SOME RESULTS ON CYCLIC GROUP DIVISIBLE DESIGNS

by

SIDNEY JACOBS

A dissertation submitted to the
Graduate Faculty in Mathematics in
partial fulfillment of the requirements
for the degree of Doctor of Philosophy,
The City University of New York.

1971

This manuscript has been read and accepted for the University Committee in Mathematics in satisfaction of the dissertation requirement for the degree of Doctor of Philosophy.

June 30, 1971
date

Alan Hoffman
Professor Alan Hoffman
Chairman of Examining Committee

June 30, 1971
date

Edgar A. Feldman
Professor Edgar Feldman
Deputy Executive Officer

Professor Louis Auslander

Professor Richard Sacksteder

Professor Burton Randol

Supervisory Committee

ACKNOWLEDGMENTS

I acknowledge with pleasure my great indebtedness to Professor Alan J. Hoffman, my advisor, for stimulating and guiding my research, and for his enthusiasm and encouragement of my academic career. I am grateful to the City University of New York for providing a congenial research atmosphere, and for a Dissertation Year Fellowship in 1970-71, during which the research and writing of this dissertation took place. I thank Mrs. Sophie Gerber for her patience and expertise in typing the manuscript.

TABLE OF CONTENTS

CHAPTER 1

Introduction

There is a good deal of parallelism in the previous research in cyclic BIBDs on the one hand, and in cyclic GDs on the other hand. In the present chapter, we summarize our results, placing them in the context of those two lines of research. It will be apparent, that in our own research, we have tried to continue the parallelism.

A balanced incomplete block design (BIBD) with parameters v, b, k, r, λ is a system of v points, b blocks, and an incidence relation $\in$, such that each block is incident with k points, each point is incident with r blocks, and each pair of points occur together on λ blocks. Simple counting arguments show that

(1.1) $$bk = vr \text{ , and } r(k - 1) = \lambda(v - 1) \text{ .}$$

It is usually assumed that $2 \leq k \leq v - 2$; however in the present work, we allow $1 \leq k \leq v$, excluding only empty blocks, $k = 0$. A symmetric ($v = b$, and hence $k = r$) BIBD with $\lambda = 1$ is the same as a finite projective plane. A collineation of a BIBD is a permutation, φ, of the points of the BIBD together with a permutation, also denoted by φ, of the blocks of the BIBD, such that the incidence relation is preserved. A collineation of a symmetric BIBD is called cyclic if it is a cycle of length $v = b$ both on the points and on the blocks. A BIBD with a cyclic collineation is called a cyclic BIBD. In a cyclic BIBD, one can identify points with residues mod v, and one then finds that any block of the BIBD is a perfect difference set (PDS, or (v,k,λ)-PDS) viz. a set $L = \{p,\ldots,p_k\}$ of residues mod v, such that in the list of

$k(k-1)$ differences $p_i - p_j$, $i \neq j$, each non-zero residue mod v occurs λ times. Conversely, given a (v,k,λ)-PDS L one obtains a cyclic BIBD with the same parameters $v = b$, $k = r$, and λ, by taking all the residues mod v as points, and the sets $L, L+1, \ldots, L+v-1$ as blocks (the addition is point-wise mod v). Singer [20] proved that a finite desarguesian projective n-space, in which we take hyperplanes as blocks, is a cyclic BIBD.

Corresponding results were obtained for group divisible designs (GDs). A GD with parameters $v, b, k, r, m, n, \lambda_1, \lambda_2$ is a system of v points, b blocks of size k, each point occurring on r blocks. The set of points is partitioned into m groups, each of size n. If a pair of points are in the same group, they occur together on λ_1 blocks; if a pair of points are from different groups, they occur together on λ_2 blocks. Collineations and cyclicity are defined as in the case of BIBDs. Bose [1] showed that a finite desarguesian affine n-space, in which one affine point x_0 has been removed, is a cyclic GD whose blocks are the hyperplanes not containing x_0 and whose groups are the lines through x_0. (See Chapter 5, §4). Shrikhande [19] observed that, analogous to the perfect difference set above, a cyclic GD is equivalent to a "group divisible difference set" (GDDS), viz. a set $L = \{p_1, \ldots, p_k\}$ of residues mod v, such that in the list of $k(k-1)$ differences $p_i - p_j$, $i \neq j$, each difference d mod v which is $\equiv 0 \bmod m$ occurs λ_1 times, while each difference d mod v which is $\not\equiv 0 \bmod m$ occurs λ_2 times. (See Proposition 2.2).

Hall [9, Theorem 2.3] and Hoffman [13, Remark 2.3] prove the existence of a polarity for cyclic projective, respectively cyclic affine planes. Our Duality Theorem, Theorem 2.1 is the analogous result for cyclic GDs.

An integer μ is a multiplier of a cyclic BIBD if multiplication (mod v) by μ defines a collineation. In Hall [9], in which the concept of a multiplier was first introduced, it is shown that if p is prime dividing the order n of a finite cyclic projective plane (n = one less than the number of points on a line), then p is a multiplier. Hoffman [13], after observing that a cyclic affine plane is necessarily finite, proved that if p is a prime dividing the order n of a cyclic affine plane (n = the number of points on an affine line), then p is a multiplier. Hall's multiplier theorem was generalized in Hall and Ryser [12], in which it is shown that if p is a prime such that $p \nmid v$, $p|k - \lambda$, and $p > \lambda$ then p is a multiplier of any cyclic BIBD with parameters v, k, λ. In Chapter 3, we prove an analogous generalization of Hoffman's multiplier theorem. For this purpose we define the intersection numbers of a block L of a GD as $s_i(L) = |G_i \cap L|$, for $i = 0,1,\ldots,m-1$, where $G_0,G_1,\ldots,G_{m-1}$ are the groups of the GD, and if S is a set, $|S|$ is the number of points of the set. Noting that in a cyclic affine plane each block has one intersection number equal to zero, and all its other intersection numbers equal to one, we call a GD affine, if its intersection numbers assume exactly two distinct values, a and b. An affine GD is called special affine if one value, say a, is assume by exactly one intersection number of each block. Our multiplier theorem, Theorem 3.1, states that given a cyclic special affine GD with parameters v, k, m, n, λ_1, λ_2 and a prime p such that $p \nmid v$, $p|k - \lambda_1$, $p > \lambda_2$, and $p > k^2 - v\lambda_2$, then p is a multiplier of the GD. Another interesting result concerning intersection numbers is Theorem 2.2. If L is a block of a cyclic affine GD, we define the

sets $A = \{i | s_i(L) = a\}$ and $B = \{j | s_j(L) = b\}$. Then the theorem states that A and B, considered as sets of residues mod m, are perfect difference sets. Here we have to allow the possibility of a singleton PDS with parameters $v = m$, $k = 1$, $\lambda = 0$.

Several authors have improved the multiplier theorem for cyclic BIBDs by relaxing somewhat the assumptions on the multiplier or by considering difference sets in abelian groups (Bruck [5], Hall [10] and [11, p.138], Mann [14], McFarland [15], Newman [16], and Turyn [21] and [22]). It seems likely that Theorem 3.1, and some of our other results can be improved along the same lines.

An important non-existence theorem was proved for finite projective planes by Bruck and Ryser [6], and extended to symmetric BIBDs by Chowla and Ryser [7]. The technique of this theorem was used by Hall and Ryser [12] to prove a non-existence theorem for cyclic BIBDs, and by Shrikhande [19] to prove a non-existence theorem for cyclic GDs. In Chapter 4, we give an example showing how one can prove the non-existence of certain cyclic affine GDs by combining Theorems 2.2 and 3.1. Other non-existence results for cyclic GDs are given in Theorems 4.1 and 4.2.

Partially balanced incomplete block designs (PBIBDs), first introduced by Bose and Nair [3], are a wide class of designs that includes BIBDs and GDs. Some of the basic properties of cyclic PBIBDs are discussed in Chapter 2. Given any two PBIBDs, a product PBIBD can be defined (Vartak [23]). In Chapter 5 we note that if X_1 and X_2 are cyclic PBIBDs, and if $|X_1|$ and $|X_2|$ are relatively prime, then the product PBIBD is cyclic (Theorem 5.1); the rest of Chapter 5 is devoted to giving various examples of cyclic PBIBDs and cyclic GDs, using product PBIBDs and other constructions.

CHAPTER 2

Cyclic Designs and Intersection Numbers

Cyclic partially balanced incomplete block designs form a convenient general context for our study of cyclic group divisible designs.

A partially balanced incomplete block design (PBIBD) is a system of v points, b blocks, an incidence relation $\in$ between points and blocks and an association scheme for the points, with the following properties (see Bose and Shimamoto [4]).

The association scheme is a partition of the set of unordered pairs of points into t classes, called associate classes. If the unordered pair (x,y) is in the i-th associate class, the points x and y are called i-associate. If x,y are h-associate the number p_{ij}^h, of points which are i-associate to x and j-associate to y is required to be independent of the choice of (x,y) in the h-th associate class. It follows that p_{ij}^h is symmetric in i and j, and that the number n_h, of h-associates of a point x, is independent of the choice of x.

Each block is assumed to consist of k points, and two points x,y occur together on λ_i blocks, where the number λ_i depends only on the associate class i containing (x,y). It follows that if x is any point, the number r_x of blocks containing x satisfies the relation

$$\sum_{i=1}^{t} \lambda_i n_i = r_x(k - 1) \quad .$$

Thus $r = r_x$ is independent of the choice of x. (This is usually stated as an additional axiom for a PBIBD.)

We note that a BIBD (defined in Chapter 1) is just a PBIBD with one associate class, while a GD (defined below in this chapter) is a certain type of PBIBD with two associate classes.

A collineation of a PBIBD is a permutation, φ, of the points of the PBIBD, together with a permutation, also denoted by φ, of the blocks of the PBIBD, which

1) preserves the incidence relation, i.e., if p is any point and B is any block, then $p \in B$ implies $\varphi(p) \in \varphi(B)$, and

2) is compatible with the association scheme, i.e., if the points p and q are i-associate, then $\varphi(p)$ and $\varphi(q)$ are also i-associate.

A PBIBD is called symmetric if the number of points, v, is equal to the number of blocks, b. A collineation of a symmetric PBIBD is cyclic if, considered as a permutation of the points, it is a cycle of length v, and as a permutation of the blocks it is also a cycle of length $b = v$. A cyclic PBIBD is a symmetric PBIBD which has a cyclic collineation. The incidence matrix of a PBIBD is the $v \times b$ matrix $A = (a_{ij})$ where $a_{ij} = 1$ if the i-th point lies on the j-th block, and $a_{ij} = 0$ otherwise.

We make a few remarks to clarify the basic properties of cyclic PBIBDs.

Remark 2.1. If the incidence matrix of a symmetric PBIBD is non-singular, then

1) Distinct blocks are distinct as sets, and

2) If a collineation is cyclic on the points, it must also be cyclic on the blocks.

Proof: 1) says that two columns of the non-singular incidence matrix

cannot be identical, and 2) is a consequence of a theorem of Parker [17].

If φ is a cyclic collineation of a cyclic (symmetric) PBIBD, and p is an arbitrarily selected point of the PBIBD which we call the base point, then the points of the PBIBD are $p = \varphi^0(p), \varphi^1(p),\ldots,\varphi^{v-1}(p)$, so that we can identify the points of the PBIBD with residues mod v. We make this identification throughout the paper, and speak interchangeably of points and residues mod v. Thus the action of φ on points is $\varphi: i \to i + 1 \mod v$. If $S = \{p_1,\ldots,p_c\}$ is any set of points of this PBIBD, we denote by $S + j$ the set $\{p_1 + j,\ldots,p_c + j\}$ where addition is mod v. We can pick arbitrarily a block $B = B_0$ which we call the base block of the cyclic PBIBD, and write $B_i = B_0 + i$, where the subscript is taken mod v. Then the action of φ on blocks is $\varphi: B_i \to B_{i+1}$. Note that the points p,q occur together on exactly λ blocks $B,C,\ldots,D$ if and only if the points $\varphi(p) = p + 1$, $\varphi(q) = q + 1$, occur together precisely on the λ blocks $B + 1, C + 1,\ldots,D + 1$.

Remark 2.2. In a cyclic PBIBD with t associate classes, such that $\lambda_1,\ldots,\lambda_t$ are all different, the fact that the cycle φ is compatible with the association scheme follows from the other defining properties of a cyclic collineation.

Indeed points p,q will be i-associate if and only if they occur together on exactly λ_i blocks, if and only if (by the observation just made) $\varphi(p)$, $\varphi(q)$ occur together on λ_i blocks, if and only if $\varphi(p)$, $\varphi(q)$ are i-associate.

Remark 2.3. In a cyclic PBIBD, compatibility of the cycle with the association scheme can be arranged, in the presence of the other defining properties of a cyclic collineation, by merging certain of the associate classes.

Proof: Consider the graph whose vertices are all ordered pairs (p,q) of points of the PBIBD, with $p \neq q$. We join (p,q) and (r,s) by an edge if

1) the pairs belong to the same associate class, or

2) $p - q \equiv r - s \mod v$.

We define a new association scheme by putting (p,q) and (r,s) in the same new associate class if and only if the corresponding vertices lie in the same connected component of the graph. Clearly we have gained compatibility of the cycle with the new association scheme, and each new associate class is a union of one or more old associate classes.

It remains to verify that the new scheme is indeed an association scheme. We denote old associate classes by Roman letters i,j,k etc., and new associate classes by Greek letters α,β,γ etc. We have to show that for p,q α-associate, the number $p_{\beta\gamma}^{\alpha}$ of points r which are β-associate to p and γ-associate to q, is independent of the choice of the pair (p,q) within associate class α. Any other α-associate pair is reached by a series of moves in the graph along edges of type 1) or 2) given above.

Hence it is enough to check that a single move of either type does not change $p_{\beta\gamma}^{\alpha}$. Now associate class α is the union of certain old associate classes $i,i',\ldots$; class β is the union of old classes $j,j',\ldots$; and class γ is the union of old classes $k,k',k'',\ldots$. In a move of type 1) the constancy of $p_{\beta\gamma}^{\alpha}$ is just the constancy of

$$p_{jk}^{i} + p_{jk'}^{i} + p_{jk''}^{i} + \ldots + p_{j'k}^{i} + p_{j'k'}^{i} + p_{j'k''}^{i} + \ldots \quad .$$

In a move of type 2) the constancy of $p_{\beta\gamma}^{\alpha}$ is due to the fact that the

new scheme is indeed compatible with the cycle.

Remark 2.4. The existence of a cyclic PBIBD with block size k and t associate classes, and parameters $\lambda_1,\ldots,\lambda_t$ is equivalent to the existence of a "PBIBD difference set" (PBIBDDS) of k residues mod v, $B = \{p_1,\ldots,p_k\}$, with the property that if the residues d and 0 are i-associate (under the same association scheme), then there are exactly λ_i ordered pairs (p_α,p_β) such that $p_\alpha \in B$, $p_\beta \in B$, and $p_\alpha - p_\beta \equiv d \bmod v$.

Proof: Given a cyclic PBIBD, we can take for our PBIBDDS any block B of the PBIBD, because the unordered pair (p,q) occurs on λ blocks if and only if the difference $d \equiv p - q$ occurs λ times as the difference $p_\alpha - p_\beta$ of an ordered pair (p_α,p_β) of points of B. Conversely, given such a PBIBD difference set B, the sets B, $B + 1$, $B + 2,\ldots,B + v - 1$ as blocks and the set of all residues mod v as points form a cyclic PBIBD with parameters $\lambda_1,\ldots,\lambda_t$.

Further discussion and examples of cyclic PBIBDs will be found in Chapter 5.

We now specialize to the case of a group divisible design (GD) for the rest of Chapters 2, 3, and 4. Proofs for all statements concerning GDs that are not proved in this chapter can be found in Bose and Connor [2]. A GD is a PBIBD with two association classes, such that

(A0) $$p_{12}^1 = 0$$

(or alternately, $p_{12}^2 = 0$). An equivalent formulation, more suitable for our purposes, will now be given. The notation here introduced will be retained for the rest of the paper. A GD is a system of v points

and b blocks of size k, each point occuring on r blocks. The set of points is partitioned into m groups $G_0, G_1, \ldots, G_{m-1}$, each of size n. If a pair of points are in the same group (i.e., if the points are 1st-associate by the earlier definition), they occur together on λ_1 blocks; if a pair of points are from different groups (2nd-associate points), they occur together on λ_2 blocks. To prevent the GD from being a BIBD, we require $\lambda_1 \neq \lambda_2$, $m > 1$, and $n > 1$.

The following equations are satisfied by the parameters of any GD.

(A1) $\quad v = mn, \quad bk = vr$

(A2) $\quad r \geq \lambda_1, \quad r \geq \lambda_2$

(A3) $\quad r(k - 1) = (n - 1)\lambda_1 + n(m - 1)\lambda_2$

(A4) $\quad \det(AA^t) = rk(rk - v\lambda_2)^{m-1}(r - \lambda_1)^{m(n-1)}$,

where A is the incidence matrix of the GD.

(A5) $\quad rk \geq v\lambda_2$.

For any block B, we define its <u>intersection numbers</u> $s_i = s_i(B)$ as the size of the block's intersection with the i-th group,

$$s_i = |B \cap G_i|, \quad i = 0,1,\ldots,m-1 \quad .$$

<u>Proposition 2.1</u>. All of the intersection numbers of all of the blocks of a GD are the same if and only if $rk = v\lambda_2$.

The sufficiency of the condition is proved in Bose and Connor [2]. Both necessity and sufficiency are proved in Dembowski [8 , p.287] by a somewhat involved counting argument. We give here a simple proof of the necessity. Assume that all the intersection numbers of all of the blocks are equal to c, hence $cm = k$. We consider any fixed point p, and count in two ways the number of pairs (q,B) such that q is a point not in the same group as p, and p and q occur together on block B,

obtaining the relation $r(m-1)c = (m-1)n\lambda_2$. On multiplying by $m/(m-1)$, we get the desired result.

A GD is <u>symmetric</u> if $v = b$, and therefore by (A1), $k = r$. We now restrict our attention to the case of a cyclic (symmetric) GD . Making the identification of points with residues mod v, mentioned after Remark 2.1, we have the following proposition which is stated without proof by Shrikhande [19]. For completeness, we give the proof here.

<u>Proposition 2.2</u>. The existence of a cyclic GD is equivalent to the existence of a "<u>group divisible difference set</u>" (GDDS), viz. a k-set, B, of residues mod v with the properties

1) if $d \equiv 0 \bmod m$ (but $d \not\equiv 0 \bmod v$), there are exactly λ_1 ordered pairs (p_α, p_β) such that $p_\alpha \in B$, $p_\beta \in B$, and $p_\alpha - p_\beta \equiv d \bmod v$.

2) if $d \not\equiv 0 \bmod m$, there are exactly λ_2 ordered pairs (p_α, p_β) such that $p_\alpha \in B$, $p_\beta \in B$, and $p_\alpha - p_\beta \equiv d \bmod v$.

The groups of the GD are $G_0 = \{0, m, 2m, \ldots, (n-1)m\}$, and $G_i = G_0 + i$, $i = 1, 2, \ldots, m-1$.

<u>Proof</u>: Given a cyclic GD, using Remark 2.4, we take an arbitrary block B for our GDDS, and we have to determine the group G_0 of residues containing 0, i.e., we have to find out which residues mod v are 1st-associate to 0 . Now if 0 and x are 1st-associate, by cyclicity x and 2x are also 1st-associate, hence by the transitivity of 1st-associateness, (A0), 0 and 2x are 1st-associate. Continuing in this manner, we see that all multiples of x are 1st-associate to 0 . If we take y to be the least positive residue that is 1st-associate to 0, y must divide $v = mn$, and since $|G_0| = n$ we must have $y = m$.

Thus $G_0 = \{0,m,2m,\ldots,(n-1)m\}$ as stated, and by cyclicity, the other groups are $G_1, G_2,\ldots,G_{m-1}$ as defined above.

Conversely, given a GDDS B, then the sets $B_0 = B$, $B_1 = B_0 + 1,\ldots,B_{v-1} = B + v - 1$ as blocks, and the set of residues mod v as points, form a cyclic GD . (Remark: In applying this proposition, we shall always arrange the notation so that the base point, 0, lies in the group G_0 .)

An example of a GDDS is the set $B = \{0,1,3\}$ mod 6 . The difference $3 \equiv 3 - 0 \equiv 0 - 3 \bmod 6$ occurs twice; all other differences occur once. The parameters of the GDDS (and of the corresponding cyclic GD) are $v = b = 6$, $m = 3$, $n = 2$, $k = r = 3$, $\lambda_1 = 2$, and $\lambda_2 = 1$. The groups are $G_0 = \{0,3\}$, $G_1 = \{1,4\}$, and $G_2 = \{2,5\}$. The intersection numbers for block B are $s_0 = 2$, $s_1 = 1$, and $s_2 = 0$.

Clearly for a cyclic GD, the intersection numbers for any block will be a cyclic permutation of those for the chosen base block. When we speak of the intersection numbers s_i of a cyclic GD, we mean the $s_i(B_0)$ obtained from the chosen base block B_0 . The s_i also depend on the choice of the cyclic collineation φ and of the base point p_0 , since we require $p_0 \in G_0$.

We put the reader on notice to always read the subscripts of groups and intersection numbers mod m hereinafter, and to read points and the subscripts of blocks mod v .

A GD is called <u>regular</u>, following Bose and Connor [2], if

(A6) $\qquad r > \lambda_1$ and $rk > v\lambda_2$.

By (A4) a symmetric GD will be regular if and only if its incidence

matrix is invertible.

An incidence structure, which we may also loosely call a design, is a triple $(X,\mathcal{B},\in)$ (or X for short) where X is a set of points, $\mathcal{B}$ is a set of blocks, and the incidence relation $\in$ is a subset of $X \times \mathcal{B}$. An isomorphism of incidence structures X_1 and X_2 is a bijection τ between the points of X_1 and X_2, and a bijection τ between the blocks of X_1 and X_2 such that a point p and block B of X_1 are incident in X_1 if and only if $\tau(p)$ and $\tau(B)$ are incident in X_2. Obviously if X_1 and X_2 are isomorphic, and X_1 is a GD, a GD structure with the same parameters can be imposed on X_2. The dual of a design is the design whose points are the blocks of the given design, and whose blocks are the points of the given design. A point and block of the dual design are incident if and only if the corresponding block and point of the given design are incident. Clearly if the incidence matrix of the given design is A, the incidence matrix of the dual design is the transpose of A, A^t. We shall write $\bar{B}$ for the block B regarded as a point of the dual design, and $\bar{p}$ for the point p regarded as a block of the dual. Note that the dual of a cyclic GD, with cyclic collineation φ, is in any case a cyclic design of some sort, with respect to the dual cycle φ^d, where $\varphi^d: \bar{B}_i \to \bar{B}_{i+1}$ is the cycle on points of the dual, and $\varphi^d: \bar{j} \to \overline{j+1}$ is the cycle on blocks of the dual. The following Duality Theorem for cyclic GDs is analogous to theorems on the existence of a polarity of Hall [9, Theorem 2.3] and Hoffman [13, remark 2.3] for cyclic projective, respectively cyclic affine planes.

Theorem 2.1. A cyclic GD is isomorphic to its dual, which is therefore a cyclic GD with the same parameters. Moreover let s_i be the inter-

section numbers of the given GD with respect to its cyclic collineation φ, base point $p_0 = 0$, and base block B_0, and let t_i be the intersection numbers of the dual GD with respect to the dual cycle φ^d, the dual base point $\bar{B}_0$, and the dual base block $\bar{p}_0 = \bar{0}$. Then we have $t_i = s_{-i}$, $i = 0,1,\ldots,m-1$ (where the subscripts are read mod m).

Proof: The required isomorphism is given by $i \to \bar{B}_{-i}$, and $B_j \to \overline{-j}$. Indeed if $B_0 = \{d_1,\ldots,d_k\}$, the following are equivalent: $i \in B_j$; there exists d_α such that $i \equiv d_\alpha + j \bmod v$; there exists d_α such that $-j \equiv d_\alpha + (-i) \bmod v$; $-j \in B_{-i}$; $\bar{B}_{-i} \in \overline{-j}$. Denoting the parameters of the dual GD by barred quantities, since the given GD is symmetric, we have $\bar{v} = b = v$, $\bar{b} = v = b$, and $\bar{k} = r = k$. Thus the isomorphism is indeed with the dual of the given GD, and not with some subsystem in which some points, blocks, or incidence relations have been suppressed. This proves the first statement of the theorem. The groups of points of the dual GD are $G_0^d = \{\bar{B}_0,\bar{B}_m,\ldots,\bar{B}_{(n-1)m}\}$, $G_1^d = \{\bar{B}_1,\bar{B}_{1+m},\bar{B}_{1+2m},\ldots,\bar{B}_{1+(n-1)m}\},\ldots$ $G_{m-1}^d = \{\bar{B}_{m-1},\bar{B}_{2m-1},\ldots,\bar{B}_{v-1}\}$. The isomorphism maps G_{-i} onto G_i^d and B_0 to $\bar{0}$. This gives immediately $t_i = |G_i^d \cap \bar{0}| = |G_{-i} \cap B_0| = s_{-i}$.

Lemma 2.1. The intersection numbers s_i of a cyclic GD satisfy the relations

$$(B0) \qquad \sum_{i=0}^{m-1} s_i^2 = k + (n-1)\lambda_1 = k^2 - n(m-1)\lambda_2$$

$$(Bj) \qquad \sum_{i=0}^{m-1} s_i(s_{i+j}) = n\lambda_2 , \quad j = 1,\ldots,m-1 .$$

Proof: The left-hand side of (B0) counts the number of ways of selecting an ordered pair of points (x,y) from a block B, such that x and y are in the same group. This is equal to the middle member in which are

tallied the k pairs (x,x), $x \in B$, plus λ_1 ways of obtaining from B each of the differences $m, 2m, \ldots, (n-1)m$. The right-hand side of (B0) is a consequence of equation (A3), when $r = k$. The left-hand side of equation (Bj) counts the number of ways of selecting an ordered pair (x,y) such that $x \in B$, $y \in B$, and $x \in G_i$ implies $y \in G_{i+j}$. This is equal to the right-hand side, which counts the λ_2 ways of obtaining from B each of the differences $j, j+m, j+2m, \ldots, j+(n-1)m$. (Alternately, one can prove the lemma by reducing equation (E1) mod $x^m - 1$, and equating coefficients.)

The following theorem can be used to show the non-existence of certain GDs (see Chapter 4). The definition of a PDS is given in Chapter 1.

Theorem 2.2. Suppose that the intersection numbers s_i of a cyclic GD assume exactly two distinct values, a and b. Then the sets $A = \{i | s_i = a\}$ and $B = \{j | s_j = b\}$, considered as sets of residues mod m, are perfect difference sets (PDSs). A and B are both non-empty, but we allow the possibility that A or B is a singleton set, i.e., a PDS with parameters $v = m$, $k = 1$, $\lambda = 0$.

Proof: If λ_A differences mod m from the set A are equal to d, and λ_B differences mod m from B are equal to d, equation (Bd) reads

$$\lambda_A a^2 + \lambda_B b^2 + (m - \lambda_A - \lambda_B)ab = n\lambda_2 .$$

Now if the theorem is false, there is another difference d', whose corresponding λ'_A, λ'_B are different from λ_A, λ_B. Subtracting the resulting equation (Bd'),

$$\lambda'_A a^2 + \lambda'_B b^2 + (m - \lambda'_A - \lambda'_B)ab = n\lambda_2 ,$$

from the first equation, and writing $\epsilon_A = \lambda_A - \lambda'_A$, $\epsilon_B = \lambda_B - \lambda'_B$, we get

$$\epsilon_A a^2 + \epsilon_B b^2 - (\epsilon_A + \epsilon_B)ab = 0 .$$

Now if $\epsilon_A = \epsilon_B \neq 0$, the above quadratic form would give $(a - b)^2 = 0$, $a = b$, contradicting the hypothesis of the theorem. Thus if the theorem is false, we must have $\epsilon_A \neq \epsilon_B$.

We now make a computation in the ring $Z[x,x^{-1}]$ reduced mod $x^m - 1$, where Z is the ring of rational integers. This ring can also be conveniently regarded as the group ring ZH , where H is the cyclic group of order m , generated by x . The important point to bear in mind when computing in this ring is that the exponent of x should be read mod m . Now for $i = 1,2,\ldots,m - 1$ we set

$$\lambda_A^i = |\{(u,v) \,|\, u \in A,\ v \in A, \text{ and } u - v \equiv i \bmod m\}|$$

$$\lambda_B^i = |\{(u,v) \,|\, u \in B,\ v \in B, \text{ and } u - v \equiv i \bmod m\}| .$$

Putting $T(x) = 1 + x + x^2 + \ldots + x^{m-1}$,

$$\varphi_A(x) = \sum_{i \in A} x^i , \text{ and}$$

$$\varphi_B(x) = \sum_{i \in B} x^i = T(x) - \varphi_A(x) ,$$

we have

$$\varphi_A(x)\varphi_A(x^{-1}) \equiv |A| + \sum_{i=1}^{m-1} \lambda_A^i x^i \bmod x^m - 1 \text{ and}$$

$$(*) \qquad \varphi_B(x)\varphi_B(x^{-1}) \equiv |B| + \sum_{i=1}^{m-1} \lambda_B^i x^i \bmod x^m - 1 .$$

On the other hand,

$$(**) \qquad \varphi_B(x)\varphi_B(x^{-1}) \equiv (T(x) - \varphi_A(x))(T(x) - \varphi_A(x^{-1}))$$
$$\equiv (m - 2|A|)T(x) + |A| + \sum_{i=1}^{m-1} \lambda_A^i x^i \bmod x^m - 1 .$$

On comparing coefficients of the right-hand sides of (*) and (**), we find $\lambda_B^i = \lambda_A^i + \text{const}$, for $i = 1,2,\ldots,m-1$ where the constant is $h = m - 2|A|$. Hence

$$\epsilon_B = \lambda_B^d - \lambda_B^{d'} = \lambda_A^d - \lambda_A^{d'} = \epsilon_A ,$$

a contradiction.

Corollary. Given a cyclic GD with $\lambda_1 = 0$ and $k^2 - v\lambda_2 > 0$, then the sets $A = \{i | s_i = 0\}$ and $B = \{j | s_j \neq 0\}$, considered as sets of residues mod m, are (non-empty) perfect difference sets.

Proof: By Proposition 2.1, $k^2 - v\lambda_2 > 0$ implies there are at least two distinct intersection numbers, but since $\lambda_1 = 0$, 0 and 1 are the only possible intersection numbers. Hence Theorem 2.2 gives the result.

The corollary can also be easily proved without using Theorem 2.1 (compare Theorem 5.4).

CHAPTER 3

A Multiplier Theorem

Given a cyclic PBIBD whose blocks are distinct as sets, and whose v points we regard as the set of residues mod v, then the integer μ is called a multiplier of the PBIBD if multiplication by μ defines a collineation. Thus the effect of μ on a block L is given by point-wise multiplication of the set L.

In this chapter we prove a multiplier theorem for certain cyclic GDs, which is a generalization of a multiplier theorem of Hoffman [13] for cyclic affine planes. A cyclic affine plane has for its points, the points of a projective plane, with the points of the line L_∞ at infinity deleted, and with one additional (affine) point X deleted. It has for its lines, the lines of the projective plane, with the line L_∞ and all lines through X deleted. The incidence relation is the restriction of the incidence relation of the projective plane, and the system is assumed to have a cyclic collineation. The order, t of the plane is the number of points on a line. Bose [1] proved that a finite desarguesian affine plane, with any affine point X deleted, is a cyclic affine plane.

Hoffman's multiplier theorem states that if p is a prime dividing t, then a cyclic affine plane of order t has p as a multiplier. The starting point for the present generalization is the fact that if we take the lines through the deleted point X as groups, then the cyclic affine plane is seen to be a cyclic (symmetric) regular GD with $v = b = t^2 - 1$, $r = k = t$, $m = t + 1$, $n = t - 1$, $\lambda_1 = 0$, $\lambda_2 = 1$, and with intersection numbers $0,1,1,\ldots,1$. (The terms and notation just used are defined in Chapter 2.) We define an affine GD as a GD in

which the intersection numbers assume exactly two distinct values, which we will denote throughout as a and b. A <u>special affine GD</u> is an affine GD in which one of the values, say a, is assumed by exactly one intersection number of each block. (If a GD is cyclic, or more generally if it has a group of collineations which is transitive on the blocks, the multiplicity of each value will be the same for each block.) We shall prove a multiplier theorem for cyclic special affine GDs. First we list a few useful facts.

By (A3) we have

(C1) In any GD, $\lambda_1 < \lambda_2$ if and only if $k^2 - v\lambda_2 < k - \lambda_1$.

We define for any positive integer e,

$$T_e(x) = 1 + x + x^2 + \ldots + x^{e-1}$$

In proving the multiplier theorem our computations take place in the rings $Z[x,x^{-1}] / (x^e - 1)$ and $Z[x,x^{-1}] / T_e(x)$, where Z is the ring of rational integers. In addition to the facts stated at the end of Chapter 2 about the first of these rings, the following facts will be used constantly.

(C2) $(x - 1)\, T_e(x) = x^e - 1$, therefore $x^e \equiv 1 \bmod T_e(x)$.

(C3) $T_n(x^m)\, T_m(x) = T_{mn}(x)$.

(C4) If $rs = e$, and $f(x)$ is any polynomial, then $f(x)\, T_r(x^s) \equiv f_1(x)\, T_r(x^s) \bmod x^e - 1$, where $f_1(x)$ is a polynomial of degree less than s.

(C5) The mapping defined by $x \to x^{-1}$ is an automorphism of the algebra $Z[x,x^{-1}] / (x^e - 1)$.

Theorem 3.1. Given a cyclic special affine GD, and a prime p satisfying the following conditions:

(D1) p does not divide mn ,

(D2) p divides $k - \lambda_1$,

(D3) $p > \lambda_2$,

(D4) $p > k^2 - v\lambda_2$,

then p is a multiplier.

Concerning the seemingly restrictive condition (D4), we note that if we are given that $\lambda_2 > \lambda_1$ and that $k - \lambda_1$ is a prime p , then by (C1), (D4) is automatically satisfied.

Proof of Theorem 3.1: We may assume that $k > \lambda_1$. This has the sole effect of excluding the trivial case in which a block is a group, or its complement, by Theorem 2 of Bose and Connor [2]. In this case (D1) by itself implies the theorem.

We note that since the intersection numbers assume two distinct values, $0 < k^2 - v\lambda_2$ by (A5) and Proposition 2.1. From (D4) and (D2), $k^2 - v\lambda_2 < k - \lambda_1$. Hence $\lambda_1 < \lambda_2$ by (C1), and the GD is regular by (A4). Thus we can strengthen (D3) and (D4) as follows:

(D3′) $p > \lambda_2 > \lambda_1$

(D4′) $p > k^2 - v\lambda_2 > 0$.

According to Proposition 2.2, if L is any block of the GD , $L = \{d_1, d_2, \ldots, d_k\}$ is a GD difference set (GDDS) of residues mod v. We define

$$\theta(x) = x^{d_1} + \ldots + x^{d_k} .$$

Then the properties of the GDDS are precisely equivalent to the equation

(E1) $\theta(x)\theta(x^{-1}) \equiv k - \lambda_1 + \lambda_2 T_v(x) + (\lambda_1 - \lambda_2) T_n(x^m) \bmod (x^v - 1)$.

We must prove that the set $pL = \{pd_1, pd_2, \ldots, pd_k\}$ is also a block of the GD, in short that $pL = L + t$ for some integer t . If this is shown for any one block L, it will also be true for any other block $L + i$, since we will have $p(L + i) = pL + pi = L + t + pi$. This will make multiplication by p a collineation as claimed. However, by (D1), pL is in any case a GDDS with the same parameters as the GDDS L . Hence

(E2) $\theta(x^p)\theta(x^{-p}) \equiv k - \lambda_1 + \lambda_2 T_v(x) + (\lambda_1 - \lambda_2) T_n(x^m) \bmod (x^v - 1)$.

Using (D2) and the fact that $T_n(x^m)$ divides $T_v(x)$ and $x^v - 1$, (E1) becomes

(E3) $\theta(x)\,\theta(x^{-1}) \equiv 0 \bmod (p, T_n(x^m))$.

Since $\theta(x^p)\,\theta(x^{-1}) \equiv \theta(x)^{p-1}\,\theta(x)\,\theta(x^{-1}) \bmod (p, x^v - 1)$, we have $\theta(x^p)\,\theta(x^{-1}) \equiv 0 \bmod (p, T_n(x^m))$ from (E3). In other words,

(E4) $\theta(x^p)\,\theta(x^{-1}) \equiv pf(x) + g(x)\,T_n(x^m) \bmod x^v - 1$.

Here we can take $g(x) = g_0 + g_1 x + \ldots + g_{m-1} x^{m-1}$ by (C4). Also we choose $0 \le g_i < p$ for $i = 0,1,\ldots,m-1$, absorbing the difference into the term $pf(x)$. Putting $f(x) = f_0 + f_1 x + \ldots + f_{v-1} x^{v-1}$, all the f_j's will be non-negative: if any were strictly negative, the right-hand side would have a strictly negative coefficient (viewed as an element of the group algebra ZG, where G is the cyclic group of order

v generated by x), whereas all the coefficients of the left-hand side are non-negative. Since $x^m \equiv 1 \bmod T_m(x)$, we get from (E4) and (C3),

(E5) $\theta(x^p)\,\theta(x^{-1}) \equiv ng(x) \bmod (p, T_m(x))$.

Referring to the notation of Theorem 2.2, we have $\theta(x) \equiv a\varphi_A(x) + b\varphi_B(x) \bmod x^m - 1$, if we use L as our base block. Since $\varphi_B(x) = T_m(x) - \varphi_A(x)$,

(E6) $\theta(x) \equiv (a - b)\,\varphi_A(x) \bmod T_m(x)$.

By (E1) and (D2), and using $x^m \equiv 1 \bmod T_m(x)$, $T_v(x) \equiv 0 \bmod T_m(x)$, we have

(E7) $\theta(x)\,\theta(x^{-1}) \equiv n(\lambda_1 - \lambda_2) \bmod (p, T_m(x))$.

From (E6), (E7), and $\theta(x^p)\theta(x^{-1}) \equiv \theta(x)^{p-1}\theta(x)\theta(x^{-1}) \bmod (p, T_m(x))$,

(E8) $\theta(x^p)\theta(x^{-1}) \equiv (a - b)^{p-1}\,\varphi_A(x)^{p-1}\,n(\lambda_1 - \lambda_2) \bmod (p, T_m(x))$.

We claim that $a - b \not\equiv 0 \bmod p$, hence $(a - b)^{p-1} \equiv 1 \bmod p$. This follows from the relation of Theorem 4.1, valid for any cyclic affine GD, that $k^2 - v\lambda_2 = (a - b)^2(|A| - \lambda_A)$, together with (D4′). (We do not really need the full strength of even (D4) for this however. We only need that $k^2 - v\lambda_2 < k - \lambda_1$, which gave us (D3′). By (A3) we can rewrite the left-hand side of the last equation as $k - \lambda_1 + n(\lambda_1 - \lambda_2)$, and then on reducing mod p, (D1), (D2), and (D3′) give the desired conclusion.)

We now invoke the assumption that the GD is special affine, so that one of the two index sets, say A_∞ is a singleton. Hence

$\varphi_A(x) = x^j$, i.e., $|L \cap G_i| = a$ only for $i = j$. If $j \neq 0$, we change our choice of base block from L to $L - j$, whence $s_0 = s_0(L - j) = |L - j \cap G_0| = a$, and $\varphi_A(x) = 1$. Thus we can rewrite (E8) as

$$\theta(x^p)\,\theta(x^{-1}) \equiv n(\lambda_1 - \lambda_2) \bmod (p, T_m(x)) \quad \text{(E9)}$$

Combining this with (E5), we have $ng(x) \equiv n(\lambda_1 - \lambda_2) \bmod (p, T_m(x))$, and since, by (D1), n is invertible mod p ,

$$g(x) \equiv \lambda_1 - \lambda_2 \bmod (p, T_m(x)) \quad \text{(E10)}$$

or

$$g(x) \equiv \lambda_1 - \lambda_2 + ph(x) + wT_m(x) \bmod x^m - 1 \quad \text{(E11)}$$

Here w can be taken as an integer, since multiplication of $T_m(x)$ by a polynomial $w(x)$ is the same, mod $x^m - 1$, as multiplication by the sum of its coefficients. Further, due to the term $ph(x)$, we can take $0 \leq w < p$. Now since $0 \leq g_i < p$, we get

$$\begin{aligned} g_1 &= g_2 = \cdots = g_{m-1} = w \ , \quad \text{and} \\ g_0 &= \lambda_1 - \lambda_2 + w + \epsilon p \quad . \end{aligned} \quad \text{(E12)}$$

Writing f = sum of the coefficients of $f(x)$, and setting $x = 1$ in (E1) and in (E4), we have

$$k^2 = k - \lambda_1 + mn\lambda_2 + n(\lambda_1 - \lambda_2) \ ,$$

$$k^2 = pf + n(mw + \lambda_1 - \lambda_2 + \epsilon p) \quad . \quad \text{(E13)}$$

Equating the two right-hand sides, reducing mod p , and cancelling n which is $\not\equiv 0 \bmod p$, we get

$$m\lambda_2 + \lambda_1 - \lambda_2 \equiv mw + \lambda_1 - \lambda_2 \mod p ,$$

$$\lambda_2 \equiv w \mod p ,$$

since $m \not\equiv 0 \mod p$. Hence

(E14) $$\lambda_2 = w ,$$

since $0 \le \lambda_2 , w < p$. Going back to (E12) we have $g_0 = \lambda_1 + \epsilon p$, whence

(E15) $$\epsilon = 0 .$$

Thus we can now rewrite (E12) as

(E16) $$g_1 = g_2 = \cdots = g_{m-1} = \lambda_2 , \quad \text{and}$$
$$g_0 = \lambda_1$$

Putting together (E13-15), $k^2 = pf + n(m - 1)\lambda_2 + n\lambda_1$, and recalling (A3), we have $k^2 = pf + k^2 - k + \lambda_1$, or

(E17) $$pf = k - \lambda_1 .$$

Using (E16) , equation (E4) becomes

$$\theta(x^p)\theta(x^{-1}) \equiv pf(x) + T_n(x^m)[\lambda_2 T_m(x) + \lambda_1 - \lambda_2] \mod x^v - 1 , \text{ or}$$

(E18) $$\theta(x^p)\theta(x^{-1}) \equiv pf(x) + \lambda_2 T_v(x) + (\lambda_1 - \lambda_2)T_n(x^m) \mod x^v - 1 ,$$

(E18′) $$\theta(x^p)\theta(x^{-1}) \equiv p\bar{f}(x) + n\lambda_2 T_m(x) + n(\lambda_1 - \lambda_2) \mod x^m - 1 ,$$

where $\bar{f}(x) = e_0 + e_1 x + \cdots + e_{m-1} x^{m-1}$ and $e_i = c_i + c_{i+m} + \cdots + c_{i+(n-1)m}$ for $i = 0,1,\ldots,m-1$. Applying the automorphism defined by $x \to x^{-1}$ to (E18) and(E18′),

(E19) $\theta(x^{-p})\theta(x) \equiv pf(x^{-1}) + \lambda_2 T_v(x) + (\lambda_1 - \lambda_2)T_n(x^m) \bmod x^v - 1$,

(E19′) $\theta(x^{-p})\theta(x) \equiv p\bar{f}(x^{-1}) + n\lambda_2 T_m(x) + n(\lambda_1 - \lambda_2) \bmod x^m - 1$.

Also, (E1) and (E2) yield

(E1′) $\theta(x)\theta(x^{-1}) \equiv k - \lambda_1 + n\lambda_2 T_m(x) + n(\lambda_1 - \lambda_2) \bmod x^m - 1$,

(E2′) $\theta(x^p)\theta(x^{-p}) \equiv k - \lambda_1 + n\lambda_2 T_m(x) + n(\lambda_1 - \lambda_2) \bmod x^m - 1$.

On the left-hand sides, (E1′) × (E2′) ≡ (E18′) × (E19′) $\bmod x^m - 1$.
Equating the right-hand sides,

$$(k - \lambda_1)^2 + 2n(k - \lambda_1)(\lambda_1 - \lambda_2) + n^2(\lambda_1 - \lambda_2)^2 + T_m(x)n\lambda_2[2(k - \lambda_1) + 2n(\lambda_1 - \lambda_2) + mn\lambda_2]$$
$$\equiv p^2\bar{f}(x)\bar{f}(x^{-1}) + n^2(\lambda_1 - \lambda_2)^2 + pn(\lambda_1 - \lambda_2)(\bar{f}(x) + \bar{f}(x^{-1})) + T_m(x)n\lambda_2[2pf + 2n(\lambda_1 - \lambda_2) + mn\lambda_2] \bmod x^m - 1 .$$

By (E17) the two expressions in brackets are equal. Equating the constant terms on both sides,

$$(k - \lambda_1)^2 + 2n(k - \lambda_1)(\lambda_1 - \lambda_2) = p^2 \sum_{i=0}^{m-1} e_i^2 + 2pn(\lambda_1 - \lambda_2)\, e_0 .$$

We complete the square by adding $n^2(\lambda_1 - \lambda_2)^2$ back to both sides:

(E20) $$[k - \lambda_1 + n(\lambda_1 - \lambda_2)]^2 = p^2 \sum_{i=1}^{m-1} e_i^2 + [pe_0 + n(\lambda_1 - \lambda_2)]^2 .$$

By (A3), the quantity inside the left-hand bracket is $k^2 - mn\lambda_2$, so that by (D4) the left-hand side is less than p^2 . Therefore the term

$p^2 \sum_{i=1}^{m-1} e^2$ on the right-hand side must be zero, $e_1 = e_2 = \cdots = e_{m-1} = 0$.

This leaves $e_0 = f$, since $f = \sum_{i=0}^{m-1} e_i$. Thus $f(x) = c_0 + c_m x^m +$

$c_{2m}x^{2m} + \cdots + c_{(n-1)m}x^{(n-1)m}$, whence

(E21) $\quad T_n(x^m)f(x) \equiv T_n(x^m)f \equiv T_n(x^m)f(x^{-1}) \mod x^v - 1$.

Since on the left-hand sides, (E1) × (E2) ≡ (E18) × (E19) mod $x^v - 1$, we equate the right-hand sides and use (E21), obtaining

$$(k - \lambda_1)^2 + T_v(x)[\lambda_2^2 mn + 2\lambda_2(k - \lambda_1) + 2\lambda_2(\lambda_1 - \lambda_2)n]$$
$$+ T_n(x^m)[(\lambda_1 - \lambda_2)^2 n + 2(k - \lambda_1)(\lambda_1 - \lambda_2)]$$
$$\equiv p^2 f(x)f(x^{-1}) + T_v(x)[\lambda_2^2 mn + 2pf\lambda_2 + 2\lambda_2(\lambda_1 - \lambda_2)n]$$
$$+ T_n(x^m)[(\lambda_1 - \lambda_2)^2 n + 2pf(\lambda_1 - \lambda_2)] \mod x^x - 1 .$$

By (E17) this is just $(k - \lambda_1)^2 \equiv p^2 f(x)f(x^{-1}) \mod x^v - 1$. Since $f(x)$ has non-negative coefficients, it must therefore consist of a single term, $f(x) = f \cdot x^{tm}$, whence $pf(x) = (k - \lambda_1)x^{tm}$ by (E17). Thus (E18) reads

(E22) $\quad \theta(x^p)\theta(x^{-1}) \equiv (k - \lambda_1)x^{tm} + \lambda_2 T_v(x) + (\lambda_1 - \lambda_2)T_n(x^m) \mod x^v - 1$.

This says that exactly $k = (k - \lambda_1) + \lambda_2 + (\lambda_1 - \lambda_2)$ of the differences $pd_\alpha - d_\beta$ have the same value $tm \bmod v$. If $pd_\alpha - d_\beta \equiv pd_{\alpha'} - d_{\beta'} \bmod v$, then by (D1), $\alpha = \alpha'$ if and only if $\beta = \beta'$. Thus $\{pd_1,\ldots,pd_k\}$ is a rearrangement of $\{d_1 + tm,\ldots,d_k + tm\}$, or $pL = L + tm$, and p is a multiplier.

CHAPTER 4

Non-existence Theorems for Cyclic GDs

We present some theorems here which can be used to show the non-existence of cyclic GDs with certain parameters. Several of these results closely parallel well-known results for perfect difference sets. Thus Propositions 4.1 and 4.2 and their proofs are identical with results for PDSs of H. Mann and J. Jans respectively (see Hall [11 , p. 140]), while Theorem 4.2 is analogous to Hall-Ryser [12 , Theorem 3.2].

For cyclic affine GDs, the multiplier theorem of Chapter 3, when combined with the PDS theorem of Chapter 2, is a powerful tool for proving non-existence. We give a detailed example of the use of these two theorems to prove the impossibility of a certain cyclic affine GD. Theorem 4.1 gives another non-existence criterion for cyclic affine GDs.

Proposition 4.1. If p is any multiplier of a cyclic PBIBD whose incidence matrix is non-singular, then p has a fixed block.

Proof: p has a fixed point, namely the residue 0 , therefore by Parker's Theorem [17], p has a fixed line.

Proposition 4.2. Let v be the number of points, and k the number of points per block, of a cyclic PBIBD. If $(k,v) = 1$, then there is a block which is fixed by all multipliers.

Proof: If we choose some block $B = B_0$ as base block, the blocks of the PBIBD are $B_i = \{d_1 + i,\ldots,d_k + i\}$, for $i = 0,1,\ldots,v - 1$. The sum of the residues of block B_i is $\sigma(B_i) = d_1 + \ldots + d_k + ki$. Since $(k,v) = 1$, the map $B_i \rightarrow \sigma(B_i)$ gives a one to one correspondence between the set of all blocks and the set of all residues mod v . Hence it is

clear that the block $\sigma^{-1}(0)$ is fixed by all multipliers.

We now give an example of how one can show the non-existence of cyclic affine GDs with certain parameters, by using the perfect difference set theorem of Chapter 2, the multiplier theorem of Chapter 3, and the existence of a fixed line for any multiplier. The non-existence of the given example cannot be obtained by any other theorems known to the author. We consider a symmetric GD with the parameters $v = b = 16$, $m = 4$, $n = 4$, $k = r = 7$, $\lambda_1 = 2$, $\lambda_2 = 3$. We shall show that this design cannot be cyclic affine. If it is cyclic affine, the index sets A and B of Theorem 2.2 are perfect difference sets mod m. There is no symmetric BIBD with $m = 4$ points and block-size 2, a fortiori there is no PDS mod 4 with block-size 2. Therefore the design is special affine, and we can use Theorem 3.1. Hence 5 is a multiplier. The incidence matrix of the design is non-singular, since $k^2 - v\lambda_2$ and $k - \lambda_1$ are greater than 0 (see (A4)). Thus by Proposition 4.1 there is a fixed block L for the multiplier. Clearly L must be a union of orbits of the multiplier. The orbits are

$$C_1 = (1, 5, 9, 13), \qquad C_2 = (3, 7, 11, 15),$$

$$C_3 = (2, 10), \qquad C_4 = (6, 14), \text{ and } (0), (4), (8), (12).$$

C_1 and C_2 are also groups, and since $\lambda_1 = 2$, they cannot be contained in L. But then to achieve $|L| = k = 7$, we have to include both C_3 and C_4 in L, which is impossible since $C_3 \cup C_4$ is a group.

Continuing to use the notation of Theorem 2.2 for an arbitrary cyclic affine GD, we have from (1.1) of Chapter 1,

(4.1) $$(m - 1)\lambda_A = |A|(|A| - 1) ,$$

and since A and B are complementary PDSs,

(4.2) $$|A| + |B| = m ,$$

(4.3) $$|B| - \lambda_B = |A| - \lambda_A .$$

Combining (4.1) and (4.2) we find

(4.4) $$\frac{|A|\cdot|B|}{m - 1} = |A| - \lambda_A .$$

If we subtract equation (B1) from equation (B0) of Chapter 2, we obtain for the case of a cyclic affine GD

(4.5) $$k^2 - v\lambda_2 = |A|a^2 + |B|b^2 - \lambda_A a^2 - \lambda_B b^2 - (m - \lambda_A - \lambda_B)\, ab .$$

Using (4.2-4.4) and recalling that for a special affine GD , $|A| = 1$ and $|B| = m - 1$ or vice versa, (4.5) yields

Theorem 4.1. For any cyclic affine GD , we have

$$k^2 - v\lambda_2 = (a - b)^2(|A| - \lambda_A) = (a - b)^2 \frac{|A|\cdot|B|}{m - 1} .$$

For any cyclic special affine GD , $k^2 - v\lambda_2 = (a - b)^2$, the square of an integer.

Theorem 4.2. Given a cyclic GD which is either regular or has $(k,v) = 1$, and let t be both a multiplier and a primitive root mod q , where q is a prime dividing v , then

1) if q divides m , then $k^2 - v\lambda_2$ is a square.

2) if q does not divide m, then $k - \lambda_1$ is a square.

Proof: Let $L = \{d_1,\ldots,d_k\}$ be a fixed block, which exists by either Proposition 4.1 or 4.2, and let $\theta(x) = x^{d_1} + \ldots + x^{d_k}$. Then $\theta(x) \equiv \theta(x^t) \equiv \theta(x^{t^2}) \equiv \ldots \bmod x^v - 1$ where the exponents $1, t, t^2, \ldots$ run through all the non-zero residues mod q (since t is a primitive root). Thus if ϵ is a primitive q^{th} root of unity (over the rationals), $\theta(\epsilon) = \theta(\epsilon^2) = \ldots = \theta(\epsilon^{q-1}) = \theta(\epsilon^{-1})$ (since $q|v$), therefore $\theta(\epsilon)$ is a rational integer h. Substituting ϵ for x in (E1),

$$(4.6) \qquad h^2 = \theta(\epsilon)\,\theta(\epsilon^{-1}) = k - \lambda_1 + \lambda_2 T_v(\epsilon) + (\lambda_1 - \lambda_2) T_n(\epsilon^m) .$$

The term $\lambda_2 T_v(\epsilon)$ disappears since $T_q(x)$ divides $T_v(x)$. If q divides m, the last term of (4.6) is $(\lambda_1 - \lambda_2)n$, and the result follows from (A3). If q does not divide m, $\epsilon^m \neq 1$ is a q^{th} root of unity, hence satisfies $T_q(x) = 0$, but q divides n, therefore $T_q(x)$ divides $T_n(x)$, so the last term of (4.6) disappears, giving the result.

Note: If $q = 2$, t is irrelevant, and the theorem is true for an arbitrary symmetric regular GD by (A4). (This is part of Theorem 9 of Bose and Connor [2]).

CHAPTER 5

Some Families of Cyclic Designs

In this chapter we collect some constructions and families of cyclic PBIBDs and GDs. No claim is made that these account for more than a tiny fraction of the existing multitude of such designs.

§1. Product PBIBDs

Suppose we have two disjoint sets X_1, X_2 with v_i points, association schemes G_i consisting of t_i associate classes, i = 1,2,and parameters p^i_{jk}, q^i_{jk}, respectively. We want to define a product association scheme on $X_1 \times X_2$, and, in case X_1 and X_2 are PBIBDs, a product PBIBD. (This was done by Vartak [23], by taking the Kronecker product of the two incidence matrices. However, to develop the few simple facts that we need, it is better to avoid using matrices.) To this end we first modify the definition of associate by "including the diagonal": we say that any point is 0-associate to itself. The properties of an association scheme and of a PBIBD, stated in Chapter 2, are still valid under this modification; in fact, we have $n_0 = 1$, $p^0_{jk} = \delta_{jk} n_j$, and $p^i_{0,k} = p^i_{k,0} = \delta_{ik} n_0$, and $\lambda_0 = r$.

We shall call two points (a,a') and (b,b') of $X_1 \times X_2$, <u>(i,j)-associate</u> with respect to the <u>product association scheme</u> $G_1 \circ G_2$ if a and b are i-associate with respect to G_1, and a' and b' are j-associate with respect to G_2. This clearly defines an association scheme on $X_1 \times X_2$, with $t_1t_2 + t_1 + t_2$ associate classes (not including the diagonal) and with

$$p^{(i,\ell)}_{(j,m)(k,n)} = p^i_{jk}\, q^\ell_{mn} \quad ,$$

where $0 \le i, j, k \le t_1$, and $0 \le \ell, m, n \le t_2$. Now assume that X_1 and X_2 are PBIBDs with b_i blocks of size k_i, replication numbers r_i, for $i = 1,2$, and parameters λ_j, $j = 0,1,\ldots,t_1$; λ'_j, $j = 0,1,\ldots,t_2$ respectively. Then we can make $X_1 \times X_2$ into a PBIBD by taking as blocks all the sets $B \times C$ where B is a block of X_1 and C is a block of X_2. (If X_1 or X_2 have distinct blocks which are identical as sets, so will $X_1 \times X_2$.) We call this the <u>product PBIBD</u>. It has v_1v_2 points, b_1b_2 blocks of size k_1k_2, and replication number r_1r_2. Any pair of points which are (i,j)-associate occur together on $\lambda_i\lambda'_j$ blocks of the product PBIBD, where $0 \le i \le t_1$, and $0 \le j \le t_2$.

We further assume that both PBIBDs are cyclic, and that $(v_1, v_2) = 1$. We make the identification of the points of X_i with residues mod v_i, for $i = 1,2$, as discussed after Remark 2.1 of Chapter 2. Let e be the unique solution mod v_1v_2 of the congruences $x \equiv 1 \bmod v_1$ and $x \equiv 0 \bmod v_2$, and let f be the unique solution mod v_1v_2 of $x \equiv 0 \bmod v_1$ and $x \equiv 1 \bmod v_2$. Then we can identify the point (a,b) of the product PBIBD uniquely with the residue $ea + fb \bmod v_1v_2$. Moreover, if B_i is chosen as base block of X_i, $i = 1,2$, then an arbitrary block $(B_1 + i) \times (B_2 + j)$ of the product is equal (as a set) to $(B_1 \times B_2) + s$, where $s = ei + fj$ is the unique solution mod v_1v_2 of $x \equiv i \bmod v_1$ and $x \equiv j \bmod v_2$. Thus the product PBIBD is seen to be cyclic with base block $B_1 \times B_2$. We summarize the discussion in a theorem.

<u>Theorem 5.1</u>: Let X_1, X_2 be two PBIBDs with association schemes G_i of t_i associate classes, with v_i points, b_i blocks of size k_i, replication numbers r_i, for $i = 1,2$, respectively, and parameters λ_j, $j = 0,\ldots,t_1$ for X_1 and λ'_j, $j = 0,\ldots,t_2$ for X_2. Then a

product PBIBD $X_1 \times X_2$ can be defined with a product association scheme $G_1 \circ G_2$ of $t_1t_2 + t_1 + t_2$ associate classes (not including the diagonal), and with $v = v_1v_2$, $b = b_1b_2$, $k = k_1k_2$, $r = r_1r_2$, and $\lambda_{(i,j)} = \lambda_i\lambda'_j$ for $i = 0,\ldots,t_1$, $j = 0,1,\ldots,t_2$. If $(v_1,v_2) = 1$, and X_1 and X_2 are cyclic PBIBDs, the product PBIBD is also cyclic.

We shall have immediate occasion to use the fact that the two PBIBDs used to form a product can have block-sizes equal to any value except 0 . We give 3 examples in which the product construction is used to obtain GDs. Let $L = \{d_1,\ldots,d_k\}$ be a (v,k,λ)-PDS with $v - 1 > k > 1$, and let v' be prime to v . (PDSs and BIBDs were defined in Chapter 1.)

Example 5.1a: If a is any integer we define a set L^* of residues mod vv' as follows. We let $L^* = \{d_1^*,\ldots,d_k^*\}$, where $d_i^* \equiv d_i \bmod v$ and $d_i^* \equiv a \bmod v'$, for $i = 1,\ldots,k$. Then L^* is a GDDS, or base block for a regular GD, with parameters $v^* = b^* = vv'$, $k^* = r^* = k$, $m^* = v'$, $n^* = v$, $\lambda_1^* = \lambda$, and $\lambda_2^* = 0$.

Example 5.1b: We define a set M^* of residues mod vv' as follows. We let $M^* = \{d_i + xv \mid i = 1,\ldots,k;\ x = 1,\ldots,v'\}$. Then M^* is a GDDS, or base block for a non-regular GD, with parameters $v^* = b^* = vv'$, $k^* = r^* = kv'$, $m^* = v$, $n^* = v'$, $\lambda_1^* = kv'$, $\lambda_2^* = \lambda v'$.

Example 5.1c: If we let L be the set of non-zero squares mod p , where p is a prime congruent to 3 mod 4 , it is well-known that L is a $(p, \frac{p-1}{2}, \frac{p-3}{4})$-PDS. If M^* is obtained as in 5.1b from this L , then $M^* \cup \{0\}$ is a GDDS, or base block for a regular GD , with parameters $v^* = b^* = pv'$, $k^* = r^* = \frac{p-1}{2}v' + 1$, $m^* = p$, $n^* = v'$, $\lambda_1^* = \frac{p-1}{2}v'$, $\lambda_2^* = \frac{p-3}{4}v' + 1$.

Proof of the properties of the examples: Let X_1 be the cyclic BIBD generated by the given PDS, so that in the notation of Theorem 5.1, $\lambda_0 = k$, and $\lambda_1 = \lambda$. In 5.1a, we take X_2 to be the BIBD whose points are the residues mod v' and whose blocks are all the singleton subsets of this set of points. This is a cyclic BIBD with $\lambda_0' = 1$, and $\lambda_1' = 0$. The product PBIBD, $X_1 \times X_2$, has $v^* = b^* = vv'$, and $k^* = r^* = \lambda_0\lambda_0' = k$. It has $\lambda_{(0,1)} = \lambda_0\lambda_1' = 0$, where two points are (0,1)-associate if they are congruent mod v, and incongruent mod v'; $\lambda_{(1,0)} = \lambda_1\lambda_0' = \lambda$, where two points are (1,0)-associate if they are incongruent mod v, but congruent mod v'; $\lambda_{(1,1)} = \lambda_1\lambda_1' = 0$, where two points are (1,1)-associate if they are incongruent mod v and incongruent mod v'. Since $\lambda_{(0,1)} = \lambda_{(1,1)} = 0$, we see that the product PBIBD is a GD with $\lambda_2^* = 0$, $\lambda_1^* = \lambda_{(1,0)} = \lambda$, where two points are in the same group if they are congruent mod v', i.e., $m^* = v'$, $n^* = v$. In 5.1b, we take X_2 to be the BIBD whose points are the residues mod v' and whose blocks are the entire set of points, counted v' times as a block. This is a cyclic BIBD with $\lambda_0' = v' = \lambda_1'$. Using the product PBIBD, $X_1 \times X_2$, the verification of the properties of 5.1b is similar to that of 5.1a, and will be omitted. In 5.1c, we recall the well-known fact that if $L = \{d_1,\ldots,d_k\}$ is the PDS of non-zero squares mod p where p is a prime congruent to 3 mod 4, then $L \cup \{0\}$ is also a PDS, with k and λ increased by 1. Indeed the resulting new differences, $d_1 - 0,\ldots,d_k - 0$, $0 - d_1,\ldots,0 - d_k$ are precisely all the non-zero residues mod p, because -1 is not a square mod p. In the case at hand it is equally clear that the new differences of $M^* \cup \{0\}$ in 5.1c are precisely all the residues mod pv' that are incongruent to 0 mod p.

Thus in passing from M^* to $M^* \cup \{0\}$, λ_1^* remains unchanged, while λ_2^* and k^* increase by 1. While $k^{*2} - v^*\lambda_2^*$ remains greater than 0, $k^* - \lambda_1^*$ increases from 0 to 1 so that the GD of 5.1c is regular.

We note that the design 5.1a is special affine, 5.1b is affine, and 5.1c is not affine. This product construction does not yield GDs for less 'extreme' choices of X_2.

§2. Divisor Difference Sets

Let X be the set of residues mod v. We can define a *divisor association scheme* for X as follows: Let $m_1 = 1$, m_2, m_3,... be all the divisors of v except v itself. We call the residues x, y mod v i-associate if $(x - y, v) = m_i$. The straightforward verification that this is an association scheme is left to the reader. A cyclic PBIBD with respect to this association scheme is called a *Divisor PBIBD*; a block of a Divisor PBIBD is called a Divisor Difference Set (DDS). (See Remark 2.4 of Chapter 2.) In view of Proposition 2.2, a GDDS is a DDS; this is not, of course, an efficient description of a GDDS since $v = mn$ will have divisors other than m.

It is convenient for the rest of the present section to change our notation once more; we index the associate classes of a Divisor PBIBD by the divisors themselves, and we say that a point is v-associate to itself. We give some examples of DDSs.

Example 5.2a: The following block, consisting of the ten powers of 2 mod 33, and the single residue 11, is a DDS.

$$B = \{2, 4, 8, 16, 32, 31, 29, 25, 17, 1, 11\} \bmod 33 \ .$$

Here $v = b = 33$, $k = r = 11$, $\lambda_1 = 3$, $\lambda_3 = 5$, and $\lambda_{11} = 0$.

Example 5.2b: If p and q are primes, one of which is $\equiv 1 \bmod 4$ and the other $\equiv 3 \bmod 4$, let L be the set consisting of all residues mod pq which are either

1) non-zero squares both mod p and mod q , or

2) non-zero non-squares both mod p and mod q .

Then L is a DDS . Here $v = pq$, $k = (p-1)(q-1)/2$, $\lambda_p = (p-1)(q-3)/4$, $\lambda_q = (q-1)(p-3)/4$, and $\lambda_1 = \frac{1}{4}[(p-2)(q-2) + 1]$.

The proof of the statements is a portion of an argument in Hall [11 ,p. 164-165], to which we refer the reader for details. If v is a composite number, for brevity we call t a primitive root of v if it is a primitive root of each prime divisor of v . We note that if the greatest common divisor of $p - 1$, $q - 1$ is 2 , the above set L can be described as the set of all powers of a primitive root of pq . Thus we have, for instance

Example 5.2c: If q is a prime $\equiv 1 \bmod 4$, and t is a primitive root mod $3q$, then the powers of t mod $3q$ form a DDS with

$$v = 3q \ , \ k = q - 1 \ , \ \lambda_3 = \frac{q-3}{2} \ , \ \lambda_q = 0 \ , \text{ and } \ \lambda_1 = \frac{q-1}{4} \ .$$

The greatest common divisor condition is also met if p,q are twin primes. In that case we get a much better result. (See Theorem 5.3).

Theorem 5.2: Let $(v_1,v_2) = 1$, and let the sets X_1 and X_2 of sizes v_1 and v_2 respectively be given the divisor association scheme. Then

the product association scheme on $X_1 \times X_2$ is the divisor association scheme. If X_1 and X_2 are Divisor PBIBDs, then $X_1 \times X_2$ is a Divisor PBIBD, and $\lambda^*_{m_1 m_2} = \lambda_{m_1} \lambda'_{m_2}$, where $m_i | v_i$, $i = 1,2$.

Proof: To prove the 1st assertion we observe that if two points u, w of $X_1 \times X_2$ are (m_1,m_2)-associate with respect to the product association scheme, then they are $m_1 m_2$-associate with respect to the divisor association scheme of the product. Indeed using e and f as defined in §2, let

$$u \equiv ea_1 + fa_2 \bmod v_1 v_2 \quad \text{and} \quad w \equiv eb_1 + fb_2 \bmod v_1 v_2 .$$

Then

$$(u - w, v_1 v_2) = (u - w, v_1)(u - w, v_2) = (a_1 - b_1, v_1)(a_2 - b_2, v_2)$$

$$= m_1 m_2$$

as desired. Thus the two association schemes are the same, and the 2nd assertion follows:

$$\lambda^*_{m_1 m_2} = \lambda_{(m_1,m_2)} = \lambda_{m_1} \lambda'_{m_2} .$$

§3. Twin Prime GDs

Theorem 5.3: If p and q are twin primes, and t is a primitive root mod pq, then the set of powers of t mod pq is a GDDS, which is a base block of a cyclic regular special affine GD, with parameters

$$v = pq , \quad k = \frac{p^2-1}{2} , \quad m = q , \quad n = p ,$$

$$\lambda_1 = (p+1)(p-3)/4 , \quad \lambda_2 = (p-1)^2/4 ,$$

$$k - \lambda_1 = (p+1)^2/4 , \quad k^2 - v\lambda_2 = (p-1)^2/4 , \quad \text{and}$$

intersection numbers $s_0 = 0$, $s_i = \frac{p-1}{2}$, for $i = 1,\ldots,q-1$.

This is proved by just plugging the information $q = p + 2$ into Example 5.2b, and noting that $\lambda_1 = \lambda_p$ in DDS notation, which means this common value becomes λ_2 in GD notation, while λ_q becomes λ_1 . The values of the s_i are easily checked, using the original definition of the base block L given in 5.2b.

§4. Cyclic Affine GDs From Affine Geometries

Let $d \geq 2$, and let $\mathcal{G}$ be a finite desarguesian affine d-space, so that $\mathcal{G}$ can be coordinatized with coordinates from a finite field of order q , where q is a prime power. If we delete one point x_0 from $\mathcal{G}$, the resulting system $\mathcal{G}'$ was shown to have a cyclic collineation by Bose [1]. We may view $\mathcal{G}'$ as a cyclic affine GD, whose blocks are the hyperplanes not containing x_0 and whose groups are the lines through x_0 . (q must be greater than 2.) The GD parameters are

$$v = b = q^d - 1 \ , \ k = r = q^{d-1} \ , \ m = q^{d-1} + \ldots + q + 1 \ ,$$

$$n = q - 1, \ \lambda_1 = 0 \ , \qquad \lambda_2 = q^{d-2} \ .$$

q^{d-1} of the s_i's are equal to 1 , and the remaining $q^{d-2} + \ldots + q + 1$ s_i's are equal to 0 .

§5. A Reduction Theorem For Cyclic GDs

Theorem 5.4: Let $L = \{p_1,\ldots,p_k\}$ be a GDDS with parameters v, k, m, n, λ_1, λ_2, where $\lambda_1 = 0$, and let f be any divisor of n , $ef = n$. Then the set L^* consisting of the same points as L , but reduced mod mf , is a GDDS with parameters $v^* = mf$, $k^* = k$, $m^* = m$, $n^* = f$,

$\lambda_1^* = 0$, $\lambda_2^* = \lambda_2 e$.

Proof: $\lambda_1 = 0$ if and only if the p_i's are all distinct mod m , if and only if $\lambda_1^* = 0$; a fortiori the p_i's are distinct mod mf , i.e., $k^* = k$. If $d \not\equiv 0 \bmod m$, each of the differences $d, d + mf, \ldots, d + (e - 1)mf \bmod v$ occurs in λ_2 ways as $p_i - p_j \bmod v$. Hence the difference $d \bmod mf$ occurs in $\lambda_2 e$ ways as $p_i - p_j \bmod mf$. This completes the proof. We note that by taking $f = 1$, we obtain the corollary to Theorem 2.2.

§6. An Unsolved Construction Problem

In view of Theorem 2.2, one would like to be able to reverse the procedure of §5, and construct, for some infinite class of (v,k,λ)-PDSs and appropriate divisors w of λ , a cyclic affine GD with parameters $v^* = vw$, $k^* = k$, $m^* = v$, $n^* = w$, $\lambda_1^* = 0$, $\lambda_2^* = \lambda/w$, and intersection numbers 0 and 1 . In fact, the cyclic affine GDs of §4 do arise this way: the PDS is the complement of a hyperplane in the projective (d-1)-space at infinity (which is cyclic by Singer's well-known theorem [20]), and $w = q - 1$. We have not succeeded in finding a non-geometric way of carrying out this construction; we conclude with one lonely example of the construction with non-geometric parameters. The example is peculiar, in that for most (larger) w one will obviously have to add, mod vw , suitable multiples of v to the points of the (v,k,λ)-PDS. The PDS here is the complement of a line of the 7-point projective plane, and the q of §4 is 2, but instead of using $w = q - 1 = 1$ and getting nothing, we use $w = 2$.

Example 5.3: The (7,4,2)-PDS $L = \{0,1,4,6\} \bmod 7$ is, taken mod 14, a

GDDS with parameters $v = 14$, $k = 4$, $m = 7$, $n = 2$, $\lambda_1 = 0$, $\lambda_2 = 1$, and intersection numbers 0 and 1 .

BIBLIOGRAPHY

[1] Bose, R.C., An Affine Analogue of Singer's Theorem. Journal of the Indian Mathematical Society, vol. 6 (1942), 1-15.

[2] _____, and W.S. Connor, Combinatorial Properties of Group Divisible Incomplete Block Designs. Annals of Mathematical Statistics, vol. 23 (1952), 367-383.

[3] _____ and K.R. Nair, Partially Balanced Incomplete Block Designs. Sankya, vol. 4 (1939), 337-372.

[4] _____ and T. Shimamoto, Classification and Analysis of Partially Balanced Incomplete Block Designs with Two Associate Classes. Journal American Statistical Assoc., vol. 47 (1952), 151-184.

[5] Bruck, R.H., Difference Sets in a Finite Group. Transactions of the A. M. S., vol. 78 (1955), 464-481.

[6] _____ and H.J. Ryser, The Non-existence of Certain Finite Projective Planes. Canadian Journal of Math., vol. 1 (1949), 88-93.

[7] Chowla, S. and H.J. Ryser, Combinatorial Problems. Canadian Journal of Math., vol. 2 (1950), 93-99.

[8] Dembowski, P., Finite Geometries, Springer-Verlag, New York, 1968.

[9] Hall, Marshall, Cyclic Projective Planes. Duke Math. J., vol. 14 (1947), 1079-1090.

[10] _____, A Survey of Difference Sets. Proceedings of the A. M. S., vol. 7 (1956), 975-986.

[11] _____, Combinatorial Theory. Blaisdell Publishing Co., Waltham, Mass., 1967.

[12] _____ and H.J. Ryser, Cyclic Incidence Matrices. Canadian Journal of Math., vol. 3 (1951), 495-502.

[13] Hoffman, A.J., Cyclic Affine Planes. Canadian Journal of Math., vol. 4 (1952), 295-301.

[14] Mann, H.B., Addition Theorems. Interscience, New York, 1965.

[15] McFarland, R.L., On Multipliers of Abelian Difference Sets. Ph.D. Thesis, Ohio State University, 1970.

[16] Newman, M., Multipliers of Difference Sets. Canadian Journal of Math., vol. 15 (1963), 121-124.

[17] Parker, E.T., On Collineations of Symmetric Designs. Proceedings of A. M. S., vol. 8 (1957), 350-351.

[18] Ryser, H.J., A Note on a Combinatorial Problem. Proceedings of the A. M. S., vol. 1 (1950), 422-424.

[19] Shrikhande, S.S., Cyclic Solutions of Symmetric Group Divisible Designs. Calcutta Statistical Assoc. Bulletin, vol. 5 (1953), 36-39.

[20] Singer, J., A Theorem in Finite Projective Geometry and Some Applications to Number Theory. Transactions of A. M. S., vol. 43 (1938), 377-385.

[21] Turyn, R.J., The Multiplier Theorem for Difference Sets. Canadian Journal of Math., vol. 16 (1964), 386-388.

[22] _____, Character Sums and Difference Sets. Pacific Journal of Math., vol. 15 (1965), 319-346.

[23] Vartak, M.N., On an Application of Kronecker Product of Matrices to Statistical Designs. Annals of Math. Statistics, vol. 26 (1955), 420-438.

AUTOBIOGRAPHY

Sidney Jacobs was born in 1935 in Baltimore, Maryland. After his public school education in Baltimore, he attended the University of Chicago, receiving a B.S. in 1958, and M.S. in 1960. During the period 1958-1970 he had a variety of assignments as a computer programmer, the most recent being at the National Bureau of Economic Research, New York, 1968-1970. He was enrolled at the Graduate Center of The City University of New York during 1969-1971. For the academic year 1970-1971, he was Adjunct Lecturer in remedial algebra in the open enrollment program at the City College of New York.