Canad. Math. Bull. Vol. 16 (3), 1973

ON THE CONSTRUCTION OF BIBD WITH $\lambda = 1$

BY
KENNETH F. N. SCOTT

1. **Introduction.** In the past three decades the problem of generating (balanced incomplete block) designs by difference sets has received much attention. Bose [2] gave the two "fundamental theorems of the method of differences". Bose, Sprott [9], Lehmer [7], Chowla [4], Takeuchi [10] and others have given specific classes of difference sets.

Bose used the existence of suitable difference sets (initial blocks) in an abelian group Γ to generate a design. The first fundamental theorem is proved under the assumption that the design admits Γ as a sharply point-transitive collineation group. For the second fundamental theorem it is assumed that Γ fixes one point and is a sharply point transitive collineation group on the remaining points.

In this paper we generate designs with $\lambda=1$, by assuming the design admits a (not necessarily abelian) collineation group which is sharply point transitive on a subset of the point set and which fixes the remaining points. This allows us to obtain a general expression for a block of the design in terms of its stabilizer in the group. It is shown that the designs with $\lambda=1$, $r\leq 15$, $k\nmid r$, $r-1$ do not admit such collineation groups.

2. **Designs with point transitive collineation groups.** We denote by $D(v, b, r, k, \lambda)$ a balanced incomplete block design with v varieties, b blocks, r replications, k varieties in a block, and such that every distinct pair of varieties occurs λ times. If the parameters are understood we refer to such a design by D. Otherwise we use the notation and terminology of Dembowski [5].

Let $D=D(v, b, r, k, 1)$ be a design. Let A and B be disjoint subsets of the point set of D whose union is the whole point set. We assume that D admits a collineation group Γ which is sharply transitive on the points of A and which fixes each point of B.

Since $\lambda=1$ the blocks of D are lines. Γ acts as a permutation group on the set of lines.

Let p be an arbitrary but fixed "base" point of the set A. We make an identification between the elements of Γ and the points of A by the map $\theta_p: A\to\Gamma$ where $\theta_p(q)=x$ if and only if the image of p under $x\in\Gamma$ is q. This is a one-one map and so $|\Gamma|=|A|=v-|B|$.

Received by the editors March 30, 1971 and, in revised form, October 8, 1971.

https://doi.org/10.4153/CMB-1973-053-1 Published online by Cambridge University Press

The following cases are possible:

(1) $B=\varnothing$.

In this case $|\Gamma|=v$ and Γ acts as a permutation group on the set of lines.

(2) $B=\{\infty\}$.

Here "∞" represents one point. In this case $|\Gamma|=v-1$. Γ acts as a permutation group on the set of lines. In doing so Γ partitions the set of lines into two sets; for any line on ∞ is mapped into another line on ∞ and any line not on ∞ is mapped onto a line not on ∞.

(3) $B=\{\infty_1, \infty_2, \ldots, \infty_k\}$.

If B contains two points, say ∞_1 and ∞_2 then, because Γ is sharply point transitive on the points of A, B must contain all the points on the line $\infty_1\infty_2$, say $\infty_1, \infty_2, \ldots, \infty_k$. In this case $|\Gamma|=v-k$. The lines of the design are partitioned by Γ into $k+2$ classes. The first consists of all lines which contain no point of B. The second consists of the set B which is a pointwise fixed line under Γ. Each of the remaining k classes consists of all the lines, except the point-wise fixed line B, on one of the points ∞_i, $1\leq i\leq k$.

(4) B contains 3 non collinear points.

As in case (3) B then contains every point on each of the three lines determined by the three points. But then B contains all points on any line intersecting two or more of the three lines. This may in fact mean that B contains the whole design. In any case B is sufficiently large that we cannot determine the design by our methods. We do not consider this case further.

We identify the elements of A with the elements of Γ and the elements of B, if any, with an appropriate number of symbols ∞_i.

The lines of D are then subsets of $A \cup B$. The collineation $\alpha \in \Gamma$ is represented by right multiplication by α where $\infty_i\alpha=\infty_i$ for each $\infty_i \in B$. We call this the right regular representation of D induced by the base point p. If we change from base point p to base point p' the effect is to multiply the representation on the left by z where $p'z=p$.

Let L be a line of the design. We are concerned with the following sets:

(a) $O_R(L)=\{Lx \mid x \in \Gamma\}$, the right orbit of L.
(b) $D_R(L)=\{ab^{-1} \mid a, b \in \Gamma \cap L, a\neq b\}$, the difference set of L.
(c) $S_R(L)=\{x \in \Gamma \mid Lx=L\}$, the right stabilizer of L.

L is not a distinguished element of $O_R(L)$ in the sense that any two lines are in the same orbit if and only if there is a collineation mapping one line into the other. Every point of D is on the same number of lines of $O_R(L)$. Because of this symmetry, it is sufficient to determine the lines on any one point of D. All remaining lines are obtained by right multiplication in Γ. The identity of Γ, e, (corresponding to the arbitrarily chosen base point) is a convenient point to consider.

The condition $\lambda=1$ allows one to show easily that if the difference sets of two lines are not disjoint then they are identical and the two lines are in the same orbit. Conversely if two lines are in the same orbit their difference sets coincide. It is convenient in this sense to talk of the difference set of an orbit. The element $x \in \Gamma$ occurs in the difference set of the line on e and x. From these comments we conclude:

THEOREM 1. *The difference sets of the orbits of D partition the set* $\Gamma-\{e\}$.

If we choose L to lie on e and not on any point of B, then an easy consequence of the condition $\lambda=1$ is that $S_R(L) \subseteq L$. It is for this reason that we shall usually choose L to lie on e. The fundamental theorem of permutation group theory is that $|O_R(L)|=|\Gamma|/|S_R(L)|$. Again using the fact that $\lambda=1$ it is easy to see that $S_R(L)=\{e\}$ if and only if $|D_R(L)|=k(k-1)$.

The above remarks for the case $S_R(L)=\{e\}$ are well known. We now consider the more general case.

DEFINITION. A pair (L, S) of subsets of Γ is said to satisfy condition K if S is the subgroup of Γ generated by all subgroups of Γ in L and $L=\bigcup_{a_i \in K} a_iS$, where $K=\{a_1, \ldots, a_l\}$ is a set of elements satisfying:

(1) $a_i \notin a_jS$ if $a_i \neq a_j$

(2) for $a_i, a_j, a_n, a_m \in S$

$$a_iSa_j^{-1} \cap a_nSa_m^{-1} = \begin{cases} a_iSa_i^{-1} & \text{if} \quad a_i=a_j=a_n=a_m \\ \{e\} & \text{if} \quad a_i=a_j, a_n=a_m, a_i \neq a_n \\ \varnothing & \text{otherwise.} \end{cases}$$

Now we can show.

THEOREM 2. *Let $e \in L$ where L is a line of D. Then $(L, S_R(L))$ satisfies condition K.*

Proof. We note that if $S_R(L)=\{e\}$ the theorem reduces to the previous remarks. Let $S_L=S_R(L)$.

1. Let S be a subgroup of Γ in L. If $S=\{e\}$ then $S \subseteq S_L$. If $S\neq\{e\}$ let $x \in S$, $x\neq e$. Then $x=ex$ and $e=x^{-1}x$ are both in Lx. But then $L=Lx$ so that $x \in S_L$. We have already noted that $S_L \subseteq L$.

https://doi.org/10.4153/CMB-1973-053-1 Published online by Cambridge University Press

2. If $S_L=L$ then trivially (L, S_L) satisfies condition K. If $S_L\neq L$ let $a\in L-S_L$. Then since $L=Lx$ for each $x\in S_L$, $ax\in Lx=L$ for each $x\in S_L$. It follows that we can choose $K=\{a_1,\ldots,a_l\}\subseteq L$ so that $L=\bigcup_{a_i\in K} a_iS_L$ where K has the property that $a_i\notin a_jS_L$ if $a_i\neq a_j$.

3. Let $H=a_iS_La_j^{-1}\cap a_mS_La_n^{-1}$ for some $a_i, a_j, a_n, a_m\in K$.

(a) if $a_i=a_j=a_n=a_m$ then $H=a_iS_La_i^{-1}$ a subgroup of Γ conjugate to S_L.

(b) if $a_i=a_j$, $a_n=a_m$, $a_i\neq a_n$, then H, being the intersection of two subgroups of Γ, is a subgroup of Γ and hence $\{e\}\subseteq H$. If $H\neq\{e\}$, then $|H|\geq 2$. But $H\subseteq La_i^{-1}$ and $H\subseteq La_n^{-1}$ which means $|La_i^{-1}\cap La_n^{-1}|\geq 2$. Therefore $La_i^{-1}=La_n^{-1}$ whence $a_n^{-1}a_i\in S_L$ or $a_i\in a_nS_L$. But this contradicts the definition of K in 2 above. Therefore $H=\{e\}$.

(c) The remaining possibilities can be considered in three steps:

(i) $a_n=a_m$, $a_i\neq a_n$, $a_i\neq a_j$

Let $x\in H$. Then there are $y, z\in S_L$ such that $x=a_iya_j^{-1}=a_nza_n^{-1}=a_nza_n^{-1}$. If $x=e$ we have $a_j=a_iy\in a_iS_L$ which is a contradiction. If $x\neq e$ then $e, x\in La_j^{-1}$, La_n^{-1} which implies $a_j=a_n$. Then $a_iy=a_nz$ so that $a_i\in a_nS_L$ which is a contradiction. Therefore $H=\varnothing$.

Similar arguments allow us to show $H=\varnothing$ in the remaining cases which are

(ii) $a_n\neq a_m$, $a_j\neq a_m$.
(iii) $a_n\neq a_m$, $a_j=a_m$.

The following corollaries are useful.

COROLLARY 3. *$|S_R(L)|$ divides k.*

COROLLARY 4. *If $a_i\in K$, $a_i\neq e$ and $S\neq\{e\}$ is a nontrivial subgroup of $S_R(L)$, then $a_i\notin N_\Gamma(S)$. In particular if $k/|S_R(L)|=l<k$ then Γ has l sub-groups of order $|S_R(L)|$ which have only $\{e\}$ in common.*

In the case where Γ is an abelian group the above results are simplified. We collect these results in

THEOREM 5. *If Γ is abelian then*

(1) *if $L\in D$ and $e\in L$, $S_R(L)=\{e\}$ or $S_R(L)=L$*
(2) *if $L\in D$ then $|O_R(L)|=|\Gamma|$ or $|\Gamma|/k$*
(3) *$k\mid r$ or $k\mid r-1$.*

Proof. Parts (1) and (2) follow easily from Corollary 4. It is well known that for a design $k\mid r(r-1)$. If $k\nmid r-1$ then $k\nmid v=rk-(r-1)$. Therefore by property (2) all line orbits are of length v. Therefore, since $b=(r/k)v$, r/k is an integer and $k\mid r$.

https://doi.org/10.4153/CMB-1973-053-1 Published online by Cambridge University Press

Suppose now that L is a line on e and on a fixed point ∞. Then L lies on $k-1$ points of Γ and so $|O_R(L)|=|\Gamma|/|S_R(L)|\geq|\Gamma|/k-1$. If $B=\{\infty\}$ then $|\Gamma|=v-1=r(k-1)$ and so $|O_R(L)|\geq r$. But there are only r lines on ∞ and so $L=S_R(L)\cup\{\infty\}$. If $B=\{\infty_1,\ldots,\infty_k\}$ then $|\Gamma|=v-k=(r-1)(k-1)$ and so $|O_R(L)|\geq|\Gamma|/(k-1)=r-1$. Now there are r lines on ∞ and one of these is the line $B=\{\infty_1,\ldots,\infty_k\}$. Therefore the remaining $r-1$ lines are in $O_R(L)$ and again we have $L=S_R(L)\cup\{\infty\}$. In this latter case it follows that Γ has k subgroups of order k any two of which have only the identity in common.

3. **Difference sets.** Let k, r be natural numbers such that $k \mid r(r-1)$. We define three types of difference sets which will allow us to generate designs with parameters

$$v=r(k-1)+1,\ b=\frac{r}{k}v,\ r,\ k,\ \lambda=1$$

Type I. Let Γ be a group of order $v=r(k-1)+1$ and let $D=\{L_1,\ldots,L_s\}$ be a collection of subsets of Γ such that:

(a) $|L_i|=k \qquad 1\leq i\leq s$

(b) $D_R(L_i)\cap D_R(L_j)=\varnothing$ if $1\leq i\neq j\leq s$

(c) $\bigcup_{i=1}^{s} D_R(L_i)=\Gamma-\{e\}$.

(d) L contains a subgroup S of Γ such that (L, S) satisfies condition K.

Then D is called a type I (r, k) difference set of Γ.

Type II. Let Γ be a group of order $v-1=r(k-1)$ and let $D=\{L_1,\ldots,L_s\}$ be a collection of subsets of Γ such that D satisfies:

(a) L_1 is a subgroup of order $k-1$ in Γ and $|L_i|=k$ for $2\leq i\leq s$

and (b), (c) and (d) above.

Then D is called a Type II (r, k) difference set.

Type III. Let Γ be a group of order $v-k=(r-1)(k-1)$ and let $D=\{L_1,\ldots,L_s\}$ be a collection of subsets of Γ such that D satisfies.

(a) L_i is a subgroup of order $k-1$ in Γ for

$$1\leq i\leq k \text{ and } |L_i|=k \text{ for } k+1\leq i\leq s.$$

and (b), (c) and (d) above.

Then D is called a Type III (r, k) difference set.

Unless we want to consider particular values of r and k we will generally suppress the (r, k) designation and speak, for example, of a Type I difference set.

https://doi.org/10.4153/CMB-1973-053-1 Published online by Cambridge University Press

If Γ is cyclic, $r=k$, and $s=1$, a Type I difference set is the perfect difference set defined by Singer [8]. If $r=k$, and $s=1$, a Type I difference set is the $(v, k, 1)$ difference set of Bruck [3]. Hoffmann [6] has considered Type II difference sets for which $r=k+1$, and Γ is cyclic. If $|D_R(L_i)|=k(k-1)$ for $1\leq i\leq s$ a Type I difference set is the difference system of Vajda [11].

THEOREM 6. *An (r, k) difference set generates a* $D(r(k-1)+1, (r^2(k-1)+r)/k, r, k, 1)$.

Proof. If $|L_i|=k$ then $L_i\alpha$ for $\alpha\in\Gamma$ is a line. If $|L_i|=k-1$ then $(L_i \cup \{\infty_i\})\alpha$ for $\alpha\in\Gamma$ is a line where $\infty_i\alpha=\infty_i$. If there are k sets L_i with $|L_i|=k-1$ then $\{\infty_1, \ldots, \infty_k\}$ is a line. The point set is the union of Γ and the set of all ∞_i. It is now easy to complete the theorem.

4. **Applications.** We consider $D(46, 69, 9, 6, 1)$. If such a design admits a Type I, Type II, or Type III difference set then the associated group Γ is non-abelian.

Suppose this design admits a Type I difference set. Then $|\Gamma|=46=2\cdot 23$. For any line L, $|S_R(L)|=1$ or 2 and hence $|O_R(L)|=46$ or 23. Therefore the lines occur in one orbit of length 23 and one orbit of length 46 or else in three orbits of length 23. Using Corollary 4 we see that Γ has at least three elements of order 2 in the first case and at least nine elements of order 2 in the second case. If x is of order 2 and L is the line on e and x then $L=Lx$. Therefore Γ has exactly 3 or 9 elements of order 2. By the Sylow theorems this is impossible and so the design does not admit a Type I difference set.

If the design admitted a Type II difference set we would have $|\Gamma|=45$. However, both groups of order 45 are abelian, so that no Type II difference set exists.

If the design admitted a Type III difference set we would have $|\Gamma|=40=2^3\cdot 5$. In this case we require 6 subgroups of order 5. However Γ has only one subgroup of order 5 and so this is impossible.

By similar arguments it is possible to show that the following designs for which $r\leq 15$, $\lambda=1$, $k\nmid r$, and $k\nmid r-1$ do not admit Type I, Type II, or Type III difference sets.

v	b	r	k	λ
46	69	9	6	1
51	85	10	6	1
76	190	15	6	1
136	204	15	10	1

Suppose that a projective plane of order n admits a Type II difference set. Then Γ is a collineation group which fixes a point ∞ and which is transitive on the remaining points. $|\Gamma|=n(n+1)$ so that Γ has at least one collineation of order 2, say

α. However Baer [1, Theorem 1], has shown that every line lies on a fixed point under α. Therefore a projective plane does not admit a Type II difference set.

If a projective plane of order n admits a Type III difference set then it is a translation plane. These are discussed extensively in Dembowski [5]. In this case Γ is called a translation group.

As a final example of the theory we consider the existence of a Type III difference set for a finite affine plane of order n. The existence of such a difference set implies the existence of a group Γ of order n^2-n which admits a partition consisting of sub-groups of order $n-1$, say $H_1, \ldots, H_{n-1}$, and one sub-group of order n, say K. K is a normal Hall subgroup of Γ and the subgroups $H_1, \ldots, H_{n-1}$ are conjugate. It follows that Γ is a Frobenius group and that n is a prime power. The planes obtained in this manner are the nearfield planes.

ACKNOWLEDGEMENTS. The author wishes to acknowledge with thanks the helpful guidance and comments of Drs. J. Dixon and C. W. L. Garner.

BIBLIOGRAPHY

1. R. Baer, *Projectivities with fixed points on every line of the plane*, Bull. Amer. Math. Soc. **52**, 273–286.

2. R. C. Bose, *On the construction of balanced incomplete block designs*, Ann. Eugenics **9** (1939), 353–399.

3. R. H. Bruck, *Difference sets in a finite group*, Trans. Amer. Math. Soc. **78** (1955), 464–481.

4. S. Chowla, *A property of biquadratic residues*, Proc. Nat. Acad. Sci. India. Sect A. **14** (1944), 45–46.

5. P. Dembowski, *Finite geometries*, Springer-Verlag, New York, 1968.

6. A. J. Hoffmann, *Cyclic affine planes*, Canad. J. Math. **4** (1952), 295–301.

7. E. Lehmer, *On residue difference sets*, Canad. J. Math. **5** (1953), 425–432.

8. J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. **43** (1938), 377–385.

9. D. A. Sprott, *Some series of balanced incomplete block designs*, Canad. J. Math. **7** (1955), 369–381.

10. K. Takeuchi, *On the construction of a series of BIB designs*, Rep. Statist. Appl. Res. Un. Japan. Sci. Engrs. **10** (1963), p. 48.

11. S. Vajda, *Patterns and configurations in finite spaces*, Charles Griffin, London, 1967.

SCOTT AND HART ASSOCIATES,
OTTAWA, ONTARIO