BALANCED INCOMPLETE BLOCK DESIGNS AND ABELIAN DIFFERENCE SETS[1]

BY

H. B. MANN

1. Balanced incomplete block designs

A balanced incomplete block design (b.i.b.) is an arrangement of v objects into b sets of k elements each called blocks such that every object occurs exactly r times and every pair of objects occurs exactly λ times in a block. Counting objects and pairs of objects in two different ways, one obtains the well-known equations

$$bk = rv, \qquad \lambda(v-1) = r(k-1). \tag{1}$$

In this paper we shall first give a new representation of balanced incomplete block designs in terms of permutation matrices, from which several known theorems follow easily. The main body of the paper is concerned with the study of Abelian difference sets. The paper contains several new results together with a self-contained exposition of known results. Theorem 3 gives a new condition for the existence of these difference sets, valid for every prime divisor of $n = k - \lambda$. Theorem 5 generalizes results previously obtained for cyclic difference sets to Abelian difference sets. Theorems 6 and 7 give a new result for cyclic difference sets which disposes of 9 of the 12 cases which are mentioned as unsettled in [3]. Another of these unsettled cases is disposed of by Theorem 3.

For any given b.i.b., we define a $v \times b$ matrix $A = (a_{ij})$ where

$a_{ij} = 1$ if the i^{th} object occurs in the j^{th} block,

$a_{ij} = 0$ otherwise.

From the properties of the design we then have

$$AA^t = (r-\lambda)I + \lambda T, \tag{2}$$

where I is a $v \times v$ unit matrix and T is a $v \times v$ matrix all of whose entries are unity. Since for every real matrix A

$$\operatorname{rank} AA^t = \operatorname{rank} A,$$

it follows that

$$b \geqq v,$$

an inequality first derived by R. A. Fisher [2].

We now assume $b = v$; hence $r = k$ and $\lambda(v-1) = k(k-1)$. Putting

Received October 8, 1962.

[1] This research was completed during the author's summer 1962 visit to the Boeing Scientific Research Laboratories, Seattle, Washington.

$k - \lambda = n$, we then have

$$AA^t = nI + \lambda T. \tag{2a}$$

We have $AT = TA = kT$; hence

$$A(A^t - (\lambda/k)T) = nI, \qquad A^{-1} = (1/n)(A^t - (\lambda/k)T),$$

and

$$A^tA = AA^t = nI + \lambda T,$$

which shows that in a symmetrical b.i.b. any two blocks have λ objects in common, a result which was also first obtained by R. A. Fisher. The determinant of the right-hand side of (2a) is $k^2n^{v-1} = |A|^2$. Hence we have

THEOREM 1. *If v is even, then $n = k - \lambda$ is a square.*

This result was obtained independently by Schützenberger [7] and by Chowla and Ryser [1].

THEOREM 2. *A symmetric b.i.b. with parameters v, k, λ exists if and only if there are k permutations $P_1, \cdots, P_k$ of order v such that*

(i) *The permutations $P_1, \cdots, P_k$ applied to $1, \cdots, v$ yield a $k \times v$ Latin rectangle.*

(ii) *For $s \neq t$, $s, t = 1, \cdots, v$ there are among the permutations $P_iP_j^{-1}$ exactly λ which carry s into t.*

Proof. Let $P_1, \cdots, P_k$ satisfy the conditions of Theorem 2. Condition (i) implies that there is for $s \neq t$ at most one permutation among $P_1, \cdots, P_k$ which carries s into t. This means that

$$A = \sum_{i=1}^{k} P_i$$

is a matrix of zeros and ones. Condition (ii) now gives

$$\sum_{i=1}^{k} P_i \sum_{i=1}^{k} P_i^{-1} = kI + \lambda(T - I) = nI + \lambda T.$$

Hence A is the incidence matrix of a symmetrical b.i.b.

On the other hand, if A is the incidence matrix of a symmetrical b.i.b., then A is a doubly stochastic matrix of zeros and ones with row and column sums equal to k. By a theorem of König (for a short proof see [5]) it is therefore the sum of k permutation matrices $P_1, \cdots, P_k$, and from (2a) we get

$$\sum_{i=1}^{k} P_i \sum_{i=1}^{k} P_i^{-1} = nI + \lambda T,$$

which shows that $P_1, \cdots, P_k$ satisfy (ii). The equation $\sum P_i = A$ shows that also (i) is satisfied, and this ends the proof.

COROLLARY 2.1. *The blocks of a symmetrical b.i.b. may be numbered in such a way that the i^{th} block contains the i^{th} object, and the objects in the blocks may be arranged in such a way that every object occurs once in every position.*

Proof. If $P_1, \cdots, P_k$ satisfy (i) and (ii), then so do $I, P_1^{-1}P_2, \cdots, P_1^{-1}P_k$, and this gives the first part of Corollary 2.1. If $P_j(l) = s$, then $a_{ls} = 1$, and

we put the l^{th} object in the j^{th} position in the s^{th} block. Since P_j must transform exactly one digit into s, every object occurs exactly once in the j^{th} position. (Note that the proof of Corollary 2.1 goes through for every symmetrical block design. The condition that every pair of objects occur λ times was not used in the proof.)

A symmetrical b.i.b. with $\lambda = 1$ *is called a finite geometry.* We then have $v = n^2 + n + 1$, and Theorem 2 gives

COROLLARY 2.2. *A finite geometry of order* $v = n^2 + n + 1$ *exists if and only if there are* $n + 1$ *permutations* $P_1, \cdots, P_{n+1}$ *such that* $I, P_2, \cdots, P_{n+1}, P_2^{-1}, P_3 P_2^{-1}, \cdots, P_{n+1} P_n^{-1}$ *applied to* $1, \cdots, v$ *give the rows of a Latin square.*

The proof of Corollary 2.2 may be left to the reader.

COROLLARY 2.3. *If a group* $\mathfrak{G}$ *of order* v *contains* k *distinct elements* $g_1, \cdots, g_k$ *such that* $g_j g_i^{-1}$, $i \neq j$ *represents every element except the unit element* λ *times, and if* $P_1, \cdots, P_k$ *are permutations representing* $g_1, \cdots, g_k$ *in the regular representation, then*

$$A = P_1 + \cdots + P_k$$

is the incidence matrix of a b.i.b.

One can construct the regular representation by multiplying $g_1, \cdots, g_k$ successively from the left (or right) by the elements of $\mathfrak{G}$. Hence the b.i.b. can be obtained by forming the blocks

$$g_1 g, \quad \cdots, \quad g_k g$$

or the blocks $gg_1, \cdots, gg_k$ for all $g \in \mathfrak{G}$.

The elements $g_1, \cdots, g_k$ are called a difference set of order λ for the group $\mathfrak{G}$. If $\mathfrak{G}$ is Abelian, then the set $g_1, \cdots, g_k$ is called an Abelian difference set.

2. Abelian difference sets

If $\mathfrak{A}$ is a set of elements in $\mathfrak{G}$, then we shall denote by A the sum of the elements of $\mathfrak{A}$ in the group ring of $\mathfrak{G}$ over any ring with unit element. Similarly for any set denoted by a German letter we shall denote by the corresponding Latin letter the sum of the elements in the set. In particular

$$G = \sum_{g \in \mathfrak{G}} g.$$

The following lemma seems crucial for the study of Abelian difference sets.

LEMMA 1. *If* A *is any element of the group ring of an Abelian group* $\mathfrak{G}$ *of order* v *over a field* Ω *whose characteristic is prime to* v, *and if* $\chi(A) = 0$ *for all nonprincipal characters* χ *of* $\mathfrak{G}$, *then*

$$A = \mu G, \qquad \mu \in \Omega. \tag{3}$$

Proof. Since the characteristic does not divide v, the regular representation

of $\mathfrak{G}$ is completely reducible [8, vol. 2, p. 237]. Hence there is a nonsingular matrix S such that for every $g \in \mathfrak{G}$

$$S^{-1}gS = \operatorname{diag}(1, \chi_2(g), \cdots, \chi_v(g)).$$

Here for some $h \in \Omega$

$$S^{-1}GS = (v, 0, \cdots, 0), \qquad S^{-1}AS = (h, 0, \cdots, 0), \qquad S^{-1}AS = \mu S^{-1}GS,$$

$$A = \mu G, \qquad \mu \in \Omega, \qquad \text{Q.E.D.}$$

COROLLARY. *If $\chi(A) = 0$ for every character χ of $\mathfrak{G}$, then $A = 0$.*

This follows, since $\chi_1(G) = v \not\equiv 0$.

LEMMA 2. *Let $v \not\equiv 0 \pmod{p}$, and assume that A is an element of the group ring $\mathfrak{R}$ of $\mathfrak{G}$ over the integers such that for every nonprincipal character χ of $\mathfrak{G}$ we have*

$$\chi(A) \equiv 0 \pmod{p^j}; \tag{4}$$

then

$$A = \mu G + p^j F, \tag{5}$$

where F is an element of $\mathfrak{R}$.

Proof. Let $\mathfrak{p}$ be a prime divisor of p in the field of v^{th} roots of unity. The residues mod $\mathfrak{p}$ form a field of characteristic p which may be considered as an algebraic extension of G.F.(p) which contains the v^{th} roots of unity, that is to say all characters mod p of $\mathfrak{G}$. Thus we may pass from the characters over the rationals to the characters mod p. Equation (4) now implies

$$\chi(A) \equiv 0 \pmod{\mathfrak{p}}$$

for all nonprincipal characters χ of G. Hence we have by Lemma 1

$$A \equiv \mu G \pmod{\mathfrak{p}}.$$

Since the coefficients of $A - \mu G$ are rational integers, it follows that

$$A = \mu G + pF,$$

where F has rational integer coefficients.

Applying induction, assume that

$$A = \mu G + p^s F, \qquad s < j.$$

From (4) we have

$$\chi(A) = p^s \chi(F) \equiv 0 \pmod{p^j}, \qquad \chi(F) \equiv 0 \pmod{p}, \qquad F = \mu_1 G + pF_1.$$

Hence

$$A = \mu' G + p^{s+1} F_1,$$

and Lemma 2 follows by mathematical induction.

For every $A = \sum a_i g_i$ we shall set

$$A(t) = \sum a_i g_i^t .$$

DEFINITION 1. *The integer t is called a multiplier of the difference set $\mathfrak{D} = (g_1, \cdots, g_k)$ if*

$$D(t) = gD, \qquad g \in \mathfrak{G}. \tag{6}$$

Since $\mathfrak{D}$ is a difference set, we must clearly have $(v, t) = 1$.

THEOREM 3. *Let $g_1, \cdots, g_k$ be an Abelian difference set for a group $\mathfrak{G}$ of order v. Let t be a multiplier of this difference set, p a prime divisor of $k - \lambda = n$, and let $v \equiv 0 \pmod{v_1}$, $v_1 > 1$. If for some value of f we have $tp^f \equiv -1 \pmod{v_1}$, then n is exactly divisible by an even power of p. If v^* is the l.c.m. of the orders of the elements of $\mathfrak{G}$, and if $v^* = v_1$, then $k = v$.*

Note that $t = 1$ is permissible.

Proof. We have

$$D(-1)D = nI + \lambda G.$$

There is a nonprincipal character χ of $\mathfrak{G}$ which maps every element into a v_1^{th} root of unity. Since this mapping is a homomorphism of $\mathfrak{G}$ into the v_1^{th} roots of unity, we get

$$\chi(D(-1))\chi(D) = n \equiv 0 \pmod{p^j}, \tag{7}$$

where n is strictly divisible by p^j. Let $\mathfrak{p}$ be a prime divisor of p in the field of v_1^{th} roots of unity. Suppose $\chi(D)$ is strictly divisible by $\mathfrak{p}^i$, $i \geqq 0$. The automorphism $\zeta \to \zeta^p$ where ζ is a primitive v_1^{th} root of unity leaves $\mathfrak{p}$ invariant. Hence

$$\chi(D) \equiv \chi(D(t)) \equiv \chi(D(tp^f)) \equiv \chi(D(-1)) \equiv 0 \pmod{\mathfrak{p}^i}.$$

Conversely, $\chi(D(-1)) \equiv 0 \pmod{\mathfrak{p}^i}$ implies $\chi(D) \equiv 0 \pmod{\mathfrak{p}^i}$, so that (7) implies $j = 2i$ and

$$\chi(D) \equiv 0 \pmod{p^i}.$$

If $v_1 = v^*$, then this is true for every nonprincipal character of $\mathfrak{G}$. In this case also $(v, p) = 1$, and by Lemma 2

$$D \equiv \mu G \pmod{p}.$$

Hence $\mu \equiv 1 \pmod{p}$ and $D = G$.

This completes the proof of Theorem 3.

LEMMA 3. *Let $\mathfrak{D}$, $\mathfrak{D}^*$ be two difference sets with parameters v, k, λ for the same group $\mathfrak{G}$. If*

$$D(-1)D^* = \lambda G + mF, \tag{8}$$

where m is an integer, $m > \lambda$, and F has integral coefficients, then

$$D^* = gD, \qquad g \in \mathfrak{G}.$$

Proof. Applying the automorphism $g \to g^{-1}$ we have

$$DD^*(-1) = \lambda G + mF(-1), \tag{8'}$$

and applying χ_1 we get

$$n = k^2 - \lambda v = m\chi_1(F).$$

On the left of (8) all elements have nonnegative coefficients, and since $m > \lambda$, it follows that F has nonnegative coefficients. Multiplying (8) and (8') together we get, on account of $mFG = m\chi_1(F)G = nG$,

$$n^2 = m^2FF(-1).$$

But a product of factors with nonnegative coefficients and of more than one term cannot reduce to one term, and therefore

$$mF = ng, \qquad g \in \mathfrak{G}.$$

Multiplying (8) by D we get, after some simplification,

$$D^* = gD, \qquad \text{Q.E.D.}$$

THEOREM 4. *Let $\mathfrak{D}$, $\mathfrak{D}^*$ be two Abelian difference sets for the group $\mathfrak{G}$ with parameters, v, k, λ. Let n be divisible by p^j, $j > 0$, $(p, v) = 1$. If for every character χ of $\mathfrak{G}$ we have*

$$(\chi(D^*), p^j) = (\chi(D), p^j),$$

then

$$D(-1)D^* = \lambda G + p^jF, \tag{9}$$

where F has integral coefficients.

Proof. We have

$$D(-1)D = D^*(-1)D^* = nI + \lambda G.$$

Hence for every nonprincipal character χ of $\mathfrak{G}$

$$\chi(D(-1))\chi(D) = \chi(D^*(-1))\chi(D^*) = n \equiv 0 \pmod{p^j}.$$

Since $(\chi(D^*), p^j) = (\chi(D), p^j)$, we have for every nonprincipal character χ of $\mathfrak{G}$

$$\chi(D(-1))\chi(D^*) \equiv 0 \pmod{p^j},$$

whence by Lemma 2

$$D(-1)D^* = \mu G + p^jF.$$

Taking the principal character χ_1 on both sides we get

$$k^2 \equiv \mu v \equiv k^2 - n \equiv \lambda v \pmod{p^j}, \qquad \mu \equiv \lambda \pmod{p^j},$$

since $(p, v) = 1$. We may therefore write

$$D(-1)D^* = \lambda G + p^jF, \tag{10}$$

Q.E.D.

COROLLARY 4.1. *If* $n \equiv 0 \pmod{n_1}$, $(n_1, v) = 1, n_1 > \lambda, n_1 = p_1^{e_1} \cdots p_s^{e_s}$, *and if there exists a* t *such that* $p_i^{f_i} \equiv t \pmod{v^*}$ *for suitably chosen values of* f_i, *where* v^* *is the l.c.m. of the orders of the elements of* $\mathfrak{G}$, *then* t *is a multiplier for every difference set* v, k, λ.

Proof. If ζ is a primitive v^{th} root of unity, then the automorphism

$$\zeta \to \zeta^{p_i^{f_i}}$$

of the field Σ of v^{th} roots of unity leaves all primefactors of p_i invariant. Hence $D(t) = D(p_i^{f_i})$ satisfies the conditions of Theorem 4, so that

$$D(-1)D(t) = \lambda G + p_i^{e_i} F_i, \qquad i = 1, \cdots, s.$$

But $p_i^{e_i} F_i = p_j^{e_j} F_j$, $p_i \neq p_j$ implies $F_i \equiv 0 \pmod{p_j^{e_j}}$; hence $p_i^{e_i} F_i = n_1 F$. The corollary now follows from Lemma 3.

Corollary 4.1 as well as Lemma 3 were first proved by Marshall Hall, Jr. for the case that $\mathfrak{G}$ is cyclic [3]. They were generalized to Abelian difference sets by P. K. Menon [6]. However, Lemma 2 simplifies the proof considerably, so that it seemed worthwhile to include it here. Except for the simplification afforded by Lemma 2 the proofs follow essentially Hall's ideas.

Let $v \equiv 0 \pmod{v_1}$. The integer t will be called a v_1 multiplier if for every character χ of $\mathfrak{G}$ for which $\chi(g)$ is a v_1^{th} root of unity for all $g \in \mathfrak{G}$ we have

$$\chi(D(t)) = \chi(g)\chi(D) \qquad \text{for some} \quad g \in \mathfrak{G}.$$

THEOREM 5. *If for some nonprincipal character* χ *of* $\mathfrak{G}$

$$\chi(D) = \zeta\chi(D(-1)) \tag{11}$$

where ζ *is a root of unity, then*

(i) n *is a square or* $n = n_1^2 q^3$ *where* $v \equiv 0 \pmod{q}$ *and* q *is a product of distinct primes* $q_1, \cdots, q_u$.

(ii) *In the latter case* v *is odd, and there is for every* q_i *a* g *in* $\mathfrak{D}$ *for which* $\chi(g)$ *has order divisible by* q_i.

(iii) *If* $q = 4m + 1$, *then* ζ *is a* v^{th} *root of unity. If* $q = 4m + 3$, *then* ζ *is a* $2v^{th}$ *root of unity, but not a* v^{th} *root of unity.*

(iv) *If an equation of the type of* (11) *holds for all characters of* $\mathfrak{G}$, *and if* $n \equiv 0 \pmod{p}$, $v \not\equiv 0 \pmod{p}$ *for some prime* p, *then* $v = k$, $D = G$.

Proof. Equation (11) implies

$$\chi(D)^2 = \zeta n.$$

Now in the field of v^{th} roots of unity, only primefactors of v have multiple factors. Hence either $n = n_1^2$ or $n = n_1^2 q$ where $v \equiv 0 \pmod{q}$, $q = q_1 \cdots q_u$, and the $\chi(g)$ for $g \in \mathfrak{D}$ must generate the field of q^{th} roots of unity. By Theorem 1, v is odd in the latter case. The field Σ of v^{th} roots of unity contains $\sqrt{(-1)^{(q-1)/2}q}$. Hence $\chi(D)/(n_1\sqrt{(-1)^{(q-1)/2}q}) = \eta$ is a $2v^{\text{th}}$ root of unity. This yields $\zeta = (-1)^{(q-1)/2}\eta^2$. Moreover, (1) and $v \equiv 0 \pmod{q}$

imply $k \equiv \lambda \equiv 0 \pmod{q}$ and $n \equiv 0 \pmod{q^2}$. This proves (i), (ii), and (iii). If the conditions of (iv) hold, then $\chi(D) \equiv 0 \pmod{p}$ for all nonprincipal characters of $\mathfrak{G}$. By Lemma 1

$$D \equiv \mu G \pmod{p},$$

and since D has coefficients 0 and 1 only, it follows that $\mu \equiv 1 \pmod{p}$, $D = G$. This completes the proof of Theorem 5.

COROLLARY 5.1. *If an equation of type* (11) *holds for all characters for which* $\chi(g)$ *is a* v_1^{th} *root of unity for all* $g \in \mathfrak{D}$, *and if* $n = n_1^2 q^3$, $q > 1$, *then* $v_1 = q^k$, *and* q *is a prime.*

Proof. If $v_1 \equiv 0 \pmod{q_1}$, $v_1 \equiv 0 \pmod{q_2}$, $q_1 \neq q_2$, then there is a nonprincipal character for which all $\chi(g)$ are q_1^{th} roots of unity. Then $n = n_1^2$ or $n = n_1^2 q_1^3$. Similarly $n = n_1^2$ or $n = n_2^2 q_2^3$, so that we must have $n = n_1^2$.

COROLLARY 5.2. *If* t *is a* v_1 *multiplier and* $t^f \equiv -1 \pmod{v_1}$, *then all conclusions of Theorem* 5 *hold. Moreover, if* $n = n_1^2 q^3$, $q > 1$, *then* $v_1 = q^s$, q *is a prime of the form* $4m + 1$, *and the Jacobi symbol* $\left(\frac{t}{q}\right) = +1$. *If* $v^* = v_1$ *and* $n \equiv 0 \pmod{p}$, $v \not\equiv 0 \pmod{p}$ *for some prime* p, *then* $v = k$.

Proof. The hypothesis of Corollary 5.2 implies that of Theorem 5 and of Corollary 5.1. Moreover, ζ in equation (11) is a v^{th} root of unity, being a character. In the field Σ of q^{th} roots of unity the automorphism $\zeta \to \zeta^t$ (ζ a primitive q^{th} root of unity) takes $\sqrt{q}$ into $\sqrt{q}$ if $\left(\frac{t}{q}\right) = +1$ and $\sqrt{q}$ into $-\sqrt{q}$ if $\left(\frac{t}{q}\right) = -1$. Now let χ be a character such that $\chi(g)$ is a q^{th} root of unity for all g. Then

$$\chi(D) = \pm\eta n_1 \sqrt{q},$$

where η is a q^{th} root of unity, and if $\left(\frac{t}{q}\right) = -1$, we would get

$$\chi(D(t)) = \mp\eta^t n_1 \sqrt{q} = -\eta^{t-1}\chi(D) = \chi(g)\chi(D), \qquad \chi(g) = -\eta^{(t-1)},$$

which is impossible, since q is odd.

In particular, every multiplier is a v_1 multiplier for every v_1 which divides v, so that we have

COROLLARY 5.3. *Let* v^* *be the l.c.m. of the orders of the elements of* $\mathfrak{G}$. *If a multiplier* t *has even order with respect to* v^*, *then* n *is a square or* $n = n_1^2 q^3$. *If* $t^f \equiv -1 \pmod{v^*}$ *and* $n \equiv 0 \pmod{p}$, $v \not\equiv 0 \pmod{p}$ *for some prime* p, *then* $v = k$.

Proof. If t has even order with respect to v^*, then it has even order with respect to a prime divisor q_1 of v^*. Let $2f$ be this order; then $t^f \equiv -1 \pmod{q_1}$, so that the conditions of Corollary 5.2 are satisfied. The second part of the theorem follows from the fact that all characters are $v^{*\text{th}}$ roots of unity.

COROLLARY 5.4. *Let* $\mathfrak{D}$ *be a difference set for the elementary Abelian group of order* 2^m; *then* n *is an even power of* 2.

The integer 1 is always a multiplier. But $v^* = 2$ and $1 \equiv -1$ (2). The second part of Corollary 5.3 now implies that n is a power of 2, and Theorem 1 that n is a square.

One also sees that the condition $n \equiv 0 \pmod{p}$, $v \not\equiv 0 \pmod{p}$ is indeed necessary for the last conclusion of Theorem 5. P. K. Menon [6] has constructed difference sets with $v = 2^{2m}$, $n = 2^{2(m-1)}$.

3. Cyclic difference sets

We now consider the case that $\mathfrak{G}$ is cyclic. In this case we shall call $\mathfrak{D}$ a cyclic difference set. The elements of the group ring can be represented as polynomials mod $(x^v - 1)$.

We put

$$T(x) = 1 + x + \cdots + x^{v-1}, \qquad \theta(x) = \sum_{i=1}^{k} x^{a_i}, \tag{12}$$

where $a_1, \cdots, a_k$ is a difference set mod v.

We then have

$$\theta(x)\theta(x^{-1}) \equiv n + \lambda T(x) \pmod{(x^v - 1)}. \tag{13}$$

THEOREM 6. *If p is a prime, $p \mid n$, $p \mid v$, $v \equiv 0 \pmod{p^s v_1}$, $(v_1, p) = 1$, and $p^f \equiv -1 \pmod{v_1}$, and if $\theta(x) = \sum_{i=1}^{k} x^{a_i}$ where $a_1, \cdots, a_k$ is a difference set with parameters v, k, λ, then*

$$\theta(x) \equiv 0 \pmod{\{(x^{v_1} - 1)^{[(p^s+1)/2]}, p\}}. \tag{14}$$

(The double modulus means that all coefficients are to be reduced mod p and all polynomials mod $(x^{v_1} - 1)^{[(p^s+1)/2]}$.) Note that $v_1 = 1$ is not excluded.

Proof. From $p \mid n$, $p \mid v$, and equation (1) it follows that $k \equiv \lambda \equiv 0 \pmod{p}$. Thus

$$\theta(x^{-1})\theta(x) \equiv 0 \pmod{\{(x^{v_1} - 1)^{p^s}, p\}}.$$

Let $2f$ be the order of $p \bmod v_1$ ($2f = 0$ if $v_1 = 1$). Let $f(x)$ be an irreducible divisor of $x^{v_1} - 1$ in G.F.(p). We have $f(x) = \prod (x - \alpha_i)$, where $\alpha_i \in$ G.F.(p^{2f}). Since $p^f \equiv -1 \pmod{v_1}$, it follows that α_i and α_i^{-1} are conjugates. Hence if $\theta(x) \equiv 0 \pmod{\{f(x)^e, p\}}$, we also have

$$x^m \theta(x^{-1}) \equiv 0 \pmod{\{f(x)^e, p\}},$$

where m is the degree of $\theta(x)$, and vice versa. Hence the theorem follows.

THEOREM 7. *If $v \equiv n \equiv 0 \pmod{p}$, $v = p^s v_1$, $(v_1, p) = 1$, and $p^f \equiv -1 \pmod{v_1}$, and if $a_1, \cdots, a_k$ is a difference set* mod v, *then $k = v$.*

Note that $v_1 = 1$ is again not excluded.

By Theorem 6 we have

$$\theta(x) \equiv 0 \pmod{\{x^{v/p} - 1, p\}} \tag{15}$$

Let $0 \leqq a < v/p$. If $x^j \equiv x^a (x^{v/p} - 1)$, $0 \leqq j < v$, then j can take only one of the p values, a, $a + v/p$, $\cdots$, $a + (p-1)v/p$. Now if we replace in $\theta(x)$ all these terms by x^a, we must on account of (15) either get no term at

all or p terms since $\theta(x)$ has coefficients 1 or 0. Hence either x^a is not a summand of $\theta(x)$ or $x^a, x^{a+v/p}, \cdots, x^{a+(p-1)v/p}$ all are summands of $\theta(x)$. This means the residues $a_1, \cdots, a_k$ of the difference set D consist of k/p groups of residues

$$b_1, b_1 + v/p, \cdots, b_1 + (p-1)v/p,$$
$$b_2, b_2 + v/p, \cdots, b_2 + (p-1)v/p$$
$$\vdots$$
$$b_{k/p}, b_{k/p} + v/p, \cdots, b_{k/p} + (p-1)v/p.$$

But then the difference v/p arises $p \cdot (k/p) = k$ times. Hence $k = \lambda = v$.

The Abelian difference sets with $v = 2^{2m}$, $n = 2^{2(m-1)}$ of P. K. Menon [6] show that Theorem 7 does not hold for all Abelian difference sets. Of the list of 12 unsolved cases in [3], the set 171, 35, 7 is shown to be impossible for Abelian difference sets by Theorem 3. Of the other 11 cases, all except 120, 35, 10 and 100, 45, 20 are impossible for cyclic difference sets by Theorem 7. An Abelian solution exists for 64, 28, 12 and for 36, 15, 6 and may possibly exist in some of the other cases.

The set 100, 45, 20 was shown to be impossible by R. J. Turyn, so that 120, 35, 10 remains the only unsolved case in Hall's list. R. J. Turyn had also previously demonstrated the impossibility of 8 of the 9 cases which are disposed of by Theorem 7. The present paper thus adds two new cases to the list of solved cases and also provides a convenient proof for 8 others. R. J. Turyn's results are contained in two reports to the Sylvania Electronic System published in 1960 and in 1961.

References

1. S. Chowla and H. J. Ryser, *Combinatorial problems*, Canadian J. Math., vol. 2 (1950), pp. 93–99.
2. R. A. Fisher, *An examination of the different possible solutions of a problem in incomplete blocks*, Annals of Eugenics, vol. 10 (1940), pp. 52–75.
3. Marshall Hall, Jr., *A survey of difference sets*, Proc. Amer. Math. Soc., vol. 7 (1956), pp. 975–986.
4. H. B. Mann, *Some theorems on difference sets*, Canadian J. Math., vol. 4 (1952), pp. 222–226.
5. H. B. Mann and H. J. Ryser, *Systems of distinct representatives*, Amer. Math. Monthly, vol. 60 (1953), pp. 397–401.
6. P. K. Menon, *Difference sets in abelian groups*, Proc. Amer. Math. Soc., vol. 11 (1960), pp. 368–376.
7. M. P. Schützenberger, *A non-existence theorem for an infinite family of symmetrical block designs*, Annals of Eugenics, vol. 14 (1949), pp. 286–287.
8. B. L. van der Waerden, *Algebra*, 4te Aufl., Berlin, Springer-Verlag, 1955, 1959.

The Ohio State University
Columbus, Ohio