced designs	617
§3. Applications of divisible designs	621
§4. Applications of Hanani's lemmas	627
§5. Block designs of block size three and four	636
§6. Solution of Kirkman's schoolgirl problem	641
§7. The basis of a closed set	644
§8. Block designs with block size five	651
§9. Divisible designs with small block sizes	660
§10. Steiner quadruple systems	664
§11. Embedding theorems for designs and partial designs	673
§12. Concluding remarks	681
X. Transversal designs and nets	690
§1. A recursive construction	690
§2. Transversal designs with $\lambda > 1$	693
§3. A construction of Wilson	696
§4. Six and more mutually orthogonal Latin squares	703
§5. The theorem of Chowla, Erdős and Straus	706
§6. Further bounds for transversal designs and orthogonal arrays	708
§7. Completion theorems for Bruck nets	713
§8. Maximal nets with large deficiency	725
§9. Translation nets and maximal nets with small deficiency	731

§10. Completion results for $\mu > 1$	749
§11. Extending symmetric nets	758
§12. Complete mappings, difference matrices and maximal nets . . .	761
§13. Tarry's theorem	772
§14. Codes of Bruck nets	778
XI. Asymptotic existence theory	781
§1. Preliminaries	781
§2. The existence of Steiner systems with v in given residue classes	783
§3. The main theorem for Steiner systems $S(2, k; v)$	787
§4. The eventual periodicity of closed sets	790
§5. The main theorem for $\lambda = 1$	793
§6. The main theorem for $\lambda > 1$	796
§7. An existence theorem for resolvable block designs	801
§8. Some results for $t \geq 3$	805
XII. Characterisations of classical designs	806
§1. Projective and affine spaces as linear spaces	806
§2. Characterisations of projective spaces	808
§3. Characterisation of affine spaces	821
§4. Locally projective linear spaces	828
§5. Good blocks	833
§6. Concluding remarks	841
XIII. Applications of designs	852
§1. Introduction	852
§2. Design of experiments	856
§3. Experiments with Latin squares and orthogonal arrays	874
§4. Application of designs in optics	880
§5. Codes and designs	892
§6. Discrete tomography	926
§7. Designs in data structures and computer algorithms	930
§8. Designs in hardware	937
§9. Difference sets rule matter and waves	946
§10. No waves, no rules, but security	956
Appendix. Tables	971
§1. Block designs	971
§2. Symmetric designs	981

§3. Abelian difference sets	990
§4. Small Steiner systems	997
§5. Infinite series of Steiner systems	999
§6. Remark on t -designs with $t \geq 3$	1001
§7. Orthogonal Latin squares	1002
Notation and symbols	1005
Bibliography	1013
Index	1093

Contents of Volume I

I. Examples and basic definitions	1
§1. Incidence structures and incidence matrices	1
§2. Block designs and examples from affine and projective geometry	6
§3. t -designs, Steiner systems and configurations	15
§4. Isomorphisms, duality and correlations	20
§5. Partitions of the block set and resolvability	24
§6. Divisible incidence structures	32
§7. Transversal designs and nets	37
§8. Subspaces	44
§9. Hadamard designs	50
II. Combinatorial analysis of designs	62
§1. Basics	62
§2. Fisher's inequality for pairwise balanced designs	64
§3. Symmetric designs	77
§4. The Bruck–Ryser–Chowla theorem	89
§5. Balanced incidence structures with balanced duals	96
§6. Generalisations of Fisher's inequality and intersection numbers	101
§7. Extensions of designs	111
§8. Affine designs	123
§9. Strongly regular graphs	136
§10. The Hall–Connor theorem	146
§11. Designs and codes	152

III. Groups and designs	162
§1. Introduction	162
§2. Incidence morphisms	163
§3. Permutation groups	167
§4. Applications to incidence structures	173
§5. Examples from classical geometry	184
§6. Constructions of t -designs from groups	190
§7. Extensions of groups	198
§8. Construction of t -designs from base blocks	206
§9. Cyclic t -designs	218
§10. Cayley graphs	225
IV. Witt designs and Mathieu groups	234
§1. The existence of the Witt designs	234
§2. The uniqueness of the small Witt designs	237
§3. The little Mathieu groups	243
§4. Properties of the large Witt design $S(5, 8; 24)$	244
§5. Some simple groups	252
§6. Witt's construction of the Mathieu groups and Witt designs	259
§7. Hussain structures and the uniqueness of $S_2(3, 6; 12)$	262
§8. The Higman–Sims group	270
V. Highly transitive groups	277
§1. Sharply t -transitive groups	277
§2. t -homogeneous groups	283
§3. Concluding remarks: t -transitive groups	291
VI. Difference sets and regular symmetric designs	297
§1. Basic facts	298
§2. Multipliers	303
§3. Group rings and characters	311
§4. Multiplier theorems	319
§5. Difference lists	330
§6. The Mann test and Wilbrink's theorem	335
§7. Planar difference sets	344
§8. Paley–Hadamard difference sets and cyclotomy	353
§9. Some difference sets with $\gcd(v, n) > 1$	363
§10. Relative difference sets and building sets	369

§11. Extended building sets and difference sets	382
§12. Constructions for Hadamard and Chen difference sets	388
§13. Some applications of algebraic number theory	410
§14. Further non-existence results	419
§15. Characters and cyclotomic fields	435
§16. Schmidt's exponent bound	441
§17. Difference sets with Singer parameters	455
VII. Difference families	468
§1. Basic facts	468
§2. Multipliers	472
§3. More examples	476
§4. Triple systems	481
§5. Some difference families in Galois fields	488
§6. Blocks with evenly distributed differences	499
§7. Some more special block designs	502
§8. Proof of Wilson's theorem	509
VIII. Further direct constructions	520
§1. Pure and mixed differences	520
§2. Applications to the construction of resolvable block designs	528
§3. A difference construction for transversal designs	531
§4. Further constructions for transversal designs	544
§5. Some constructions using projective planes	564
§6. t -designs constructed from graphs	584
§7. The existence of t -designs for large values of λ	588
§8. Higher resolvability of t -designs	595
§9. Infinite t -designs	598
§10. Cyclic Steiner quadruple systems	600
Notation and symbols	1005
Bibliography	1013
Index	1093

Chapters IX–XIII plus the appendices can be found in Volume II. The complete bibliography and index for both volumes is included here.

IX

Recursive Constructions

Alabado sea la infinita
 Urdimbre de los efectos y de las causas. . .
(Borges)

In the first few sections of this chapter we shall develop some important recursive construction methods which will be applied to mutually orthogonal Latin squares, pairwise balanced designs, and in particular block designs.

§1. Product Constructions

In this section, we consider some product constructions. The first two of these concern difference matrices and are due to Jungnickel (1979) and Shrikhande (1964), respectively; the simple proofs are left to the reader. We note that Shrikhande's result generalises Lemma I.9.6.

1.1 Lemma. *Let $A = (a_{ij})$ be a $(g, k; \lambda)$ -difference matrix and $B = (b_{ij})$ an $(h, k; \mu)$ -difference matrix over the (additively written) respective finite groups G and H . Then the $k \times \lambda\mu gh$ -matrix*

$$\left(\begin{array}{ccc|ccc|cccc} (a_{11}, b_{11}) & \dots & (a_{11}, b_{1n}) & (a_{12}, b_{11}) & \dots & (a_{12}, b_{1n}) & \dots & \dots & (a_{1m}, b_{1n}) \\ \dots & \dots \\ \dots & \dots \\ (a_{k1}, b_{k1}) & \dots & (a_{k1}, b_{kn}) & (a_{k2}, b_{k1}) & \dots & (a_{k2}, b_{kn}) & \dots & \dots & (a_{km}, b_{kn}) \end{array} \right)$$

is a $(gh, k; \lambda\mu)$ -difference matrix over $G \oplus H$, where $m = \lambda g$ and $n = \mu h$. ■

1.2 Lemma. *Let A be an $OA_\lambda(k, g)$ with entries in a finite group G and let $D = (d_{ij})$ ($i = 1, \dots, k', j = 1, \dots, g\lambda'$) be a $(g, k'; \lambda')$ -difference matrix*

over $G = \{\gamma_1, \dots, \gamma_g\}$. Then the matrix $A \otimes D$ defined by

$$A \otimes D = \begin{pmatrix} a_{11} + D & \dots & a_{1,g^2\lambda} + D \\ \cdot & & \cdot \\ \cdot & & \cdot \\ a_{k1} + D & \dots & a_{k,g^2\lambda} + D \end{pmatrix}$$

is an $OA_{\lambda\lambda'}(kk', gg')$.¹

If E is a (g, k, λ) -difference matrix, then $E \otimes D$ is a $(g, kk', g\lambda\lambda')$ -difference matrix. In particular, the Kronecker product of two generalised Hadamard matrices (VIII.3.4) is a generalised Hadamard matrix. ■

1.3 Example. The existence of $(3, 3; 1)$ - and $(3, 6; 2)$ -difference matrices (see Theorem VIII.3.14) implies that of a $(3, 18; 6)$ -difference matrix over $\mathbb{Z}_3 \times \mathbb{Z}_6$. More generally, we obtain $(3, 3\lambda; \lambda)$ -difference matrices for all $\lambda = 2^i 3^j$ with $j \geq i - 1$. All these difference matrices are generalised Hadamard matrices.

1.4 Definition. Let $(A, \circ), (B, *)$ be quasigroups (see Definition VIII.4.10). Their *direct product* is defined as the set $A \times B$ with the operation \square defined by

$$(1.4.a) \quad (a, b) \square (a', b') := (a \circ a', b * b').$$

1.5 Lemma. Let (A, \circ) and (A, \circ') be orthogonal quasigroups, and let $(B, *)$, $(B, *')$ be orthogonal quasigroups too. Then the direct products $(A, \circ) \times (B, *)$ and $(A, \circ') \times (B, *')$ are orthogonal quasigroups. If (A, \circ) and $(B, *)$ are idempotent, then $(A, \circ) \times (B, *)$ is also idempotent. ■

The proof is straightforward. Again MacNeish's theorem (I.7.7.b) follows immediately; furthermore

$$(1.5.a) \quad N^*(gh) \geq \min\{N^*(g), N^*(h)\}.$$

For the sake of completeness we mention the following connection between quasigroups and Steiner triple systems.

¹ Note that this would be the Kronecker product of matrices if G were written multiplicatively.

1.6 Observations. Define a binary operation \circ on the point set V of an $S(2,3;v)$ by

$$(1.6.a) \quad a \circ b = c \quad \text{if } a \neq b \text{ and } \{a, b, c\} \text{ is a line,}$$

$$(1.6.b) \quad a \circ a = a \quad \text{for all } a \in V.$$

Then (V, \circ) is an idempotent quasigroup with the properties

$$(1.6.c) \quad x \circ y = y \circ x,$$

$$(1.6.d) \quad x \circ (x \circ y) = y \quad \text{for all } x, y \in V.$$

Conversely, every finite idempotent quasigroup satisfying (1.6.c) and (1.6.d) determines an *STS* by the rule: x, y, z are on a line iff $x \neq y$ and $x \circ y = z$.

1.7 Lemma. *Let (V, \circ) and $(W, *)$ be idempotent quasigroups which satisfy (1.6.c, d). Then $(V, \circ) \times (W, *)$ has the same properties. ■*

The proof is straightforward.

1.8 Corollary.

$$(1.8.a) \quad u, v \in B(3) \Rightarrow uv \in B(3). \quad \blacksquare$$

Next we mention analogous properties of Steiner quadruple systems.

1.9 Observations. Let an *SQS* be given. Define a ternary operation f on the point set V by

$$(1.9.a) \quad f(x, y, z) := u \quad \text{if } |\{x, y, z\}| = 3 \text{ and } \{x, y, z, u\} \text{ is a block;}$$

$$(1.9.b) \quad f(x, x, y) = f(x, y, x) = f(y, x, x) := y \quad \text{for all } x, y \in V.$$

Then f has the properties

$$(1.9.c) \quad f(x, y, z) = f(y, x, z) = f(x, z, y),$$

$$(1.9.d) \quad f(x, y, f(x, y, z)) = z \quad \text{for all } x, y, z \in V,$$

and the equation

$$(1.9.e) \quad f(a, b, x) = c$$

has a unique solution x for all $a, b, c \in V$. Conversely, every ternary algebra with these three properties determines an *SQS* by the following rule. Four

distinct points a, b, c, d are on a block iff $f(a, b, c) = d$. If (V, f) and (W, g) are such ternary algebras, then their direct product, defined in the obvious way, has the same properties. Hence

$$(1.9.f) \quad u, v \in S(3, 4) \Rightarrow uv \in S(3, 4).$$

Note that $2 \in S(3, 4)$ (two points, no blocks), and that a ternary operation \circ on a 2-set, satisfying (1.9.b), has all the properties of 1.9. Hence (1.9.f) specializes to

$$(1.9.g) \quad 2 \cdot S(3, 4) \subseteq S(3, 4).$$

In view of Hanani's theorem stating that $S(3, 4) = 2\mathbb{N} \setminus 6\mathbb{N}$, (1.9.f) is a very weak result; see §10 for a proof of Hanani's theorem.

1.10 Remark. These examples may be generalised to the idea of applying universal algebra to combinatorial structures; cf. Ganter (1976a), Evans (1975), Quackenbush (1975). A nice introductory paper on this subject was given by Evans (1979).

Next we shall use difference matrices and orthogonal arrays for product constructions of difference families, as well as the other way round.

1.11 Proposition. *Let k be the order of an affine plane. Furthermore, let $A = (a_{ij})$ be an $OA(k, k)$ over $S = \mathbb{N}_1^k$. Moreover, let $\mathbf{D} = (D_1, \dots, D_s)$ and $\mathbf{E} = (E_1, \dots, E_t)$ be difference families in the groups G and G' with parameters (v, k, λ) and (v', k, λ') , respectively, say $D_i = \{d_{i1}, \dots, d_{ik}\}$ and $E_j = \{e_{j1}, \dots, e_{jk}\}$ for $i \in \mathbb{N}_1^s$ and $j \in \mathbb{N}_1^t$. Then there is a $(vv', k, \lambda\lambda')$ -difference family in $G \oplus G'$.*

Proof. We may assume that the last k columns of A are $(1, 1, \dots, 1)^T, \dots, (k, k, \dots, k)^T$. We omit these k columns and get a $k \times k(k-1)$ -matrix $B = (b_{ij})$. Now let the desired difference family \mathbf{F} consist of the following base blocks:

- λ' copies of $\{(d_{i1}, 0), \dots, (d_{ik}, 0)\}$ for each $i \in \mathbb{N}_1^s$;
- λ copies of $\{(0, e_{j1}), \dots, (0, e_{jk})\}$ for each $j \in \mathbb{N}_1^t$;
- one copy of $\{(d_{i1}, e_{jb_{in}}), \dots, (d_{ik}, e_{jb_{kn}})\}$ for each $n \in \mathbb{N}_1^{k^2-k}$
and each pair $(i, j) \in \mathbb{N}_1^s \times \mathbb{N}_1^t$.

The somewhat lengthy though not difficult verification of this construction is left to the reader; cf. Jungnickel (1978). ■

1.12 Corollary. *With notation as in VII.5.3, for prime powers k we have*

$$(1.12.a) \quad v \in D_\lambda(k) \quad \text{and} \quad v' \in D_{\lambda'}(k) \quad \Rightarrow \quad vv' \in D_{\lambda\lambda'}(k);$$

in particular

$$(1.12.b) \quad v, v' \in D(k) \Rightarrow vv' \in D(k). \quad \blacksquare$$

1.13 Examples. (a) Let q and $q + 1$ be prime powers and $n \in \mathbb{N}$. Then there is a $((q^2 + q + 1)^n, q + 1, 1)$ -difference family in $(\mathbb{Z}_{q^2+q+1})^n$. The case $n = 1$ is just a Singer difference set, see Theorem VI.1.10. Note that the result also follows from Lemma VII.5.5 if $q^2 + q + 1$ is also a prime power (e.g. for $q = 2, 3, 8$), but not for $q = 4, 7, 16, 31, 127$.

(b) Let $v = q_1 \dots q_n$ be the prime power factorisation of v and assume

$$q_i \equiv 1 \pmod{6} \quad \text{for } i = 1, \dots, n.$$

Then there is a $(v, 3, 1)$ -difference family in $EA(q_1) \oplus \dots \oplus EA(q_n)$, by (VII.5.4.a) and Proposition 1.11.

(c) Let k be a prime power and assume that each factor q in the prime power factorisation of v is congruent to $1 \pmod{k(k-1)}$ and sufficiently large. Then, by Wilson's Theorem VII.6.6 and Corollary 1.12, there is a $(v, k, 1)$ -difference family. The existence of difference families for given k, λ and all sufficiently large v satisfying the necessary condition (VII.1.9.b) is an unsettled question.

1.14 Proposition. *Assume the existence of a (v, k, λ) -difference family $\mathbf{D} = (D_1, \dots, D_s)$ in G and of both a $(g, k, \lambda\lambda')$ -difference family $\mathbf{E} = (E_1, \dots, E_t)$ and a (g, k, λ') -difference matrix $A = (a_{ij})$ in G' . Then there is a $(gv, k, \lambda\lambda')$ -difference family \mathbf{F} in $G \oplus G'$.*

Proof. As base blocks of \mathbf{F} take

$$\{0\} \times E_j \quad \text{for } j \in \mathbb{N}_1^t$$

and

$$\{(d_{i1}, a_{1j}), \dots, (d_{ik}, a_{kj})\} \quad \text{for all } (i, j) \in \mathbb{N}_1^s \times \mathbb{N}_1^{g\lambda'},$$

where $D_i = \{d_{i1}, \dots, d_{ik}\}$. Then it is easily checked that \mathbf{F} is a $(gv, k, \lambda\lambda')$ -difference family; cf. Jungnickel (1978). \blacksquare

1.15 Examples. (a) Proposition 1.14 and Lemma VIII.3.10 yield alternative proofs for Examples 1.13.(b), (c). An alternative proof of Example 1.13.(a) will be given a little later.

(b) Using Proposition 1.14, Lemma VIII.3.10 and Wilson's Theorem VII.6.6, we obtain the existence of a (v, k, λ) -difference family whenever v admits a prime power factorisation

$$(1.15.a) \quad v = q_1 q_2 \dots q_n$$

with $\lambda(q_i - 1) \equiv 0 \pmod{k(k-1)}$, where the q_i ($i = 1, \dots, n$) are sufficiently large.

(c) Assume that k or $k - 1$ divides 2λ . Then there exists a (v, k, λ) -difference family whenever each factor q_i in the prime power factorisation of v satisfies the condition

$$(1.15.b) \quad \lambda(q_i - 1) \equiv 0 \pmod{k(k-1)}.$$

This follows from Lemma 1.1 (with $\lambda' = 1$), together with Lemma VIII.3.10. Thus, for example, we obtain (compare with Examples VII.5.4)

$$(1.15.c) \quad v \in D_1(3) \cap D_2(4) \cap D_5(6) \cap D_6(7),$$

whenever $q_i \equiv 1 \pmod{6}$ for $i = 1, \dots, m$;

$$(1.15.d) \quad v \in D_2(5) \cap D_3(6),$$

whenever $q_i \equiv 1 \pmod{10}$ for $i = 1, \dots, n$;

$$(1.15.e) \quad v \in D_3(7) \cap D_4(8),$$

whenever $q_i \equiv 1 \pmod{14}$ for $i = 1, \dots, n$;

$$(1.15.f) \quad v \in D_4(9),$$

whenever $q_i \equiv 1 \pmod{18}$ for $i = 1, \dots, n$.

(d) Let $t, n \in \mathbb{N}$ and $4t - 1$ be a prime power. Then

$$(1.15.g) \quad (4t - 1)^n \in D_{t-1}(2t - 1).$$

This result follows by using a Paley difference set (Theorem VI.1.12), and is a special case of (c).

(e) There is a $(91, 10, 1)$ -difference set in \mathbb{Z}_{91} (Theorem VI.1.10). Also there are $(13, 13; 1)$ -difference matrices (Lemma VIII.3.10), and $(7, 14; 2)$ -difference

matrices (Theorem VIII.3.14). Thus there is a $(91, 10; 2)$ -difference matrix in \mathbb{Z}_{91} by Lemma 1.1. Hence by an easy induction,

$$(1.15.h) \quad 91^n \in D_{2^{n-1}}(10) \quad \text{for every } n \in \mathbb{N}.$$

1.16 Exercises. (a) Show the existence of $(133^n, 12, 2^{n-1})$ -difference families and of $(16^m 31^n, 6, 2^m)$ -difference families ($m, n \in \mathbb{N}$).

(b) Assume that $q^d + \dots + q + 1$ is a prime power. Show that, for $n \in \mathbb{N}$,

$$(q^d + \dots + q + 1)^n \in D_\lambda(q^{d-1} + \dots + q + 1) \text{ with } \lambda = q^{d-2} + \dots + q + 1,$$

$$(q^{d+1} + \dots + q + 1)^n \in D_\lambda(q^d + \dots + q + 1) \text{ with } \lambda = q^{d-1} + \dots + q + 1.$$

In a certain sense, Propositions 1.11 and 1.14 are complementary. In 1.11 one uses information on k and in 1.14 information on g . Proposition 1.11 has the advantage of allowing the combination of (v, k, λ) -difference families for $\lambda > 1$ without enlarging the λ -value. In Proposition 1.14 we used difference matrices to construct difference families. The converse is done in the following construction; cf. Jungnickel (1979).

1.17 Proposition. *Assume the existence of a (v, g, λ) -difference family over G and of a $TD[k; g]$ with a parallel class. Then there exists a $(v, k; \lambda)$ -difference matrix over G .*

Proof. The existence of a parallel class allows us to assume that $(1, \dots, 1)^T, \dots, (g, \dots, g)^T$ are columns of an $OA(g, k; 1)$ corresponding to the given $TD[k; g]$. As in the proof of Proposition 1.11, we drop these columns and obtain a $(k \times g(g-1))$ -matrix $B = (b_{mn})$ over \mathbb{N}_1^g . Let $D_i = (d_{i1}, \dots, d_{ig})$ be the i -th base block in the given (v, g, λ) -difference family $\mathbf{D} = (D_1, \dots, D_s)$ and replace each entry b_{mn} of B by $d_{i b_{mn}}$. This yields a $k \times g(g-1)$ -matrix A_i . Put

$$A := (A_1 A_2 \dots A_s 0),$$

where 0 denotes a $k \times \lambda$ -zero matrix. Now consider rows h and l of A . The difference 0 occurs λ times from the zero matrix used. As the submatrix of B determined by rows h and l contains in its columns each pair with distinct entries precisely once, we obtain the difference $d_{i\beta} - d_{i\gamma}$ ($\beta \neq \gamma$) from A_i exactly once, by our construction. As \mathbf{D} was a (v, g, λ) -difference family, $(A_1 A_2 \dots A_s)$ yields each non-zero element of G exactly λ times from rows h and l . ■

Note that $s = \frac{b}{v} = \lambda \frac{v-1}{g(g-1)}$, hence the column number of A is $sg(g-1) + \lambda = v$, as it must be.

1.18 Examples. (a) Let q be a prime power and assume the existence of a $TD[k; q+1]$ with a parallel class. Then there exists a $(q^2 + q + 1, k; 1)$ -difference matrix in \mathbb{Z}_{q^2+q+1} by Singer's Theorem VI.1.10.

(b) There are $(15, 7; 3)$ -, $(21, 5; 1)$ -, $(40, 13; 4)$ -, and $(57, 8; 1)$ -difference matrices in the cyclic groups of the respective orders. The reader is asked to check this.

(c) Let q be a prime power and let G be a group of order $q+1$. Then there is a $(q+1, q; q-1)$ -difference matrix over G . To see this, use the trivial $(q+1, q, q-1)$ -difference set $G \setminus \{0\}$. Note that this yields non-abelian difference matrices too (though of moderate size; the maximum feasible value of k is $q^2 - 1$ by Corollary VIII.3.7).

It is worthwhile to state the following consequence of Proposition 1.17.

1.19 Corollary. *Assume the existence of a $(v, g, 1)$ -difference family. Then*

$$(1.19.a) \quad g \in TD(k) \Rightarrow v \in TD(k).$$

In particular,

$$(1.19.b) \quad q+1 \in TD(k) \Rightarrow q^2 + q + 1 \in TD(k) \quad \text{for prime powers } q.$$

Thus

$$(1.19.c) \quad 21 \in TD(6),$$

$$(1.19.d) \quad 57 \in TD(9),$$

$$(1.19.e) \quad 273 \in TD(18).$$

Proof. Use Lemma 1.1 together with (I.7.15.a) and Corollary VIII.3.8. The particular examples follow from 1.18.(a). ■

The values given in (1.19.c, d, e) improve those following from MacNeish's Corollary I.7.8 and give the best result for the numbers 57 and 273 known to date. For 21, the better result $21 \in TD(7)$ is known, see Corollary VIII.3.17.

1.20 Exercises. (a) Try to generalise Proposition 1.17 by using a $TD_\mu[k; g]$ with a parallel class. Show that this is possible under the additional assumption $k(\mu - 1) \leq \lambda\mu$. Use this to show the existence of $(q + 1, q^2; q^2 - q)$ - and of $(q + 1, 2q; 2(q - 1))$ -difference matrices in any group of order $q + 1$, whenever q is a prime power.

(b) Let G be any group of order g and assume the existence of a $TD_\lambda[k; g]$. Show the existence of a $(g, k; g\lambda)$ -difference matrix over G .

Hint: Construct the corresponding $OA_\lambda(k, g)$ on the symbol set G .

(c) Prove the following strengthening of the construction given in Example 1.18.(c) which is due to Colbourn and Kreher (1996): Assume the existence of an $OA_\lambda(k, g)$ with at least λ constant columns. Then, over any group of order $g + 1$, a $(g + 1, k; \lambda(g - 1))$ -difference matrix exists. In particular, over any group of order $g + 1$, a $(q + 1, q + 1; q - 1)$ -difference matrix exists provided that q is a prime power, cf. Jungnickel (1995b).

1.21 Remarks. (a) A recent study of quasigroups, their connections to various types of designs and the corresponding spectra is due Bennett (1989) who also has an extensive bibliography on this area of research. Regarding the application of universal algebra to designs, we mention two further interesting papers, namely Ganter and Metz (1977) and Ganter and Werner (1975).

(b) Further recursive constructions for cyclic difference families and cyclic designs were given by Colbourn and Mathon (1980), Colbourn and Colbourn (1980b, 1984), Jimbo and Kuriki (1983), Grannell and Griggs (1986), Mathon (1987), Jimbo (1993) and Buratti (1997a, c, 1998c). Narayani and Blanchard (1995) gave a new composition theorem for (in general non-cyclic) difference families; a generalisation of their approach can be found in Ray-Chaudhuri and Zhu (1992).

(c) Regarding cyclic Steiner systems with $t \geq 3$ (cf. §III.9), the case of cyclic Steiner quadruple systems has found particular interest, see §VIII.10.

(d) Evans (1989) gave a partial converse of the construction of a cyclic $(q^2 + q + 1, k; 1)$ -difference matrix from a cyclic Singer difference set and a $TD[k; q + 1]$ mentioned in Example 1.18.

(e) Colbourn and Kreher (1996) gave some new recursive constructions for difference matrices with $\lambda \neq 1$, using PBD 's, OA 's and finite fields as ingredients. They also provided a table on the largest known size of an (s, r, λ) -difference matrix in the range $s \leq 32$ and $\lambda \leq 30$. For a larger table of this kind, see

§IV.11.4 of Colbourn and Dinitz (1996a). Further recursive constructions for difference matrices and difference families are due to Buratti (1998a).

In this section we have seen how closely related the concepts of difference families and difference matrices are. The corresponding interaction between pairwise balanced designs and transversal designs will be of paramount importance in the recursive constructions of designs.

§2. Use of Pairwise Balanced Designs

We shall present some important recursive constructions, in particular for *PBD*'s and *TD*'s. We use Hanani's notation (cf. I.2.19).

2.1 Lemma. *Let $g \in TD(k+n)$ and $k, k+1, \dots, k+n \in K$; also, let $0 \leq g_i \leq g$ for $i = 1, \dots, n$. Then*

$$(2.1.a) \quad \begin{aligned} kg + g_1 + \dots + g_n &\in GD(K, \{g, g_1, \dots, g_n\}) \\ &\subseteq B(K \cup \{g, g_1, \dots, g_n\}). \end{aligned}$$

Proof. Delete $g - g_1, \dots, g - g_n$ points from the last n point classes of a $TD[k+n; g]$. ■

2.2 Lemma. *Let $g \in TD(k+n)$ and $k, k+1, \dots, k+n, g+1, g_1+1, \dots, g_n+1 \in K$; $0 < g_i \leq g$ for $i = 1, \dots, n$. Then*

$$(2.2.a) \quad kg + g_1 + \dots + g_n + 1 \in B(K).$$

Proof. Proceed as in Lemma 2.1 and use (I.6.5.b). ■

2.3 Theorem. *If $v \in B(L)$ and $L \subseteq B(K)$, then $v \in B(K)$.*

Proof. Let $D = (V, \{B_1, \dots, B_b\}, \epsilon)$ be an $S(2, L; v)$. By hypothesis, there are *PBD*'s $D_i = (B_i, \{C_{i1}, \dots, C_{ib_i}\}, \epsilon)$ with $|C_{i\mu}| \in K$ for all i, μ . Then

$$(V, \{C_{ij} : i \in \mathbb{N}_1^b, j \in \mathbb{N}_1^{b_i}\}, \epsilon)$$

is the desired *PBD*. Wilson (1972a) calls this procedure "breaking up blocks". ■

2.4 Corollary.

$$(2.4.a) \quad B(B(K)) = B(K) \quad \text{for each } K \subseteq \mathbb{N}.$$

Note that $B(\emptyset) = B(\{1\}) = \{1\}$, and that the usual convention $1 \in B(K)$ for all $K \subseteq \mathbb{N}$ is reasonable.

Proof. Since $(A, \{A\}, \in)$ is a trivial $S(2, L, |A|)$ for any finite set A with $|A| \in L$, we have $L \subseteq B(L)$ for each $L \subseteq \mathbb{N}$; in particular $B(K) \subseteq B(B(K))$. By Theorem 2.3, we also have $B(B(K)) \subseteq B(K)$. ■

2.5 Lemma. If $v \in S_\lambda(t, K)$ and $K \subseteq S_\mu(t, L)$ (for notation see I.3.3), then $v \in S_{\lambda\mu}(t, L)$. Similarly,

$$(2.5.a) \quad GD_\lambda(K, M) = GD_\lambda(B(K), M). \quad \blacksquare$$

The proofs are straightforward generalisations of the previous one. Note that K and L may be infinite subsets of \mathbb{N} .

2.6 Lemma.

$$(2.6.a) \quad GD_\lambda(K, B(K, \lambda)) \subseteq B(K, \lambda),$$

$$(2.6.b) \quad GD_\lambda(K, B(K, \lambda) - 1) + 1 \subseteq B(K, \lambda),$$

$$(2.6.c) \quad GD_\lambda(K, GD_\lambda(K, N)) \subseteq GD_\lambda(K, N).$$

Proof. In a $GD_\lambda[K, GD_\lambda(K, N); v]$, say (V, \mathbf{B}, I) , form a $GD_\lambda[K, N; |G|]$ on each point class G , say (G, \mathbf{A}_G, I) . Then

$$\left(V, \mathbf{B} + \sum_G \mathbf{A}_G, I \right)$$

is a $GD_\lambda[K, N; v]$. This proves (2.6.c). (2.6.a) is a special case. In order to prove (2.6.b), introduce a new point ∞ on the point classes G and form an $S_\lambda(2, K, |G| + 1)$ on each set $G \cup \{\infty\}$. This proves (2.6.b). ■

2.7 Observation. The mapping $B : 2^{\mathbb{N}} \rightarrow 2^{\mathbb{N}}$ which is defined by

$$(2.7.a) \quad K \mapsto B(K), \quad \text{for all } K \subseteq \mathbb{N},$$

is a *closure operator*; i.e. it has the properties

$$(2.7.b) \quad K \subseteq B(K),$$

$$(2.7.c) \quad K \subseteq B(L) \Rightarrow B(K) \subseteq B(L),$$

and hence

$$(2.7.d) \quad B(B(L)) = B(L)$$

for all $K, L \subseteq \mathbb{N}$.

A subset $K \subseteq \mathbb{N}$ is called *closed* if $B(K) = K$ or, in case of ambiguity, *B-closed*.

The concept of closed subsets of \mathbb{N} was introduced by Wilson (1972a, b). It is a very important tool which considerably simplified previous constructions of Hanani and other authors.

2.8 Examples. (a) For each $K \subseteq \mathbb{N}$ and $\lambda \in \mathbb{N}$, the set $B(K, \lambda)$ is closed.

(b) The sets $6\mathbb{N} + \{1, 3\}$, $12\mathbb{N} + \{1, 4\}$, $20\mathbb{N} + \{1, 5\}$ are closed. The next lemma generalises this example.

2.9 Lemma. Let $K \subseteq \mathbb{N}$ be given and define α, β by

$$(2.9.a) \quad \alpha := \gcd\{k - 1 : k \in K\},$$

$$(2.9.b) \quad \beta := \gcd\{k(k - 1) : k \in K\}.$$

Then

$$(2.9.c) \quad \lambda(v - 1) \equiv 0 \pmod{\alpha},$$

$$(2.9.d) \quad \lambda v(v - 1) \equiv 0 \pmod{\beta}$$

are necessary conditions for the existence of an $S_\lambda(2, K; v)$. Let L be the set of all $v \in \mathbb{N}$ satisfying these two conditions. Then L is closed.

Proof. The necessity of (2.9.c) and (2.9.d) follows by counting the flags (p, B) with $p \neq C$ and $c, p \in B$ for a given point c , and the triples (x, y, B) with $x \neq y$ and $x, y \in B$. Note that Corollary I.2.11 is the special case $K = \{k\}$.

In order to prove that L is closed, let $\mathbf{D} = (V, \mathbf{B}, \epsilon)$ be an $S(2, L; v)$. Choose a point $d \in V$ and count the flags (p, B) with $p \neq d$ and $d, p \perp B$. Thus

$$\begin{aligned} v - 1 &= \sum_{B \in (d)} (|B| - 1), \\ \lambda(v - 1) &= \sum_{B \in (d)} \lambda(|B| - 1) \equiv 0 \pmod{\alpha}, \end{aligned}$$

by (2.9.c). Now count the triples (x, y, B) with $x \neq y$ and $x, y \perp B$. Thus

$$\begin{aligned} v(v - 1) &= \sum_{B \in \mathbf{B}} |B|(|B| - 1), \\ \lambda v(v - 1) &= \sum_{B \in \mathbf{B}} \lambda |B|(|B| - 1) \equiv 0 \pmod{\beta}, \end{aligned}$$

by (2.9.d), since $|B| \in L$. Hence $v \in L$. ■

As an example consider the set $30\mathbb{N} + \{1, 6, 16, 21\}$. Note that $30\mathbb{N} + \{1, 6\}$ is not closed; cf. Exercise VIII.1.9.

2.10 Definition. Let $TD^*(k)$ be the set of $g \in \mathbb{N}$ for which a $TD[k; g]$ with a parallel class exists. By Lemma VIII.4.13, $TD^*(k)$ is also the set of $g \in \mathbb{N}$ for which $k - 2$ mutually orthogonal idempotent quasigroups of order g exist. The following theorem is a special case of a theorem of Bose, Shrikhande and Parker (1960); see also Theorem X.1.1.

2.11 Theorem. *The set $TD^*(k)$ is closed for every $k \in \mathbb{N}$.*

Proof. It suffices to prove the following assertion. Let $(V, \mathbf{B}, \epsilon)$ be a PBD . Assume that on each block $B \in \mathbf{B}$ there are two idempotent orthogonal quasigroups $(B, \circ), (B, *)$. Define \circ and $*$ on V as follows.

$$(2.11.a) \quad x \circ x = x * x = x \quad \text{for all } x \in V$$

and

$$(2.11.b) \quad x \circ y := x \overset{B}{\circ} y, \quad x * y := x \overset{B}{*} y,$$

if $x \neq y$ and B is the block through x and y . Then $(V, \circ), (V, *)$ are orthogonal idempotent quasigroups. The proof is left to the reader.

Another proof of the theorem will be given in §X.1. ■

2.12 Examples. We use Theorem 2.11 and Lemma 2.1 with $n = 1, 2$. Thus

$$\begin{aligned} 50 &= 7 \cdot 7 + 1 \in B(\{7, 8\}) \subseteq TD^*(7), \\ 54 &= 7 \cdot 7 + 5 \in B(\{5, 7, 8\}) \subseteq TD^*(5), \\ 70 &= 7 \cdot 9 + 7 \in B(\{7, 8, 9\}) \subseteq TD^*(7), \\ 57 &\in B(8) \subseteq TD^*(8), \\ 253 &\in B(\{16, 13\}) \subseteq TD^*(11), \text{ cf. (VIII.5.6.b) with } q = 4. \end{aligned}$$

2.13 Proposition.

$$(2.13.a) \quad B(\{3, 4\}) = (3\mathbb{N}_0 + \{1, 3\}) \setminus \{6\}.$$

Proof. $6 \notin B(\{3, 4\})$ follows from (I.8.4.a). “ \subseteq ” now follows from (2.9.c, d).

If $g \in K := B(\{3, 4\})$ and $g \in TD(4)$, $g_1 \in K \cup \{0\}$, and $g_1 \leq g$, then $3g + g_1 \in K$. This follows with Lemma 2.1, since K is closed. Note that $7 \in B(3) \subset K$, and that $g \in TD(4)$ if $g \not\equiv 2 \pmod{4}$, by (I.7.8.a). The table

g	3	4	7	9	12	13
g_1	0, 1, 3	0, 1, 3, 4	0, 1, 3, 4	0, 1, 3, 4, 7	0, 1, 3, 4, 7, 9	0, 1, 3, 4, 7, ..., 13
$3g + g_1$	9, 10, 12	12, 13, 15, 16	21, ..., 25	27, ..., 31, 34	36, ..., 43, 45	39, ..., 43, 46, ..., 52

yields some small values of K , but leaves the gaps 18, 19, and 33. But $19, 33 \in K$ by (I.6.11.a), and $18 \in K$ by (I.5.13.a). Now it is easily seen that each $x \equiv 0$ or $1 \pmod{3}$ with $x > 52$ has a representation $x = 3g + g_1$ with $g, g_1 \equiv 0$ or $1 \pmod{3}$, $g \not\equiv 2 \pmod{4}$ and $7 \leq g_1 \leq g$. Hence the assertion follows by induction. ■

The proof would be even shorter if one used result (I.7.9.b).

§3. Applications of Divisible Designs

3.1 Definition. A $GD_\lambda[K, G]$ is a divisible design D with parameter λ , block sizes in $K \subseteq \mathbb{N}$ and point class sizes in G , and a $GD_\lambda[K]$ is a $GD_\lambda[K, \mathbb{N}]$. Without loss of generality, we may assume that the point set is $\{1, 2, \dots, v\} \subset \mathbb{N}$, and that the (non-empty) point classes are G_1, G_2, \dots, G_s , where

$$(3.1.a) \quad x \in G_i, \quad y \in G_j \quad \text{and} \quad i < j \quad \Rightarrow \quad x < y.$$

The s -tuple (G_1, \dots, G_s) is called the *point class list* (or, briefly, the *class list*) of \mathbf{D} . We put $g_i := |G_i|$ for $i = 1, \dots, s$, hence $\sum_{i=1}^s g_i = v$. The *point class type* (or, briefly, the *class type*) of \mathbf{D} is the s -tuple

$$(3.1.b) \quad (g_1, \dots, g_s) \in \mathbb{N}^s.$$

If some of the g_i ($i = 1, \dots, s$) are equal, say

$$(3.1.c) \quad g_1 = \dots = g_{\alpha_1} \neq g_{\alpha_1+1} = \dots = g_{\alpha_1+\alpha_2} \neq g_{\alpha_1+\alpha_2+1} = \dots,$$

we also write

$$(3.1.d) \quad (g_1^{\alpha_1}, \dots, g_t^{\alpha_t}) \quad \text{with} \quad \sum_{j=1}^t \alpha_j = s$$

instead of (3.1.b). Thus every pairwise balanced design has class type (1^v) , and every $GD_\lambda[K, g; sg]$ has class type (g^s) .

If \mathbf{D} is an incidence structure (in most applications a *PBD* or a *GDD*) on the point set $V = \{1, 2, \dots, v\}$, then a *weighting* of V is just a mapping $w: V \rightarrow \mathbb{N}_0$.

With these conventions, we can state the following general composition theorem due to Wilson (1972b).

3.2 Theorem. *Let $\mathbf{D} = (V, \mathbf{B}, \mathbf{G})$ be a $GD_\lambda[H]$ with class list (G_1, \dots, G_s) , and let $w: V \rightarrow \mathbb{N}_0$ be a weighting. For each block $B = \{x_1, \dots, x_h\}$ of \mathbf{D} , assume the existence of a $GD_\mu[K]$, say \mathbf{D}_B , with class type $(w(x_1), \dots, w(x_h))$. Then there exists a $GD_{\lambda\mu}[K]$, say \mathbf{E} , with class type*

$$(3.2.a) \quad \left(\sum_{x \in G_1} w(x), \dots, \sum_{x \in G_s} w(x) \right).$$

Note: Wilson calls \mathbf{D} the *recipe* and the \mathbf{D}_B the *ingredients* (for the construction).

Proof. Let the incidence matrix of \mathbf{D}_B be

$$(3.2.b) \quad M_B = \begin{array}{|c|} \hline M(x_1, B) \\ \hline M(x_2, B) \\ \hline \dots\dots\dots \\ \hline M(x_h, B) \\ \hline \end{array}$$

where each $M(x_i, B)$ is a $w(x_i) \times b_B$ -matrix such that $M(x_i, B)M(x_i, B)^T$ is diagonal and $M(x_i, B)M(x_j, B)^T = \mu J$ for $i \neq j$. If $w(x_i) = 0$, then the matrix $M(x_i, B)$ is omitted. Now replace each $1 = a_{xB}$ in the incidence matrix (a_{xB}) of D by the auxiliary matrix $M(x, B)$ defined by (3.2.b), and each $0 = a_{xB}$ by a $w(x) \times b_B$ -zero-matrix. In this case write

$$M(x, B) = \begin{pmatrix} 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}.$$

Then the matrix

$$\begin{pmatrix} M(x_1, B_1) & \dots & M(x_1, B_b) \\ \dots & \dots & \dots \\ M(x_v, B_1) & \dots & M(x_v, B_b) \end{pmatrix}$$

describes the desired $GD_{\lambda\mu}[K]$. ■

3.3 Remark. We may w.l.o.g. assume that each $M(x, B) \neq 0$ has a 1 in the upper left corner. If $\lambda = \mu = 1$, then E has a subspace which is isomorphic to D . (Consider only the upper left corners of all auxiliary matrices.)

3.4 Corollary. *If D is an $S_\lambda(2, H; v)$, then E has class type*

$$(w(x_1), \dots, w(x_v)). \quad \blacksquare$$

3.5 Corollary. *Let D be a $GD_\lambda[H, G; v]$ (see I.6.1) and suppose that $mk \in GD_\mu(K, m)$ for each $k \in H$. Then there is a $GD_{\lambda\mu}[K, mG; mv]$, say E . Here $mG := \{mx : x \in G\} \subseteq \mathbb{N}$.*

Proof. Use Theorem 3.2 with $w(x) = m$ for each $x \in V$. Or directly: replace the 1's in each column of the incidence matrix of D by the partial matrices M_1, \dots, M_k (see Proposition I.6.2) of the incidence matrix of the respective $GD_\mu[K, m; mk]$. ■

3.6 Corollary. *Let D be a $GD_\lambda[K, G; v]$ and suppose that*

$$(3.6.a) \quad m \in TD_\mu(l) \quad \text{for } l := \max K.$$

Then there is a $GD_{\lambda\mu}[k, mG; mv]$.

Proof. Condition (3.6.a) is equivalent to requiring that $km \in GD_\mu(k, m) \subseteq GD_\mu(K, m)$ for each $k \in K$. Now apply Corollary 3.5. ■

This special case of Theorem 3.2 is used very often, especially in case $\mu = 1$. The most important applications of transversal designs are those given in Lemmas 2.1, 2.2, and Corollary 3.6. Note that MacNeish's Theorem I.7.7 is a special case of Corollary 3.6.

Next we shall present Hanani's recursion lemma which proved to be extremely successful for his existence theorems.

3.7 Definition and Notation. For $K \subseteq \mathbb{N}$ and $m, \lambda \in \mathbb{N}$ define $R_{K,\lambda}^m$ to be the set of all $x \in \mathbb{N}$ such that

$$(3.7.a) \quad mx \in GD_\lambda(K, m).$$

For $\lambda = 1$ write R_K^m instead of $R_{K,1}^m$, and if $K = \{k\}$ write k for $\{k\}$. Our definition means

$$(3.7.b) \quad mR_{K,\lambda}^m = GD_\lambda(K, m).$$

Wilson's notation for R_K^m is $NG(m, K)$. By Lemma 2.5, we get

$$(3.7.c) \quad R_{K,\lambda}^m = R_{B(K),\lambda}^m.$$

Let us remark that Hanani (1975) determined the sets $R_{k,\lambda}^m$ completely for $k = 3$, and Brouwer, Schrijver and Hanani (1977) did the same for $k = 4$, cf. §9.

3.8 Examples. (a) $R_{K,\lambda}^1 = B(K, \lambda) = S_\lambda(2, K)$, see Notation I.2.19.

$$(b) R_k := R_k^{k-1} = \{x \in \mathbb{N} : (k-1)x \in GD(k, k-1)\} \\ = \{x \in \mathbb{N} : (k-1)x + 1 \in B(k)\}, \text{ see (I.6.5.d).}$$

The notation R_k is customary, see e.g. Wilson (1972a). We chose the notation $R_{K,\lambda}^m$ introduced in 3.7 as a straightforward generalisation.

$$(c) g \in TD_\lambda(k) \iff k \in R_{k,\lambda}^g.$$

In general, our knowledge about the sets $R_{K,\lambda}^m$ is unsatisfactory. By Corollary VII.6.7, the sets $B(K, \lambda)$ and R_K are infinite for $\max K = k > 1$. The following fundamental lemma is implicit in Hanani's work.

3.9 Main Lemma (Hanani's Recursion Lemma). *If $K, G \subseteq \mathbb{N}$ and $m, \lambda, \mu \in \mathbb{N}$, then*

$$(3.9.a) \quad m \cdot GD_\lambda(R_{K,\mu}^m, G) \subseteq GD_{\lambda\mu}(K, mG).$$

Proof. Put $H := R_{K,\mu}^m$. By hypothesis, $mH = GD_\mu(K, m)$. Now apply Corollary 3.5. ■

These theorems and lemmas are fairly general, and hence they need some explanation by examples. The following results are due to Wilson (1972b).

3.10 Corollary. *The sets $R_{K,\lambda}^m$ are closed. In particular the sets $B(K, \lambda)$ and R_k are closed.*

Proof. In the Main Lemma take $G = \{1\}$, $\lambda = 1$. Then

$$m GD(R_{K,\mu}^m, 1) = mB(R_{K,\mu}^m) \subseteq GD_\mu(K, m).$$

By (3.7.b),

$$B(R_{K,\mu}^m) \subseteq R_{K,\mu}. \quad \blacksquare$$

3.11 Lemma. *Let $K \neq \{1\}$ be a non-empty subset of \mathbb{N} . Put*

$$(3.11.a) \quad L := B(K, \lambda),$$

and suppose that the positive integer m has the property

$$(3.11.b) \quad x \equiv 1 \pmod{m} \quad \text{for all } x \in L.$$

Define $Y \subseteq \mathbb{N}_0$ by

$$(3.11.c) \quad L = B(K, \lambda) = mY + 1.$$

Then, with the convention $0 \in GD_\lambda(X, Y)$ for all $X, Y \in \mathbb{N}$,

$$(3.11.d) \quad GD(R_{K,\lambda}^m, Y) = Y.$$

Proof. By the Main Lemma 3.9,

$$m GD(R_{K,\lambda}^m, Y) = GD_\lambda(K, mY) = GD_\lambda(K, B(K, \lambda) - 1).$$

With (2.6.b) and (3.11.c) the assertion follows, as trivially $Y \subseteq GD(R_{K,\lambda}^m, Y)$. ■

Note that the case $m = 1$ is already contained in (2.6.b) and (2.5.a).

3.12 Exercise. If q is a prime power, then

$$(3.12.a) \quad q \in R_q^q,$$

$$(3.12.b) \quad q + 1 \in R_q \cap R_{q+1} = R_q^{q-1} \cap R_{q+1}^q.$$

3.13 Lemma. If $m, r \in R_k$ and $m \in TD(k)$, then $mr \in R_k$.

Proof. By hypothesis, there is a $GD[k, k-1; r(k-1)]$. By Corollary 3.6, we obtain $mr(k-1) \in GD[k, m(k-1), mr(k-1)]$. Hence $mr(k-1) + 1 \in B(\{k, m(k-1) + 1\}) = B(k)$, which implies the assertion. ■

3.14 Example. Let \mathcal{D}_1 be an $S(2, 6; 31)$. Since $5 \in TD(6)$, Corollary 3.6 implies the existence of a $GD[6, 5; 155]$, i.e. of an $S(2, 6; 156)$ containing a subspace of order 31. Hence there is a $GD(6)$ with 156 points and class type $125 \cdot (1) + (31)$. Furthermore, there is a $TD[6; 31]$, hence a $GD(6)$ with 186 points and class type $124 \cdot (1) + 2 \cdot (31)$. Moreover, $126 \in B(6)$, by VIII.9.5. Now let \mathcal{D} be the projective plane $PG(2, 125)$, and let N be a subset of an oval, $0 \leq |N| \leq 126$. Weight the point set V of \mathcal{D} as follows.

$$w(x) = \begin{cases} 31 & \text{if } x \in N \\ 1 & \text{otherwise.} \end{cases}$$

If B is a block of \mathcal{D} , then $|B \cap N| \leq 2$. If

$$B \cap N = \begin{cases} 0 \\ 1 \\ 2 \end{cases},$$

there is a $GD(6)$ with class type

$$\begin{cases} 126 \cdot (1), \\ 125 \cdot (1) + (31), \\ 124 \cdot (1) + 2 \cdot (31). \end{cases}$$

Hence the hypothesis of Theorem 3.2 is satisfied, and Corollary 3.4 yields $15751 + 30 \cdot \mathbb{N}_0^{126} \subseteq GD(6, \{1, 31\}) \subseteq B(6)$; i.e.

$$(3.14.a) \quad [30\mathbb{N} + 1]_{15751}^{19531} \subseteq B(6).$$

3.15 Notation. Let $F_K(u)$ denote the set of positive integers for which there exists an $S(2, K; v)$ with a subspace of order u . For instance

$$\begin{aligned} F_K(0) &= F_K(1) = B(K), \\ F_k(k) &= B(k), \\ F_K(u) &= \emptyset \quad \text{if } u \notin B(K), \\ GD(K, u), GD(K, u - 1) + 1 &\in F_K(u). \end{aligned}$$

Doyen and Wilson (1973) proved that

$$(3.15.a) \quad F_3(u) = \{u\} \cup \{[6\mathbb{N} + \{1, 3\}]_{2u+1}^\infty\} \quad \text{for } u \in 6\mathbb{N} + \{1, 3\}.$$

We shall prove this result in Theorem 11.3. Wilson (1972b) calls the following theorem the ‘‘Adjunction Theorem’’.

3.16 Theorem. Let $\mathbf{D} = (V, \mathbf{B}, \mathbf{G})$ be a $GD[K]$ and $d \in \mathbb{N}$. If

$$(3.16.a) \quad |G| + d \in F_K(d) \text{ for each point class } G \text{ of } \mathbf{D},$$

then, for each $G \in \mathbf{G}$,

$$(3.16.b) \quad |V| + d \in F_K(|G| + d) \subseteq B(K).$$

Proof. Let U be a set of d new points. If $G \in \mathbf{G}$, construct an $S(2, K; |G| + d)$ on $G \cup U$, with block set \mathbf{B}_G , such that U is the point set of a fixed subspace (independent of G). Note that this is always possible, since any subspace of a PBD may be replaced by any other subspace of the same order. Then $\mathbf{B} + \sum_{G \in \mathbf{G}} \mathbf{B}_G$ is the block set of the desired $S(2, K; |V| + d)$. ■

3.17 Examples.

$$\begin{aligned} 88 &= 4 \cdot 21 + 4 \in B(\{4, 25\}) = B(4), \quad \text{cf. Example VII.3.2.(a),} \\ 366 &= 6 \cdot 60 + 6 \in F_6(66) \subseteq B(6), \quad \text{cf. Exercise VIII.1.10,} \\ 85 &= 5 \cdot 16 + 5 \in F_5(21) \subseteq B(5), \quad \text{cf. (I.2.19.b).} \end{aligned}$$

§4. Applications of Hanani's Lemmas

Most of the following examples are due to Hanani and Wilson.