BULL. AUSTRAL. MATH. SOC. 05B05, 05B07, 05B10
VOL. 31 (1985), 105-115.

IRREDUCIBLE DESIGNS FROM SUPPLEMENTARY DIFFERENCE SETS

D.R. BREACH AND ANNE PENFOLD STREET

A family of n k-subsets of the integers modulo v are said to be *supplementary difference sets* if developing them by addition modulo v leads to a balanced incomplete block design, and to be *minimal* if no proper subfamily leads to a balanced incomplete block design when developed modulo v. In other words, the family of supplementary difference sets is minimal precisely when it leads to a balanced incomplete block design which cannot be partitioned into a union of proper subdesigns, each consisting of complete cyclic sets of v blocks. We discuss the conditions under which such a balanced incomplete block design can be partitioned in some non-cyclic fashion into a union of proper subdesigns.

I. Introduction and examples

Consider a family $\{D_1, D_2, \ldots, D_n\}$ of k-subsets of Z_v, the integers reduced modulo v. Such sets are said to be *supplementary difference sets* if developing them by addition modulo v in the usual way leads to a pairwise balanced incomplete block design $B[k, \lambda; v]$ (otherwise a 2-(v, k, λ) design). The family is a *minimal family* if no

Received 24 August 1984. The research of the second author was supported by ARGS.

proper subset of $\{D_1, D_2, \ldots, D_n\}$ leads to a balanced incomplete block design when developed modulo v. In other words, the family of supplementary difference sets is minimal precisely when it leads to a balanced incomplete block design which cannot be partitioned into a union of proper subdesigns, each consisting of complete cyclic sets of v blocks.

EXAMPLE 1. Consider the supplementary difference sets, modulo 11,

$$D_1 = \{0, 1, 2, 3, 4\}, \quad D_2 = \{0, 2, 4, 6, 8\}, \quad D_3 = \{0, 3, 6, 9, 1\},$$

$$D_4 = \{0, 4, 8, 1, 5\}, \quad D_5 = \{0, 5, 10, 4, 9\}.$$

These generate a $B[5, 10; 11]$ design (Street [3]). None of these five sets is a difference set and no two are supplementary difference sets. But is it possible for the 55 blocks they generate to contain a subdesign with collections of blocks chosen from different cycles? A $B[5, \lambda; 11]$ with odd λ cannot exist, since the number of blocks would be $11\lambda/2$, which is not an integer. The blocks of a $B[5, 2; 11]$, which is a symmetric design, intersect pairwise in precisely two elements. Thus we may choose at most two blocks from each of the five cyclic sets, and so at most ten blocks in all, whereas a $B[5, 2; 11]$ has eleven blocks. This leaves the possibility that the design might be the union of a $B[5, 4; 11]$ with a $B[5, 6; 11]$. To show that this cannot be so we apply results of Breach and Thompson [1].

LEMMA. *A* $B[5, 4; 11]$ *design has the following properties:*

(i) if there is a disjoint pair of blocks then each of them intersects all other blocks of the design in at least two points;

(ii) no block can intersect more than one other block in four points;

(iii) if two blocks intersect in four points then each of them intersects all the blocks of the design.

Consider those blocks of our $B[5, 10; 11]$ which are developed from D_1.

(a) Suppose that no two consecutive blocks can be taken from the

https://doi.org/10.1017/S0004972700002318 Published online by Cambridge University Press

cycle so at most five blocks can be chosen. Five such blocks must contain a disjoint pair. For example, without loss of generality, we can choose the blocks D_1, $D_1 + 2$, $D_1 + 4$, $D_1 + 6$, $D_1 + 8$. Then $D_1 \cap (D_1+6) = \emptyset$. But $|D_1 \cap (D_1+4)| = 1$, which contradicts *(i)* of the lemma.

Hence if no two blocks are consecutive then at most four blocks can be chosen from the cycle of D_1.

(b) If two consecutive blocks from the cycle are allowed then they may be taken to be D_1 and $D_1 + 1$. By *(ii)* of the lemma three consecutive blocks are not allowed so $D_1 + 2$ and $D_1 + 10$ are then forbidden. Also

$$D_1 \cap (D_1+5) = D_1 \cap (D_1+6) = (D_1+1) \cap (D_1+6) = (D_1+1) \cap (D_1+7) = \emptyset$$

and by *(iii)* of the lemma $D_1 + 5$, $D_1 + 6$, $D_1 + 7$ are forbidden also. Another application of *(iii)* shows that at most two of $D_1 + 3$, $D_1 + 4$, $D_1 + 8$, $D_1 + 9$ are possible.

Hence no more than four blocks can be chosen from the cycle of D_1. Since $x \to 2x \pmod{11}$ is transitive on $\{D_1, D_2, D_3, D_4, D_5\}$ we can take no more than four blocks from each of five cycles to give at most 20 blocks. But a $B[5, 4; 11]$ has 22 blocks.

This shows that our design is irreducible not just into cyclic subdesigns but into any subdesigns. However a design developed from a minimal family of supplementary difference sets may be reducible as the following example shows.

EXAMPLE 2. Let $D_1 = \{0, 1, 2\}$, $D_2 = \{0, 3, 6\}$, $D_3 = \{0, 4, 8\}$, $D_4 = \{0, 1, 3\}$, $D_5 = \{0, 3, 5\}$, $D_6 = \{0, 4, 5\}$ be supplementary difference sets modulo 10. These generate a $B[3, 4; 10]$ design and are a minimal family. Nevertheless the design can be decomposed into two $B[3, 2; 10]$ designs. The blocks of one of these designs are given in Table 1 (page 108).

EXAMPLE 3. The sets $D_1 = \{0, 1, 3, 4\}$, $D_2 = \{0, 5, 7, 12\}$,

https://doi.org/10.1017/S0004972700002318 Published online by Cambridge University Press

TABLE 1. A $B[3, 2; 10]$ design contained in a $B[3, 4; 10]$ design generated by a minimal family of supplementary difference sets.

012	036	159	124	035	045
234	258	371	346	257	267
456	470	593	568	479	489
678	692	715	780	691	601
890	814	937	902	813	823

$D_3 = \{0, 4, 6, 9\}$ form a family of supplementary difference sets modulo 13 corresponding to a $B[4, 3; 13]$. This design is irreducible. Supposing it were reducible, then it would contain a $B[4, 1; 13]$ with a, b and c blocks belonging to the cycles of D_1, D_2 and D_3 respectively. Table 2 shows the number of times $\pm i$, $i = 1, \ldots, 6$ occurs as a difference of two elements from D_j, $j = 1, 2, 3$. Certainly the family is minimal.

TABLE 2. Number of times that i occurs as a difference, modulo 13, of two elements from D_j.

i	D_1	D_2	D_3
±1	2	1	0
±2	1	1	1
±3	2	0	1
±4	1	0	2
±5	0	2	1
±6	0	2	1

Now the a, b and c blocks that together form a $B[4, 1; 13]$ design contain every unordered pair of elements just once and therefore constitute a family of supplementary difference sets, modulo 13. When developed cyclically these yield a $B[4, 13; 13]$ design which contains a copies of the cycle from D_1, b copies of the cycle from D_2 and c copies of the cycle from D_3. By counting the number of times elements

https://doi.org/10.1017/S0004972700002318 Published online by Cambridge University Press

differing by $\pm i$, $i = 1, \ldots, 6$ occur together we obtain (from Table 2)

$$\begin{aligned} 2a + b &= 13 , \\ a + b + c &= 13 , \\ 2a + c &= 13 , \\ a + 2c &= 13 , \\ 2b + c &= 13 , \\ 2b + c &= 13 . \end{aligned}$$

The only solution these equations have is

$$a = b = c = \frac{13}{3}$$

which for integral a, b, c is impossible. Therefore the $B[4, 3; 13]$ is irreducible.

II. Towards a general theory

THEOREM 1. *Let $D_1, D_2, \ldots, D_m$ be a family of supplementary difference sets, modulo v , which generate a $B[k, \lambda; v]$ design (so $|D_i| = k$). If this design contains a $B[k, \mu; v]$ subdesign then λ divides both $m\mu v$ and $m\mu k$.*

Proof. In any $B[k, \lambda; v]$ design the number of blocks is $\big(v(v-1)/k(k-1)\big)\lambda$. Let the subdesign have a_i blocks in the cycle of D_i . Then a count of blocks gives

$$a_1 + a_2 + \ldots + a_m = \frac{v(v-1)}{k(k-1)}\,\mu = \frac{v(v-1)}{k(k-1)}\,\lambda \cdot \frac{\mu}{\lambda} = mv\,\frac{\mu}{\lambda} ,$$

since each D_i provides v blocks in the $B[k, \lambda; v]$ design.

In any $B[k, \lambda; v]$ design each symbol is incident with exactly $\big((v-1)/(k-1)\big)\lambda$ blocks. But in the cyclically generated design each D_i generates a cycle of blocks containing each symbol k times. Therefore $\big((v-1)/(k-1)\big)\lambda = mk$. For the subdesign the number of incidences per symbol is $\big((v-1)/(k-1)\big)\mu$ so $m\mu k/\lambda$ must be an integer. □

Note that it is not necessary to have a minimal set of difference sets for the theorem to apply.

This test quickly decides the case of Example 2 where for a subdesign

https://doi.org/10.1017/S0004972700002318 Published online by Cambridge University Press

to exist we must have $4 \cdot 13 \cdot \mu/3$ an integer. The smallest value for μ is 3 corresponding to the original $B[4, 3; 13]$ design.

For the case of just two supplementary difference sets, we can say much more as indicated by

THEOREM 2. *Let D_1 and D_2 be minimal supplementary difference sets, modulo v, for a $B[k, \lambda; v]$ design. Then any subdesign must be symmetric and must contain half the blocks of each of the cycles of D_1 and D_2.*

Proof. Suppose that $\pm i$ occurs α_i times as a difference of elements in D_1 and β_i times as a difference of elements from D_2. Then

$$\alpha_i + \beta_i = \lambda \quad \text{for} \quad i = 1, 2, \ldots, [v/2] . \tag{1}$$

Since neither of D_1 and D_2 taken separately is a difference set there is at least one value of i for which $\alpha_i \neq \beta_i$.

If a blocks of the first cycle and b blocks of the second cycle are used to make a $B[k, \mu; v]$ then (see Theorem 1)

$$a + b = 2\mu v/\lambda . \tag{2}$$

This collection of blocks treated as supplementary difference sets generates a $B[k, v\mu; v]$ design. If we count the number of occurrences of pairs of elements differing by $\pm i$ (modulo v) we find that

$$a\alpha_i + b\beta_i = \mu v . \tag{3}$$

If λ is eliminated between (1) and (2) then

$$(\alpha_i+\beta_i)(a+b) = 2\mu v . \tag{4}$$

Now if v is eliminated from (3) and (4) we find that

$$(a-b)(\alpha_i-\beta_i) = 0 \tag{5}$$

for all i. But $\alpha_i \neq \beta_i$ for at least one i so

$$a = b = \mu v/\lambda .$$

https://doi.org/10.1017/S0004972700002318 Published online by Cambridge University Press

Furthermore, for any balanced incomplete block design, Fisher's inequality holds and demands that the number of blocks be not less than the number of elements. The blocks not taken from each cycle also form a design to which Fisher's inequality also applies. Therefore $a = b = v/2$. Thus the sub-design has equal numbers of elements and blocks and is therefore symmetric with $\mu = \frac{1}{2}\lambda$. □

COROLLARY. *If* $B[k, \lambda; v]$ *is a design generated by a minimal pair of supplementary difference sets,* D_1 *and* D_2 *, and* λ *is odd then the design is not reducible.*

As a prologue to our principal theorem and to introduce some notation we consider a further example on supplementary difference sets. This is a generalisation of Example 1.

EXAMPLE 4. Let p be a prime, with $p = 2s + 1$. Let a *standard set* of integers modulo p be a set of the form

$$\{a, a+\alpha, a+2\alpha, \ldots, a+h\alpha\} \subseteq \{0, 1, \ldots, p-1\}$$

where $\alpha \not\equiv 0 \pmod{p}$. Then the family of all standard sets of s elements each is a $B[s, \frac{1}{2}s(s-1); p]$ design (Street, [3], Lemma 2). This design is generated from the supplementary difference sets

$$D_\alpha = \{0, \alpha, 2\alpha, \ldots, (s-1)\alpha\} , \quad \alpha = 1, 2, \ldots, s .$$

It is convenient to make this family of sets by using a primitive root of p .

LEMMA. *Let* x *be a primitive root of the prime* $p = 2s + 1$ *. For the residues* $x^i \pmod{p}$, $0 \le i < s$, *write* $\|x^i\|$ *for whichever of* x^i *and* $p - x^i$ *lies between* 0 *and* s *. Then as* i *runs from* 0 *to* $s - 1$, $\|x^i\|$ *runs through the set of integers* $\{1, 2, \ldots, s\}$ *in some order.*

Proof. Since x is a primitive root of p , $x^0 = 1 \equiv x^{p-1}$ and $x^s \equiv -1 \pmod{p}$. Let $0 \le \alpha \le s-1$ and $0 \le \beta \le s-1$ and suppose $\alpha \ne \beta$. If $\|x^\alpha\| = \|x^\beta\|$ then either $x^\alpha \equiv x^\beta \pmod{p}$, which is impossible if x is a primitive root, or $x^\alpha \equiv p - x^\beta \pmod{p}$. But then

https://doi.org/10.1017/S0004972700002318 Published online by Cambridge University Press

$x^{\alpha-\beta} \equiv -1 \equiv x^{s} \pmod{p}$ and $|\alpha-\beta| = s$ which is impossible from the given bounds on α and β. Hence for $0 \leq i \leq s-1$ the numbers $\|x^{i}\|$ are all distinct and so must form the set $\{1, 2, \ldots, s-1\}$. □

As a consequence the set $\{0, \|x^{0}\|, \|x^{1}\|, \ldots, \|x^{s-1}\|\}$ is the set $D_{(1)} = \{0, 1, 2, \ldots, s-1\}$. The supplementary difference set $D_{(m)}$ is formed from $D_{(1)}$ by multiplying the elements by x^{m-1} and reducing modulo p. Symbolically

$$D_{(m)} = x^{m-1}D_{(1)} \pmod{p} .$$

Now suppose d is fixed and that $d = \alpha_{j} - \alpha_{k}$ for q pairs (j, k) where $\alpha_{j}, \alpha_{k} \in D_{(1)}$. Then in $D_{(m)}$ the difference $x^{m-1}d \pmod{p}$ occurs q times. Let n_{ij} be the number of times $\|x^{i}\|$ occurs as a difference in $D_{(j)}$ and construct the matrix $N = [n_{ij}]$. Then for the current example N is a circulant and every row and every column contains the integers $0, 1, 2, \ldots, s-1$. In other words the easily determined differences over the set $D_{(1)}$ cyclically determine the distribution over $D_{(m)}$. Since N has a constant row sum $\frac{1}{2}s(s-1)$ the sets $D_{(m)}$ generate a $B[s, \frac{1}{2}s(s-1); p]$ design. Note the sets $D_{(m)}$ and D_{m} are in general not the same. However the use of the multiplier x on $D_{(1)}$ generates the family D_{m}, modulo p, in some order.

To return to Example 1 we note that the set $\{0, 3, 6, 9, 1\}$ as a difference set is equivalent to $\{0, 8, 5, 2, 10\} = D_{(4)}$. Now 2 is a primitive root of 11 and this leads to the matrix

$$N = \begin{bmatrix} 4 & 0 & 2 & 1 & 3 \\ 3 & 4 & 0 & 2 & 1 \\ 1 & 3 & 4 & 0 & 2 \\ 2 & 1 & 3 & 4 & 0 \\ 0 & 2 & 1 & 3 & 4 \end{bmatrix} , \text{ and } \operatorname{Det} N = 1550 .$$

(We suspect that for general n, the determinant of N is non-zero, but

https://doi.org/10.1017/S0004972700002318 Published online by Cambridge University Press

have been unable to prove it.)

Suppose a subdesign $B[5, \mu; 11]$ exists, and it contains a_j blocks from the cycle of $D_{(j)}$. Let $\mathbf{a}$ be the column vector with ith component a_i and let $\mathbf{e}$ be the column vector each of whose components is 1. Then by taking the blocks of the subdesign to be supplementary difference sets for a $B[5, 11\mu; 11]$ design we arrive at the matrix equation

$$N\mathbf{a} = 11\mu\mathbf{e} . \tag{6}$$

Since $\operatorname{Det} N \neq 0$ this has a unique solution for $\mathbf{a}$ which must be proportional to μ, as $\mathbf{e}^T = [1, 1, \ldots, 1]$. But when $\mu = 10$ we know that the solution exists because the given $B[5, 10; 11]$ is also described by (6). In that case all the a_i's are equal to 11 and so (6) has the solution

$$a_1 = a_2 = a_3 = a_4 = a_5 = 11\mu/10 .$$

The only possible value for μ is 10 so the $B[5, 10; 11]$ design is not reducible.

In general suppose that $D_1, D_2, \ldots, D_n$ are a minimal set of supplementary difference sets modulo v with $|D_i| = k$ which generate a $B[k, \lambda; v]$ design. Define the difference distribution matrix N as before. In general N will not be square. Suppose there is a $B[k, \mu; v]$ subdesign with $a_1, a_2, \ldots, a_n$ blocks from cycles of $D_1, D_2, \ldots, D_n$ respectively. Let the vectors $\mathbf{a}$ and $\mathbf{e}$ be defined as before. Then we have the general Theorem 3.

THEOREM 3. *If the rank of N is n then a subdesign $B[k, \mu; v]$ of the design $B[k, \lambda; v]$ generated by the minimal family of supplementary difference sets $D_1, D_2, \ldots, D_n$ must contain exactly v blocks from each of the cycles generated by $D_1, D_2, \ldots, D_n$.*

Proof. For the equation

$$N\mathbf{a} = v\mu\mathbf{e} \tag{7}$$

(analogous to equation (6)) to have a solution for $\mathbf{a}$ the rank of N must

https://doi.org/10.1017/S0004972700002318 Published online by Cambridge University Press

equal the rank of the augmented matrix $[N, v\mu\mathbf{e}]$. If this condition is satisfied and rank $N = n$, since the components of $\mathbf{e}$ are all unity, the components of $\mathbf{a}$ are proportional to $v\mu$. But when $\mu = \lambda$ equation (7) has the solution $\mathbf{a} = v\mathbf{e}$ corresponding to the given $B[k, \lambda; v]$ design. Therefore (7) has the solution $a = (v\mu/\lambda)\mathbf{e}$ and no other solution since the rank of N is n . Hence the theorem. □

If rank $N < n$ it is still algebraically possible for (7) to have solutions provided rank N = rank$[N, v\mu\mathbf{e}]$. In such cases the columns of N will be linearly dependent. Since each column corresponds to a supplementary difference set we may say that these sets are *linearly dependent with respect to differences*. Now if the family of difference sets is not minimal then it is easy to show that they are linearly dependent with respect to differences. However it is conceivable that a family of supplementary difference sets could be linearly dependent with respect to differences and yet be minimal in which case equation (7) might have a fundamentally different solution for $\mathbf{a}$. We are uncertain whether this can ever happen if $v|b$; we suspect not. However if $v\nmid b$, then it certainly can, as is shown by the following.

EXAMPLE 5. $D_1 = \{0, 1, 3\}$, $D_2 = \{0, 1, 4\}$, $D_3 = \{0, 3, 4\}$, $D_4 = \{0, 2, 4\}$ form a minimal family of supplementary difference sets modulo 9 , and generate a $B[3, 3; 9]$. This design has a $B[3, 1; 9]$ subdesign, consisting of three blocks from the first cycle (013, 346, 670) , six from the third (145, 256, 478, 580, 712, 823) and three from the fourth (024, 357, 681) . Since 014 belongs to no parallel class, the remaining blocks form an irreducible $B[3, 2; 9]$; it is isomorphic to [2, #30].

References

[1] D.R. Breach and A.R. Thompson, "Reducible 2-(11, 5, 4) and 3-(12, 6, 4) designs", *J. Austral. Math. Soc. Ser. A* (to appear).

[2] Elizabeth J. Morgan, "Some small quasi-multiple designs", *Ars Combin.* 3 (1977), 233-250.

[3] Anne Penfold Street, "On quasi-multiple designs", *Combinatorial Mathematics* V, 206-208 (Lecture Notes in Mathematics, 622. Springer-Verlag, Berlin, Heidelberg, New York, 1977).

Department of Mathematics,
University of Canterbury,
Christchurch,
New Zealand;

Department of Mathematics,
University of Queensland,
St Lucia,
Queensland 4067,
Australia.

https://doi.org/10.1017/S0004972700002318 Published online by Cambridge University Press