© DISCRETE MATHEMATICS 3 (1972) 343--357. North-Holland Publishing Company

ON RESOLVABLE DESIGNS

Haim HANANI

University of the Negev, Beer Sheva, Israel

D.K. RAY-CHAUDHURI and Richard M. WILSON

The Ohio State University, Columbus, Ohio

Received 24 September 1971

Abstract. A balanced incomplete block design (BIBD) $B[k, \lambda; v]$ is an arrangement of v elements in blocks of k elements each, such that every pair of elements is contained in exactly λ blocks. A BIBD $B[k, 1; v]$ is called resolvable if the blocks can be partitioned into $(v-1)/(k-1)$ families each consisting of v/k mutually disjoint blocks. Ray-Chaudhuri and Wilson [8] proved the existence of resolvable BIBD's $B[3, 1; v]$ for every $v \equiv 3 \pmod 6$. In addition to this result, the existence is proved here of resolvable BIBD's $B[4, 1; v]$ for every $v \equiv 4 \pmod{12}$.

§1. Introduction

In the year 1847 Kirkman [6] introduced the "school girl problem". Fifteen school girls are arranged for a walk in 5 rows of three. Different row arrangements have to be made for the 7 days of the week so that any pair of girls walk in the same row exactly one day of the week. In the general case the problem is to arrange $(6n+3)$ girls in $(2n+1)$ rows of three and to find different row arrangements for $(3n+1)$ days such that any pair of girls belongs to the same row on exactly one day. In modern terminology such arrangement corresponds to the construction of resolvable balanced incomplete block desings with block-size 3.

Many partial solutions of the "school girl problem" have been found during the late 19th century and early 20th century. Most of them may be found in the book by Ball [1, pp. 267–298]. However, the complete solution of this problem has been given only lately by Ray-Chaudhuri and Wilson [8].

The method used by Ray-Chaudhuri and Wilson may be applied to the construction of resolvable balanced incomplete block designs with

block-size 4, or, in the "school girl" terminology, to girls walking in rows of four. The complete solution of this problem is given herewith.

§2. Pairwise balanced designs

Let X be a finite set (of *points*) and let $\mathcal{B} = \{B_i | i \in I\}$ be a family of subsets B_i (called *blocks*) of X. The pair $(X, \mathcal{B})$ is then called a *design*.

The *order* of a design $(X, \mathcal{B})$ is $|X|$ (the cardinality of X) and the set $\{|B_i| \; |B_i \in \mathcal{B}\}$ is the set of *block-sizes* of the design.

Let v and λ be positive integers and K a set of positive integers. A design $(X, \mathcal{B})$ is a *pairwise balanced design* $B[K, \lambda; v]$ iff

(i) $|X| = v$ (the design is of order v).

(ii) $\{|B_i| \; |B_i \in \mathcal{B}\} \subset K$ (the design has block-sizes from K).

(iii) every pairset $\{x, y\} \subset X$ is contained in exactly λ blocks B_i.

In the sequel we shall deal exclusively with designs having $\lambda = 1$ and accordingly we condense our notation and denote pairwise balanced designs by $B[K; v] \equiv B[K, 1; v]$.

The set of positive integers v for which pairwise balanced designs $B[K; v]$ exist will be denoted by $B(K)$.

Clearly for every K

(1) $\qquad K \subset B(K)$

holds. Also

(2) $\qquad K \subset K' \Rightarrow B(K) \subset B(K')$.

From (1) and (2),

(3) $\qquad B(K) \subset B(B(K))$.

On the other hand also

(4) $\qquad B(K) \supset B(B(K))$,

because if $v \in B(B(K))$ then there exists a pairwise balanced design $(X, \mathcal{B})$ of order v and with block-sizes from $B(K)$. Thus for each block $B \in \mathcal{B}$ we may construct a pairwise balanced designs $(B, \mathcal{A}_B)$ with block-sizes from K. The design $(X, \mathcal{A})$ where $\mathcal{A} = \bigcup_{B \in \mathcal{B}} \mathcal{A}_B$ is clearly a pairwise balanced design with block-size from K and consequently $v \in B(K)$. By (3) and (4),

(5) $\qquad B(K) = B(B(K)).$

Further from (2) and (5),

(6) $\qquad K \subset B(K') \Rightarrow B(K) \subset B(K')\,.$

A pairwise balanced design $B[K;v]$ with $K = \{k\}$ consisting of exactly one integer $k \geq 2$ is called a *balanced incomplete block design* (BIBD) and will be denoted by $B[k;v]$ (for $B[\{k\};v]$). Similarly, the set of positive integers v for which BIBD's $B[k;v]$ exist will be denoted by $B(k)$.

Let a BIBD $B[k;v]$ be given; then every point of the BIBD is contained in exactly $r = (v-1)/(k-1)$ blocks (r is the *replication number* of the BIBD) and the total number of blocks is $b = v(v-1)/(k(k-1))$. Since r and b are necessarily integers, a necessary condition for the existence of a BIBD $B[k;v]$ is

(7) $$\begin{aligned} &v-1 \equiv 0 (\mathrm{mod}\ (k-1)), \\ &v(v-1) \equiv 0 (\mathrm{mod}\ k(k-1))\,. \end{aligned}$$

The condition (7) is not in general sufficient but it has been proved by Reiss [9] that it is sufficient for $k = 3$ and by Hanani [3, 5] that it is sufficient for $k = 4$ and $k = 5$.

In the special case of BIBD's it is obtained from (5) and (6)

(8) $\qquad B(k) = B(B(k))$

and

(9) $\qquad K \subset B(k) \Rightarrow B(K) \subset B(k)$

respectively.

A *parallel class* of blocks of a design $(X, \mathcal{B})$ is a subclass $\mathcal{B}_1 \subset \mathcal{B}$ such that each point $x \in X$ is contained in exactly one block of $\mathcal{B}_1$, i.e., $\mathcal{B}_1$ is a partition of X. A parallel class $\mathcal{B}_1$ is *uniform* if all blocks of $\mathcal{B}_1$ have the same size. Of course, every parallel class of blocks of a BIBD is uniform.

A *resolvable BIBD* $B^*[k;v]$ is a BIBD $B[k;v]$ the blocks of which can be partitioned into $(v-1)/(k-1)$ (uniform) parallel classes. The set of positive integers v for which resolvable BIBD's $B^*[k;v]$ exist will be denoted by $B^*(k)$.

Let $v \in B^*(k)$, then of course the condition (7) must be satisfied and moreover $v \equiv 0 \pmod{k}$, say $v = \alpha k$. By (7), $v-1 = \alpha k-1 \equiv 0 \pmod{(k-1)}$ and it follows that $\alpha \equiv 1 \pmod{(k-1)}$ or

$$v \equiv k \pmod{(k(k-1))} \tag{10}$$

which is a necessary condition for the existence of a resolvable BIBD $B^*[k;v]$. Ray-Chaudhuri and Wilson [8] proved that condition (10) is sufficient for $k = 3$. It will be proved in this paper that it is sufficeint also in the case of $k = 4$.

§3. Group divisible designs

A group divisible design is a pairwise balanced design with a distinguished parallel class of blocks. More precisely let v be a positive integer and K and M sets of positive integers, then a *group divisible design* $\mathrm{GD}[K, M; v]$ is a triple (X, G, A), where X is a set having v points, $G = \{G_j \mid j \in I\}$ is a parallel class of subsets G_j (called *groups*) of X which partition X and satisfy $\{|G_j| \mid G_j \in G\} \subset M$, and $\mathsf{A} = \{A_i \mid i \in I\}$ is a class of subsets (*blocks*) of X satisfying $\{|A_i| \mid A_i \in \mathsf{A}\} \subset K$ and such that every pair $\{x, y\} \subset X$ is either contained in a unique group or a unique block, but not both.

The set of positive integers v for which group divisible designs $\mathrm{GD}[K, M; v]$ exist will be denoted by $\mathrm{GD}(K, M)$.

Clearly

$$\mathrm{GD}(K, M) \subset B(K \cup M) \tag{11}$$

holds. Further, by adjoining an additional point to each of the groups we obtain

(12) $\quad \mathrm{GD}(K, M) + 1 \subset B(K \cup (M + 1))$

where if H is a set of integers, then $H + 1 = \{h_i + 1 | \, h_i \in H\}$.

A group divisible design GD$[K, M; v]$ will be called a *uniform group divisible design* GD$[k, m; v]$ if both sets $K = \{k\}$, $k \geq 2$ and $M = \{m\}$ consist of one integer each, i.e., if all the groups are of size m and all the blocks of size k. In such case v must be a multiple of m and $v \geq mk$. As usual GD(k, m) will denote the set of integers v for which GD$[k, m; v]$ exist.

As special cases of (11) and (12) we have

(13) $\quad \mathrm{GD}(k, m) \subset B(\{k, m\})$

and

(14) $\quad \mathrm{GD}(k, m) + 1 \subset B(\{k, m + 1\})$.

In the case $m = k-1$ the stronger result holds

(15) $\quad \mathrm{GD}(k, k-1) + 1 = B(k)$.

It is also easily verified that

(16) $\quad mK \subset \mathrm{GD}(k, m) \Rightarrow mB(K) \subset \mathrm{GD}(k, m)$,

where $mH = \{mh_i | \, h_i \in H\}$. Further

(17) $\quad ms \in \mathrm{GD}(k, m) \Rightarrow m\mathrm{GD}(s, t) + 1 \subset B(\{k, mt + 1\})$.

The last result may be generalized, namely

(18) $\quad mS \in \mathrm{GD}(k, m) \Rightarrow m\mathrm{GD}(S, T) + 1 \subset B(\{k\} \cup (mT + 1))$.

Let us denote by $R(k)$ the set of replication numbers for which BIBD's with block-size k exist and accordingly by $R^*(k)$ the set of replication numbers for which resolvable BIBD's with block-size k exist. In other words

(19) $R(k) = \{r \mid (k-1)r + 1 \in B(k)\}$,

(20) $R^*(k) = \{r \mid (k-1)r + 1 \in B^*(k)\}$.

It is easily proved that

(21) $R(k) = B(R(k))$,

namely by (1), $R(k) \subset B(R(k))$; to prove $B(R(k)) \subset R(k)$, let $n \in B(R(k))$; from (15) and (19),

(22) $R(k) = \{r \mid (k-1)r \in \mathrm{GD}(k, k-1)\}$

and by (16), $(k-1)n \in \mathrm{GD}(k, k-1)$; consequently, by (22), $n \in R(k)$.

Let a resolvable BIBD $(X, \mathcal{B})$ $B^*[k; v]$ be given. For every parallel class $\mathcal{B}_i \subset \mathcal{B}$ of blocks choose a distinct point $y_i \notin X$ and adjoin it to all the blocks of $\mathcal{B}_i$. Further form an additional block from the r elements y_i, where $r = (v-1)/(k-1)$. The obtained design will be called a *completed resolvable design* $\mathrm{CB}[k; r]$. More formally a completed resolvable design $\mathrm{CB}[k; r]$ is a pairwise balanced design $B[\{k+1, r\}; kr+1]$ having exactly one block of size r. By $\mathrm{CB}(k)$ we shall denote the set of integers r for which completed resolvable designs $\mathrm{CB}[k; r]$ exist.

Clearly,

(23) $\mathrm{CB}(k) = R^*(k)$

holds. Further,

(24) $K \subset \mathrm{CB}(k) \Rightarrow B(K) \subset \mathrm{CB}(k)$.

To prove (24) let $r \in B(K)$ and it will be shown that $r \in \mathrm{CB}(k)$. $\mathrm{CB}[k; r]$ is equivalent to $\mathrm{GD}[\{k+1, r\}, k; rk]$ with exactly one block of size r (this block intersects each group in exactly one point). Consider a set of r groups having k points each and in each of the groups choose a specified point. On these r specified points form a pairwise balanced design $B[K; r]$ and for each of its blocks B_i, form on the respective groups a group divisible design $\mathrm{GD}[\{k+1, |B_i|\}, k; k|B_i|]$ in

such way that the block of size $|B_i|$ be the block B_i itself. Delete the block B_i. Take all the other blocks of GD$[\{k+1, |B_i|\}, k; k|B_i|]$ for all values of i and add the block of size r of all the specified points. The obtained design is GD$[\{k+1, r\}, k; rk]$ which proves (24).

We can now prove

$$R^*(k) = B(R^*(k)). \tag{25}$$

$R^*(k) \subset B(R^*(k))$ follows from (1). Further let $r \in B(R^*(k))$; then by (23) $r \in B(\mathrm{CB}(k))$ and putting in (24) $K = \mathrm{CB}(k)$, we obtain $r \in \mathrm{CB}(k)$. Again by (23), $r \in R^*(k)$.

§4. Transversal designs

A *transversal design* $T[s; t]$ is a uniform group divisible design GD$[s, t; st]$ in which the block-size s is equal to the number of groups and consequently every block intersects every group in exactly one point. A transversal design $T[s; t]$ has exactly t^2 blocks. A *resolvable transversal design* $T^*[s; t]$ is a transversal design $T[s; t]$ in which the blocks can be partitioned into t parallel classes (each consisting of t blocks). $T(s)$ and $T^*(s)$ are the sets of integers t for which designs $T[s; t]$ and $T^*[s; t]$ respectively exist.

Clearly, we have

$$s \leq s' \Rightarrow T(s) \supset T(s') \tag{26}$$

and

$$T^*(s) = T(s+1). \tag{27}$$

Galois proved that if q is a prime-power then there exists a projective plane PG$[2, q]$ which is equivalent (see e.g. [2, p. 175]) to the statement

$$q^2 + q + 1 \in B(q+1). \tag{28}$$

Deleting a block and its elements from PG $[2, q]$ a finite affine plane AG $[2, q]$ is obtained which is equivalent to

(29) $\quad q^2 \in B(q)$;

it is easily seen that also

(30) $\quad q^2 \in B^*(q)$

holds. From (28) and (29) it follows by (15)

(31) $\quad c^2 + q \in \mathrm{GD}(q+1, q)$

and

(32) $\quad q^2 - 1 \in \mathrm{GD}(q, q-1)$

respectively, and (31) is equivalent to

(33) $\quad q \in T(q+1) = T^*(q)$.

MacNeish [7] proved that

(34) $\quad \{t, t'\} \subset T(s) \Rightarrow tt' \in T(s)$

(for a simple proof see e.g. [2, p. 191]). Making use of (26) and (33) it follows from (34) by induction

Theorem 1. *If* $t = \Pi p_i^{\alpha_i}$ *is the factorisation of* t *into powers of distinct primes, then* $t \in T(s+1) = T^*(s)$, *where* $s = \min p_i^{\alpha_i}$.

It has been proved lately by Hanani [4], that

(35) $\quad t > 51 \Rightarrow t \in T^*(4) = T(5)$

and

(36) $t > 62 \Rightarrow t \in T^*(6) = T(7)$.

Given a transversal design $T[s+1;t]$, if we delete some (or all) points from one of its groups we obtain

(37) $(t \in T(s+1) \wedge 0 \leq h \leq t) \Rightarrow st+h \in \mathrm{GD}(\{s, s+1\}, \{t, h\})$

and considering (11),

(38) $(t \in T(s+1) \wedge 0 \leq h \leq t) \Rightarrow st+h \in B(\{s, s+1, t, h\})$.

Let

(39) $U(k) = \{u | k(k-1)u + k \in B^*(k)\}$.

By (20), $U(k)$ may also be defined as

(40) $U(k) = \{u | ku + 1 \in R^*(k)\}$.

Ray-Chaudhuri and Wilson [8] proved

Theorem 2. *Let $k = 3$ or 4. If $\{t, h\} \subset U(k)$, $0 \leq h \leq t$ and $t \in T(k+2)$, then $w = (k+1)t+h \in U(k)$.*

Proof. By (31) with $q = k$, $k(k+1) \in \mathrm{GD}(k+1, k)$ and by (32) with $q = k+1$, $k(k+2) \in \mathrm{GD}(k+1, k)$. Further by (37), $w \in \mathrm{GD}(\{k+1, k+2\}, \{t, h\})$ and by (18), $kw+1 \in B(\{k+1, kt+1, kh+1\})$. Considering also that from (20) and (30) follows $q+1 \in R^*(q)$ and therefore $k+1 \in R^*(k)$, and by (40), $\{kt+1, kh+1\} \subset R^*(k)$ it follows by (25), $kw+1 \in R^*(k)$.

§5. Special constructions

In this section we shall give direct constructions of several resolvable BIBD's which will be needed later in this paper. The set X of points of the BIBD will be usually a set Z_n of residua modulo some integer n, or

a Galois field GF(q), or a cartesian product of two or more such sets. The points will be given in parentheses ( ) and the letters x, y will denote generators of Galois fields. Blocks will be given in braces { } and whenever they should be taken cyclically this will be denoted by a note mod ( ) after the block. Parallel classes of blocks will be given in brackets [ ].

Lemma 1. *If $q = 6t + 1$ is a prime-power, then $3q \in B^*(3)$.*

Proof. Let $X = Z_3 \times \mathrm{GF}(q)$. The blocks are

$$\left[\begin{array}{l}\{(0,0),(1,0),(2,0)\}, \\ \{(0,x^{\alpha}),(0,x^{\alpha+2t}),(0,x^{\alpha+4t})\} \bmod (3,-), \alpha = 0,1,\ldots,t-1, \\ \{(0,x^{\alpha+t}),(1,x^{\alpha+3t}),(2,x^{\alpha+5t})\} \bmod (3,-), \alpha = 0,1,\ldots,t-1.\end{array}\right] \bmod(-,q),$$

$$[\{(0,x^{\alpha}),(1,x^{\alpha+2t}),(2,x^{\alpha+4t})\} \bmod(-,q)] \bmod(3,-), \alpha = 0,1,\ldots,t-1.$$

Lemma 2. *If $q = 6t + 1$ is a prime-power, then $2q + 1 \in B^*(3)$.*

Proof. Let $X = Z_2 \times \mathrm{GF}(q) \cup (\infty)$. Further let x be a generator of GF(q) and m an integer satisfying $2x^m = x^t + 1$. The blocks are

$$\left[\begin{array}{l}\{(0,0),(1,0),(\infty)\}, \\ \{(0,x^{\alpha+t+m}),(0,x^{\alpha+3t+m}),(0,x^{\alpha+5t+m})\}, \alpha=0,1,\ldots,t-1, \\ \{(0,x^{\alpha+2\beta t+m}),(1,x^{\alpha+2\beta t}),(1,x^{\alpha+2\beta t+t})\}, \alpha=0,1,\ldots,t-1, \beta=0,1,2.\end{array}\right] \bmod(-,q)$$

Lemma 3. *If $q = 4t + 1$ is a prime-power, then $3q + 1 \in B^*(4)$.*

Proof. Let $X = Z_3 \times \mathrm{GF}(q) \cup (\infty)$. The blocks are

$$\left[\begin{array}{l}\{(0,0),(1,0),(2,0),(\infty)\}, \\ \{(0,x^{\alpha}),(0,x^{\alpha+2t}),(1,x^{\alpha+t}),(1,x^{\alpha+3t})\} \bmod(3,-), \alpha=0,1,\ldots,t-1.\end{array}\right] \bmod(-,q).$$

Lemma 4. $69 \in B^*(3)$.

Proof. $X = Z_3 \times Z_{23}$. The blocks are

$$\left[\begin{array}{l}\{(0,0),(1,0),(2,0)\},\{0,18),(0,19),(0,15)\}, \\ \{(1,18),(1,19),(1,22)\},\{(2,18),(2,19),(2,22)\}, \\ \{(0,2),(0,4),(0,17)\},\{(1,2),(1,4),(1,17)\}, \\ \{(2,2),(2,15),(2,17)\},\{(0,22),(1,15),(2,4)\}, \\ \{(0,1),(0,8),(0,13)\} \bmod(3,-),\{(0,3),(0,9),(1,14)\} \bmod(3,-),\end{array}\right] \bmod(-,23),$$

$$\left.\begin{array}{l}\{(0,7),(0,21),(1,6)\}\ \mathrm{mod}(3,-),\{(0,5),(1,20),(2,11)\}\ \mathrm{mod}(3,-),\\ \{(0,10),(1,16),(2,12)\}\ \mathrm{mod}(3,-).\end{array}\right]\mathrm{mod}(-,23),$$

$$[\{(0,0),(1,13),(2,16)\}\ \mathrm{mod}(-,23)]\ \mathrm{mod}(3,-),$$
$$[\{(0,0),(1,10),(2,14)\}\ \mathrm{mod}(-,23)]\ \mathrm{mod}(3,-),$$
$$[\{(0,0),(1,2),(2,22)\}\ \mathrm{mod}(-,23)]\ \mathrm{mod}(3,-),$$
$$[\{(0,0),(1,18),(2,11)\}\ \mathrm{mod}(-,23)],$$
$$[\{(1,0),(2,18),(0,11)\}\ \mathrm{mod}(-,23)].$$

Lemma 5. $100 \in B^*(4)$.

Proof. $X = Z_4 \times \mathrm{GF}(25)$. $x^2 = 2x + 2$. The blocks are

$$\left.\begin{array}{l}\{(0,0),(1,0),(2,0),(3,0)\},\\ \{(\alpha, x^{6\alpha+6\beta}),(\alpha, x^{6\alpha+6\beta+2}),(\alpha, x^{6\alpha+6\beta+5}),(\alpha, x^{6\alpha+6\beta+19})\},\\ \qquad\qquad \alpha = 0,\ 1,\ 2,\ 3,\ \beta = 0,\ 1,\\ \{(0, x^{\nu}),(1, x^{\nu+6}),(2, x^{\nu+12}),(3, x^{\nu+18})\},\ \nu = 3,4,7,9,10,12-18,20-23\end{array}\right]\ (\mathrm{mod}(-,25),$$

$$[\{(0, x^{\mu}),(1, x^{\mu+6}),(2, x^{\mu+12}),(3, x^{\mu+18})\}\ \mathrm{mod}(-,25)],$$
$$\mu = 0,1,2,5,6,8,11,19.$$

Lemma 6. $172 \in B^*(4)$.

Proof. $X = \mathrm{GF}(4) \times \mathrm{GF}(43)$. $x = 3$, $y^2 = y + 1$. The blocks are

$$\left.\begin{array}{l}\{(0,0),(y^0,0),(y^1,0),(y^2,0)\},\\ \{(0, x^{3\alpha+7\beta}),(0, x^{3\alpha+7\beta+21}),(y^{\beta}, x^{3\alpha+7\beta-14}),(y^{\beta}, x^{3\alpha+7\beta+35})\},\\ \qquad\qquad \alpha = 0,\ 1,\ \ldots,\ 6,\ \beta = 0,\ 1,\ 2,\\ \{(y^{\beta}, x^{3\alpha+7\beta}),(y^{\beta}, x^{3\alpha+7\beta+21}),(y^{\beta+1}, x^{3\alpha+7\beta+14}),(y^{\beta+1}, x^{3\alpha+7\beta+35})\},\\ \qquad\qquad \alpha = 0,\ 1,\ \ldots,\ 6,\ \beta = 0,\ 1,\ 2.\end{array}\right]\ \mathrm{mod}(-,43),$$

$$[\{(0,0),(y^0, x^{3\gamma+3}),(y^1, x^{3\gamma+33}),(y^2, x^{3\gamma+22})\}\ \mathrm{mod}(-,43)],$$
$$\gamma = 0,1,\ldots,13.$$

Lemma 7. $232 \in B^*(4)$.

Proof. $X = Z_3 \times Z_7 \times Z_{11} \cup (\infty)$. The blocks are

$$\left.\begin{array}{l}\{(0,0,0),(1,0,0),(2,0,0),(\infty)\},\\ \{(0,0,1),(0,0,10),(1,0,5),(1,0,6)\}\ \mathrm{mod}(3,-,-),\\ \{(0,0,\mu+1),(0,0,-\mu-1),(1,\mu,0),(1,-\mu,0)\}\ \mathrm{mod}(3,-,-),\ \mu = 1,2,3,\\ \{(0,1,5),(0,6,6),(1,1,6),(1,6,5)\}\ \mathrm{mod}(3,-,-),\\ \{(0,2,1),(0,5,10),(1,2,10),(1,5,1)\}\mathrm{mod}(3,-,-),\end{array}\right]\ \mathrm{mod}(-,7,11).$$

$$\left[\begin{array}{l}\{(0,3,4),(0,4,7),(1,3,7),(1,4,4)\} \bmod(3,-,-),\\ \{(0,1,\epsilon),(0,6,-\epsilon),(1,2,2\epsilon),(1,5,-2\epsilon)\} \bmod(3,-,-),\ \epsilon=\pm1,\\ \{(0,1,2\epsilon),(0,6,-2\epsilon),(1,2,-4\epsilon),(1,5,4\epsilon)\} \bmod(3,-,-),\ \epsilon=\pm1,\\ \{(0,1,3\epsilon),(0,6,-3\epsilon),(1,3,2\epsilon),(1,4,-2\epsilon)\} \bmod(3,-,-),\ \epsilon=\pm1,\\ \{(0,1,4\epsilon),(0,6,-4\epsilon),(1,3,-3\epsilon),(1,4,3\epsilon)\} \bmod(3,-,-),\ \epsilon=\pm1,\\ \{(0,2,3\epsilon),(0,5,-3\epsilon),(1,3,-5\epsilon),(1,4,5\epsilon)\} \bmod(3,-,-),\ \epsilon=\pm1,\\ \{(0,2,5\epsilon),(0,5,-5\epsilon),(1,3,\epsilon),(1,4,-\epsilon)\} \bmod(3,-,-),\ \epsilon=\pm1,\end{array}\right] \bmod(-,7,11).$$

Lemma 8. $388 \in B^*(4)$.

Proof. $X = Z_4 \times \mathrm{GF}(97)$. $x = 5$. The blocks are

$$\left[\begin{array}{l}\{(0,0),(1,0),(2,0),(3,0)\},\\ \{(\alpha,x^{24\alpha+6\beta}),(\alpha,x^{24\alpha+6\beta+2}),(\alpha,x^{24\alpha+6\beta+40}),(\alpha,x^{24\alpha+6\beta+47})\},\\ \qquad\qquad \alpha=0,1,2,3,\beta=0,1,\ldots,7,\\ \{(0,x^{\nu}),(1,x^{\nu+24}),(2,x^{\nu+48}),(3,x^{\nu+72})\},\\ \qquad \nu = 1,3\text{–}5,7,9\text{–}11,13,15\text{–}17,19,21\text{–}23,25,27\text{–}29,31,\\ \qquad 33\text{–}35,37,39,41,43,45,48\text{–}51,54\text{–}57,60\text{–}63,66\text{–}69,\\ \qquad 72\text{–}75,78\text{–}81,84\text{–}88,90\text{–}95.\end{array}\right] \bmod(-,97),$$

$$[\{(0,x^{\mu}),(1,x^{\mu+24}),(2,x^{\mu+48}),(3,x^{\mu+72})\} \bmod(-,97)],$$

$$\mu = 0,2,6,8,12,14,18,20,24,26,30,32,36,38,40,42,44,46,47,52\text{–}53,58\text{–}59,64\text{–}65,70\text{–}71,76\text{–}77,82\text{–}83,89.$$

§6. Harrison-type theorems

Theorem 3. *If* $km \in B^*(k)$, $kn \in B^*(k)$ *and* $n \in T^*(k)$, *then* $kmn \in B^*(k)$.

Proof. Consider $B^*[k;km]$ as a design $(X, \mathcal{B})$ where the elements of X are groups having n points each. Let $\mathcal{B}_1 \subset \mathcal{B}$ be one of the parallel classes of blocks. For every block B of $\mathcal{B}_1$ form a resolvable BIBD $B^*[k;kn]$ on the union of groups of B. For every block of other parallel classes form the blocks of $T^*[k;n]$.

Theorem 4. *If* $3m \in B^*(3)$ *and* $3n \in B^*(3)$, *then* $3mn \in B^*(3)$.

Proof. From (10) it follows that $n \equiv 1 \pmod 2$ and therefore by Theorem 1, $n \in T^*(3)$. Accordingly the conditions of Theorem 3 are satisfied.

Theorem 5. *If* $4m \in B^*(4)$ *and* $4n \in B^*(4)$, *then* $4mn \in B^*(4)$.

Proof. From (10) it follows that $n \equiv 1 \pmod 3$ and therefore by (35) and Theorem 1, $n \in T^*(4)$ with possible exception of $n = 10, 22, 34$ and 46. Because of symmetry of m and n it remains to prove that $4mn \in B^*(4)$ for $\{m, n\} \subset \{10, 22, 34, 46\}$ and this will be done herewith. We shall in most cases factorise $4mn = 4m_1 n_1$ so that $n_1 = 4$ and accordingly $4n_1 = 16 \in B^*(4)$ by (30) and $n_1 = 4 \in T^*(4)$ by (33). It will remain to be proved that $4m_1 \in B^*(4)$. This is shown in table 1.

Table 1

m	n	$4mn$	
10	10	400	$m_1 = 25$. $4m_1 = 100 \in B^*(4)$ by Lemma 5.
10	22	880	$m_1 = 55$. $4m_1 = 220 = 3 \cdot 73 + 1 \in B^*(4)$ by Lemma 3.
10	34	1360	$m_1 = 85$. $4m_1 = 340 = 3 \cdot 113 + 1 \in B^*(4)$ by Lemma 3.
10	46	1840	$1840 = 3 \cdot 613 + 1 \in B^*(4)$ by Lemma 3.
22	22	1936	$m_1 = 121$. $4m_1 = 484 = 12 \cdot 40 + 4$. Put $w = 40 = 5 \cdot 8$. $8 \in U(4)$ because $12 \cdot 8 + 4 = 100 \in B^*(4)$ by Lemma 5. $8 \in T(6)$ by (26) and Theorem 1. Consequently by Theorem 2, $40 \in U(4)$.
22	34	2992	$2992 = 3 \cdot 997 + 1 \in B^*(4)$ by Lemma 3.
22	46	4048	$m_1 = 253$. $4m_1 = 1012 = 3 \cdot 337 + 1 \in B^*(4)$ by Lemma 3.
34	34	4624	$4624 = 12 \cdot 385 + 4$. Put $w = 385 = 5 \cdot 73 + 20$. $73 \in U(4)$ because $4 \cdot 73 + 1 = 293 \in R^*(4)$ by Lemma 3. $20 \in U(4)$ because $4 \cdot 20 + 1 = 81 \in R^*(4)$ by Lemma 3. $73 \in T(6)$ by (33) and (26). Consequently by Theorem 2, $385 \in U(4)$.
34	46	6256	$m_1 = 391$. $4m_1 = 1564 = 3 \cdot 521 + 1 \in B^*(4)$ by Lemma 3.
46	46	8464	$m_1 = 529$. $4m_1 = 2116 = 12 \cdot 176 + 4$. Put $w = 176 = 5 \cdot 37 + 1$. $37 \in U(4)$ because $4 \cdot 37 + 1 = 149 \in R^*(4)$ by Lemma 3. $1 \in U(4)$ because $4 \cdot 1 + 1 = 5 \in R^*(4)$ by Lemma 3. $37 \in T(6)$ by (33) and (26). Consequently by Theorem 2, $176 \in U(4)$.

§7. Resolvable designs

The following theorem has been proved by Ray-Chaudhuri and Wilson [8].

Theorem 6. *A necessary and sufficient condition for the existence of a resolvable* BIBD $B^*[3; v]$ *is that* $v \equiv 3 \pmod 6$.

Proof. The necessity follows from (10). To prove sufficiency we shall show that for every non-negative integer u, $u \in U(3)$ holds. For $u = 0$ this is trivial, for $u = 1$ see (30). For $u = 3, 6, 9, 12, 15$ we have $v = 6u + 3 = 21, 39, 57, 75, 93$ respectively and $u \in U(3)$ follows from Lemma 1. For $u = 2, 4, 8, 10, 14, 26$ we have $v = 15, 27, 51, 63, 87, 159$ respectively and $u \in U(3)$ follows from Lemma 2. For $u = 5$ we show that $r = 3u + 1 = 16 \in R^*(3)$: by (30), $9 \in B^*(3)$ and consequently by (20), $4 \in R^*(3)$, on the other hand by (29), $16 \in B(4)$ and therefore by (25), $16 \in R^*(3)$. For $u = 11$, $v = 69$ and by Lemma 4, $11 \in U(3)$. For $u = 7, 13, 27$ we have respectively $v = 45$ (= 3·3·5), 81 (= 3·3·9), 165 (= 3·5·11) and $u \in U(3)$ follows from Theorem 4.

For other values of u we prove $u \in U(3)$ by induction using Theorem 2.

For $16 \leqslant u \leqslant 20$ take $t = 4$, $h = u - 16$,
$21 \leqslant u \leqslant 25$ take $t = 5$, $h = u - 20$,
$28 \leqslant u \leqslant 35$ take $t = 7$, $h = u - 28$,
$36 \leqslant u \leqslant 45$ take $t = 9$, $h = u - 36$,
$46 \leqslant u \leqslant 55$ take $t = 11$, $h = u - 44$,
$56 \leqslant u \leqslant 65$ take $t = 13$, $h = u - 52$,
$66 \leqslant u \leqslant 71$ take $t = 16$, $h = u - 64$.

For $u \geqslant 72$ put $u = 24l + m$, $l \geqslant 3$, $0 \leqslant m \leqslant 23$, and for
$0 \leqslant m \leqslant 4$ take $t = 6l - 1$, $h = 4 + m$,
$5 \leqslant m \leqslant 23$ take $t = 6l + 1$, $h = m - 4$.

Theorem 7. *A necessary and sufficient condition for the existence of a resolvable* BIBD $B^*[4; v]$ *is that* $v \equiv 4 \pmod{12}$.

Proof. The necessity follows from (10). To prove sufficiency we show that for every non-negative integer u, $u \in U(4)$ holds. For $u = 0$ this is trivial. For $u = 1$–$4, 6$–$7, 9$–$10, 12$–$13, 15, 18, 20, 22, 24, 31, 34, 79$ we have $12u + 4 \in B^*(4)$ by Lemma 3 and accordingly $u \in U(4)$. For $u = 8$, $12u + 4 = 100 \in B^*(4)$ by Lemma 5. For $u = 11$, $r = 4u + 1 = 45$; by (33) and (26), $9 \in T(5)$ and by (13), $45 \in B(\{5, 9\}; \{5, 9\} \subset R^*(4)$ because as we proved already $\{1, 2\} \subset U(4)$ and therefore by (25), $45 \in R^*(4)$. For $u = 14$, $12u + 4 = 172 \in B^*(4)$ by Lemma 6, for $u = 19$, $12u + 4 = 232 \in B^*(4)$ by Lemma 7, and for $u = 32$, $12u + 4 = 388 \in B^*(4)$ by Lemma 8. For $u = 5, 16$–$17, 21, 23, 33$ we have respectively

$v = 64\,(= 4{\cdot}4{\cdot}4)$, $196\,(= 4{\cdot}7{\cdot}7)$, $208\,(= 4{\cdot}4{\cdot}13)$, $256\,(= 4{\cdot}4{\cdot}16)$, $280\,(= 4{\cdot}7{\cdot}10)$, $400\,(= 4{\cdot}10{\cdot}10)$ and $u \in U(4)$ follows from Theorem 5.

For other values of u we prove $u \in U(4)$ by induction using Theorem 2.

For $25 \leqslant u \leqslant 30$ take $t = 5$, $h = u - 25$,
$35 \leqslant u \leqslant 42$ take $t = 7$, $h = u - 35$,
$43 \leqslant u \leqslant 48$ take $t = 8$, $h = u - 40$,
$49 \leqslant u \leqslant 54$ take $t = 9$, $h = u - 45$,
$55 \leqslant u \leqslant 66$ take $t = 11$, $h = u - 55$,
$67 \leqslant u \leqslant 78$ take $t = 13$ $h = u - 65$,
$80 \leqslant u \leqslant 89$ take $t = 16$, $h = u - 80$.

For $u \geqslant 90$ put $u = 30l + m$, $l \geqslant 3$, $0 \leqslant m \leqslant 29$, and for
$0 \leqslant m \leqslant 4$ take $t = 6l - 1$, $h = 5 + m$,
$5 \leqslant m \leqslant 24$ take $t = 6l + 1$, $h = m - 5$,
$25 \leqslant m \leqslant 29$ take $t = 6l + 5$, $h = m - 25$.

References

[1] W.W.R. Ball, Mathematical recreations and essays (revised by H.S.M. Coxeter) (Macmillan, New York, 1947).

[2] M. Hall, Jr., Combinatorial theory (Blaisdell, Waltham, Mass., 1967).

[3] H. Hanani, The existence and construction of balanced incomplete block designs, Ann. Math. Statist. 32 (1961) 361–386.

[4] H. Hanani, On the number of orthogonal Latin squares, J. Combinatorial Theory 8 (1970) 247–271.

[5] H. Hanani, On balanced incomplete block designs with blocks having five elements, J. Combinatorial Theory 12 (1972) 184–201.

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

[7] H.F. MacNeish, Euler squares, Ann. Math. 23 (1922) 221–227.

[8] D.K. Ray-Chaudhuri and R.M. Wilson, Solution of Kirkman's school girl problem, Proc. Symp. in Pure Mathematics 19 (Am. Math. Soc., Providence, R.I., 1971) 187–203.

[9] M. Reiss, Ueber eine Steinersche combinatorische Aufgabe, J. Reine Angew. Math. 56 (1859) 326–344.