Rev. Téc. Ing., Univ. Zulia
Vol.2 , N°1 y 2 , 1979

A RING PARTITION CONSTRUCTION FOR BIBDS

R.C. Mullin
Department of Combinatories and Optimization
Faculty of Mathematics
University of Waterloo
Waterloo, Ontario, Canada

ABSTRACT

A method for finding initial difference blocks for certain balanced incomplete block designs by means of partitions of elements in finite rings is given. It is shown that multiplier theory for difference sets, when expressed in terms of finite rings, can be useful in certain instances for obtaining appropriate partitions. In particular, despite the non-existence of a difference set for a (*49, 49, 16, 16, 5*) design, one can construct a (*49, 98, 32, 16, 10*) design by attempting the former.

RESUMEN

En este trabajo se da un método para encontrar "bloques diferencia" iniciales para cierto diseño de bloque incompleto balanceado (equilibrado) por medio de particiones de elementos en anillos finitos.

Se prueba que la teoría de multiplicadores para conjuntos diferencia, cuando se expresan en términos de anillos finitos, puede ser útil en ciertos casos para obtener particiones apropiadas.

En particular, a pesar de la no existencia de un conjunto diferencia para un diseño (*49, 49, 16, 16, 5*) se puede construír un diseño (*49, 98, 32, 16, 10*) por experimentación del anterior.

1. DIFFERENCE SETS AND CYCLIC MULTIPLIERS REVISITED

Let G denote a finite Abelian group of order v (written additively). A difference set in G is a subset $D = \{d_1, d_2, \ldots, d_k\}$ of elements of G such that every non-zero group element g can be expressed in exactly λ ways in the form

$$d_i - d_j = g,$$

where d_i and d_j belong to D. It is easily verified that

$$\lambda = k(k-1) / (v-1) .$$

This is also a consequence of the fact that such a difference set can be used to generate the incidence matrix of a (v,k,λ) configuration by a well-known construction [1].

If G is cyclic, we refer to D as a cyclic difference set. Let $D = \{d_1, d_2, \ldots, d_k\}$ and $D' = \{d_1', d_2', \ldots, d_k'\}$ be cyclic difference sets on the same parameters (v,k,λ). Let t be an integer such that $(t, v) = 1$ and s be an arbitrary integer. Then

$E = \{td_1, td_2, \ldots, td_k\} = tD$ and $E' = \{d_1' + s, d_2' + s, \ldots, d_k' + s = D + s$

are both cyclic difference sets. Then t is a multiplier of the difference set if there exists an integer s such that $E = E'$.

Multipliers for cyclic difference sets form an important part of cyclic difference set theory. The reader is referred to Baumert [1] for an excellent account of that theory.

A common extension of the theory of multipliers from cyclic groups to arbitrary finite groups G is made in terms of the group algebra of G over a suitable field or ring, frequently the ring of rational integers. Although that approach does not differ greatly from that taken here, the present point of view is advantageous for the main construction of this paper. Despite the existence of certain difference sets, it is still possible, in some instances, to obtain useful information for the construction of certain designs.

2. RINGS AND DIFFERENCE SETS

Every finite Abelian group can be written as the additive group of a commutative ring with identity. Indeed, since every Abelian group can be written as the direct product of cyclic groups, the direct product of corresponding modular rings would serve the purpose. There are in general many rings which can be associated with each Abelian group; often others than those mentioned above are more convenient. Our theory deals with an arbitrary ring with identity. Although it is unnecessary for many theorems, we assume that the ring is commutative since this is the case in practice.

Now let R be a finite commutative ring with identity. Any ring referred to henceforth is assumed to be of this type. The additive period of 1 is the *characteristic* of the ring, and if the ring has characteristic m, then we can view the ring of integers modulo m as a subring M of R. Indeed M is the subring generated by 1. We refer to M as the integer ring of R, and identify the integers in R with the corresponding rational integers whenever convenient. Clearly if $(t,m) = 1$, t is invertible in R. For notational convenience we denote an integer in R by a lower case Latin letter, and use the same symbol if we are viewing this element as a rational integer. Arbitrary elements of R will be denoted by lower case Greek letters.

Let D be a difference set in (the additive structure of) a ring R. Let t be an integer in R. Then t is a multiplier of D if there exists an element α in R such that $tD = D + \alpha$.

A multiplier t is said to fix a difference set D if $tD = D$.

The following results are cited without proof. They are essentially variants of standard results obtained by employing the group algebra.

LEMMA 2.1 *Let R be a ring of characteristic m. If t is a multiplier of a difference set D and if $(t-1, m) = 1$, then there is a difference set D^* that is fixed by t.*

LEMMA 2.2 *Let D be a (v,k,λ) difference set in a ring R with* *character set C and characteristic m. Let n be a product of distinct primes such that $n \mid k-\lambda$, $(n,k) = (n,m) = 1$ and $n > \lambda$. If every prime divisor p_j of n has the property that there exists an integer α_j such that $p_j^{\alpha_j} \equiv t \bmod m$, then t is a multiplier of D.*

3. ADJUGACY CLASSES AND THE MAIN CONSTRUCTION

Let R be a finite ring with identity and let R^* denote the set of non-zero elements of R. Let α be an invertible element of R, and S be a subset of R^*. Then we denote $\{\alpha s : s \in S\}$ by αS. Let $\pi = \{P_1, P_2, \ldots, P_n\}$ be a partition of R^*. Then π is said to be adjugacy partition for α if for each $P_i \in \pi$ there is a part P_j such that $\alpha P_i = P_j$. Clearly $\alpha\pi = \{\alpha P_1, \alpha P_2, \ldots, \alpha P_p\}$ is a permutation of π. Note that a given α may have several adjugacy partitions; every partition is an adjugacy partition for the identity element of R^*. Given a partition π we refer to any invertible element of R^* for which Π is adjugacy class as an adjugate of π. Clearly the set of adjugates of any fixed permutation π is a subgroup of the group of units of R.

Let M denote any multiset of elements of R^* and π be a partition of R^*. Then M is said to be conformal with π if for each part P_i there exists a non-negative integer $f(P_i)$ such that each member of P_i occurs in M with frequency $f(P_i)$. Clearly if M and π are conformal, so are M and $\alpha\pi$ where π is an adjugacy class for α.

Note that the notation $P_1, P_2, \ldots, P_n$ for the parts of π implicitly establishes a bijection between the parts of π and $N=\{1,\ldots,n\}$. Hence, given π and M conformal, and α adjugate to π, we can define a function g_α from N to the non-negative integers by the rule $g_\alpha(i) = f(Q_i^\alpha)$ where Q_i^α is the pre-image of P_i under α. (Technically, g is a function of π and M as well as α, but these are omitted as there is no danger of ambiguity). We define the vector V_α to be the n-tuple $(g_\alpha(1), (g_\alpha(2), \ldots, g_\alpha n)$ (with the same caveat regarding π and M).

THEOREM 3.1 (Main Construction). *Let R be a finite ring with identify and π be a partition of R^*. Let B be a k-subset of R^* such that the multiset M of differences of distinct members of B is conformal with π. If there exists a set $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$ of adjugates of π with vectors V_{α_i} and a set of non-negative integers ε_i, $i=1,2,\ldots,t$ such that $\sum_{i=1}^{t} \varepsilon_i V_{\alpha_i} = (\lambda, \lambda, \ldots, \lambda)$, then there exists a balanced incomplete block design | , p. | with parameters*

$$(|R| \, , \, |Q| \sum_{i=1}^{t} \varepsilon_i \, , k \sum_{i=1}^{t} \varepsilon \, , k \, , \lambda) \, .$$

Proof: Consider the multiset I of "blocks" $\alpha_i B$, $i = 1,2,\ldots,t$ where $\alpha_i B$ is taken with frequency ε_i. Consider the differences generated by these blocks. If d belongs to P_i, then it occurs as a difference $g_\alpha(i)$ times in the set of differences of $\alpha_i B$, and hence $\sum_{i=1}^{t} \varepsilon_i g_\alpha(i)$ times as a difference of elements in the multiset I. Hence I is a set of initial blocks [2] for a design with the specified parameters. □

4. APPLICATIONS

Clearly the difficulty in applying Theorem 3.1 is in finding appropriate adjugacy partitions and adjugates. Sometimes these can be associated with multiplier orbits in "failed" difference sets. We illustrate by showing the existence of a design with parameters $(49, 98, 32, 16, 10)$ which can be obtained by examining a "failed" difference set $(49, 16, 5)$. There is no $(49, 16, 5)$ difference set in either Z_{49} or $Z_7 \times Z_7$. However, let us assume that such were to exist in $Z_7 \times Z_7 = G$. We may view this group as either the additive group of the Galois field $GF(72)$ or the ring product $R_{7,7} = Z_7 \times Z_7$. Let us first consider G as the additive group of $GF(7^2)$. In this ring the integer subring is the ground field $GF(7)$. Now take $p = 11$. Clearly $(11,7) = 1$ and $7 < 11$. Hence $11 \equiv 4$ is a multiplier. Moreover $(3,7) = 1$ Hence any difference set would be fixed by 4. By division by a suitable factor we can assume that $1 \in \mathcal{D}$.

Hence $1,2,4 \in \mathcal{D}$, since these are the powers of $4 \bmod 7$. These are, of course, the quadratic residues $mod\ 7$. Since 4 has multiplicative period $3 \bmod 7$, $\mathcal{D}$ would also contain 0 and 4 other orbits of length 3. Hence $\mathcal{D}$ would have the form

$$\{(0,0),\ (1,0)\ (2,0),\ (4,0)\}\ \bigcup_{i=1}^{4}\ \{(\underline{a_i},b_i),\ (\underline{2a_i},2b_i),\ (\underline{4a_i},4b_i)\},$$

where (α,β) is a member of $Z_7 \times Z_7$, and we identify the ground field $GF(7)$ with the first component.

Now the set $R_i = \{b_i, 2b_i, 4b_i\}$ is the set of residues $mod\ 7$ if b_i is a residue; it is the set of non-residues $mod\ 7$ if b_i is a non-residue, and is $\{0\}$ if $b_i = 0$. Continuing by the criterion that $\mathcal{D}$ should behave as much as possible as a difference set, we decide that $b_i \neq 0$, for $i = 1,2,3,4$.

Indeed, if some $b_i \neq 0$, then $(y,0)$, $y \in GF(7)$ is a subset of $\mathcal{D}$. (The first components of such an orbit must constitute the non-residues $mod\ 7$, since $\mathcal{D}$ contains no repeated elements). Hence each difference $(y,0)$, $y \neq 0$, would occur 7 times in $\mathcal{D}$, contrary to the assumption $\lambda = 5$. In fact, each pair $(y,0)$, $y \neq 0$, would have to occur as a difference 5 times, and hence 0 would have to occur as a difference 30 times in the second component of $\mathcal{D}$. It already occurs 12 times because of the presence of $Z = \{(0,0),\ (0,1),\ (0,2),\ (0,4)\}$. Since $b_i \neq 0$, a second component of $\mathcal{D}$ can not occur as a difference within R_i. Let $\chi(a) = 1$ if a is a residue $mod\ 7$, and $\chi(a) = -1$ if a is a non-residue $mod\ 7$. Then the differences between R_i and R_j would have to have either zero or six second components of 0 according as $\chi(b_i)\ \chi(b_j) = 0\ 1$ or 1 respectively.

Consider the following table.

Number of residues b_i	Number of non-residues b_i	Number of zero differences in second component generated by $\{R_i\}$
0	4	36
1	3	18
2	2	6
3	1	18
4	0	36

Thus either one or three of the b_i would have to be a residue. Similar analysis show that exactly one of the a_i, say a_1, would have to be 0. Moreover, precisely zero or two of the remaining a_i would have to be a residue. Let $A(D)$ denote the number of a_i that are residues in D, and $B(D)$ the number of b_i that are residues in D. There are two possible cases, depending on whether or not b_1 is a residue.

CASE 1. b_1 is a residue. Let $Z^* = Z \cup \{(0,1), (0,2), (0,4)\}$. Let $D^* = D - Z^*$.

Then the following cases are possible.

	$A(D)$	$B(D)$
A_1	0	0
A_2	0	2
A_3	2	0
A_4	2	2

Let us denote by RR, RN, NR and NN the cases in which $a_i b_i$ are both residues, a_i is a residue, b_i is a non-residue, etc. This leads to the following distributions.

A_1	NN	NN	NN
A_2	NN	NR	NR
A_3	NN	RN	RN
A_{41}	RR	RR	NN
A_{42}	RN	RR	NR

By the symmetry between components in Z^*, we see that cases A_2 and A_3 are equivalent.

CASE 2. b_2 is a non-residue. Here we note that if any difference set D in $Z_7 \times Z_7$ is multiplied by an invertible element in the corresponding direct product of rings, the result is also a difference set. By switching to this ring we see that if D were a difference set corresponding to case 2, multiplication by $(1,3)$ would give a difference set corresponding to case 1. Thus we need only consider distributions A_1, A_2, $A_{4,1}$, and $A_{4,2}$.

However it is only necessary to consider distribution A for our present purposes. Since there are only nine distinct pairs of "type" NN, and nine such pairs are required, we have a unique completion of the candidate difference set to $D_1 = \{(0,0), (0,1), (0,2), (0,4), (1,0), (2,0), (4,0), (3,3), (3,5), (3,6), (5,3), (5,5), (5,6), (6,3), (6,5), (6,6)\}$. But D_1 is not a difference set, since $(1,1)$ is represented as a difference only 4 times, whereas $(1,3)$ is represented 6 times. The set D_1 is still useful nonetheless. If we view G as the direct product of rings $Z_7 \times Z_7 = R$, we define a partition π of R^* as follows. (Result that if $\alpha \in Z_7^*$, then $\chi(\alpha) = 1$ if α is a quadratic residue, and $\chi(\alpha) = -1$ otherwise). Let $P_1 = \bigcup_{\alpha \in Z_7^*} \{(0,\alpha), (\alpha,0)\}$, $P_2 = \{(\alpha,\beta) : \alpha,\beta \in Z_7^*\ \chi(\alpha\beta) = 1\}$ and $P_3 = \{(\alpha,\beta) : \alpha\,\beta \in Z_7^*,\ \chi(\alpha\beta) = -1\}$. We show that M, the multiset of differences of D_1 is conformal with π. Noting that $R = \{1,2,4\}$ and $N = \{3,5,6\}$ are $(7,3,1)$ difference sets in D it is trivial that every element of P_1 occurs precisely 5 times in M. Now each element of the form (α,β), $\alpha\beta \neq 0$ is represented as a difference of the members of $N \times N = H$. Now let $D_1 - H = K$. Then clearly no member of P_2 can occur as a difference of members of K. Moreover since $[R - N]$, the multiset of differences between R and N in that order can be written in the form $R + 2N$, each member of P_2 occurs exactly 3 times as a difference between elements of H and K in some order. Hence each member of P_3 occurs precisely 4 times in M. Now consider any member of P_3. It occurs precisely once as a difference of members of K. Further, since $[N - R] = N + 2R$, every element of P_3 can be written precisely 4 times as a difference between members of H and K in some order. Therefore each member of P_3 occurs 6 times in M. In summary, $\delta(P_1) = 5$, $\delta(P_2 = 4)$, $\delta(P_3) = 6$. Now clearly $(1,1)$ and $(1,3)$ are adjugates of π, with $(1,3)P_1 = P_1$ and $(1,3)P_2 = P_3$. Moreover $V_{(1,1)} = (5,4,6)$ and $V_{(1,3)} = (5,6,4)$. Applying theorem 3.1, we see that D_1 and $(1.3)D_1$ are a pair of initial blocks for a $(49, 98, 32, 16, 10)$ BIBD. This design is listed as unknown in the catalogue of Collens [3]. The set D_1 is not the only candidate that is conformal with π. Many of the other orbit structures of the other distributions of this section work as well, illustrating the tendency of multiplier orbits to correspond to adjugacy partitions. In those instances when the orbit lengths are incompatible with k however, the present techniques to not apply. For example, consider the case of a $(121,16,2)$ difference set in $Z_{11} \times Z_{11}$. In this case there would be a difference set fixed by 7. But 7 is primitive in $GF(11)$ hence it has period 10. Since $k = 16$, no attempt at a "multiple copy" of the corresponding design is possible by the preceding methods.

REFERENCES

[1] BAUMERT, L.D.: "*Cyclic Difference Sets*", Lecture Notes in Mathematics 182, Springer-Verlag, Berlin (1971).

[2] BOSE, R.C. : "*On the Construction of Balanced Incomplete Block Designs*", Ann. Eugenics, 9 (1939) 353 - 399.

[3] COLLENS, R.J.: "A *Listing of Balanced Incomplete Block Designs*", Proc. Fourth Southeastern Conference on Combinatorics, Graph Theory, and Computing, Boca Raton (1973), 187 - 231.