SYMMETRIC DESIGNS, DIFFERENCE SETS, AND AUTOCORRELATIONS OF FINITE BINARY SEQUENCES

Thesis by

Wayne Jeremy Broughton

In Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy

Pasadena, California

1995

(Submitted May 23, 1995)

To my parents

ACKNOWLEDGEMENTS

I would like to express my gratitude and indebtedness to my advisor, Professor Richard M. Wilson, for his teaching, guidance, and constant encouragement. I also thank Prof. David Wales, Prof. W.A.J. Luxemburg, and Dr. William Doran for agreeing to be on my examining Committee.

I am very grateful to Prof. Michel Kervaire and Prof. Shalom Eliahou, some of whose work was the starting point for much of this thesis, for their hospitality during my stay at the University of Geneva. I thank Prof. Richard J. Turyn, Prof. Alexander Pott, Prof. James A. Davis and Dr. Jonathan Jedwab for helpful suggestions.

I am also grateful to all of my instructors during my years of education at the University of British Columbia and the California Institute of Technology. I thank Dr. John Blanchard, Dr. Hunter Snevily, Dr. Farshid Hajir, and many others for useful discussions. Finally, I would like to acknowledge the support of my fellow graduate students at the California Institute of Technology, and the tremendous help of the administrative and secretarial staff of the Mathematics Department.

ABSTRACT

Symmetric designs with parameters (v, k, λ) are very regular structures useful in the design of experiments, and (v, k, λ)-difference sets are a common means of constructing them, as well as being interesting subsets of groups in their own right. We investigate (v, k, λ)-symmetric designs and (v, k, λ)-difference sets, especially those satisfying $v = 4n + 1$, where $n = k - \lambda$. These must have parameters of the form $(t^2 + (t + 1)^2, t^2, t(t - 1)/2)$ for $t \geq 1$. Such difference sets exist for $t = 1, 2$. Generalizing work of M. Kervaire and S. Eliahou, we conjecture that abelian difference sets with these parameters do not exist for $t \geq 3$, and we prove this for large families of values of t (or n). In particular, we eliminate all values of t except for a set of density 0. The theory of biquadratic reciprocity is especially useful here, to determine whether or not certain primes are biquadratic, and hence semi-primitive, modulo the factors of v.

Cyclic difference sets also correspond to (± 1)-sequences of length v with constant periodic autocorrelation. Such sequences are of interest in communications theory, especially if they also have small aperiodic correlations. We find and prove bounds on the aperiodic correlations of a binary sequence that has constant periodic correlations. As an example, such sequences corresponding to cyclic difference sets satisfying $v = 4n$ have aperiodic autocorrelations bounded absolutely by $(3/2)n$, with a similar bound in the case of cyclic Hadamard difference sets (those satisfying $v = 4n - 1$).

Finally, we present an alternative construction of a class of symmetric designs due to A.E. Brouwer which includes the $v = 4n + 1$ designs as a special case.

TABLE OF CONTENTS

1. INTRODUCTION AND PRELIMINARIES

1.1. Block Designs

Special examples of combinatorial *block designs* date back to the first half of the 19th century. More general classes were studied in connection with finite geometry, notably by J. Steiner [Ste]. In this century, other classes of block designs became important to statisticians in the design of experiments (whence the name), and since then design theory has grown to be one of the major branches of modern combinatorics. Designs have been investigated in connection with, and found applications in, finite geometry, coding theory, graph theory, the theory of Hadamard matrices, digital communications and radar signal design, cryptography, as well as the design of experiments. A few major references to the theory are [BJL], [HP], and [L], and some examples of applications and interactions with other fields are in [AK], [CvL], [SP], [Go], and [St]. An introduction to design theory with nice proofs of the elementary results below can be found in [vLW].

An important class of designs, particularly in the design of experiments, are the *balanced incomplete block designs* ([Y]), defined to be "incidence structures" consisting of the following:

(a) a set $\mathcal{P}$ of size v whose elements are called *points*;

(b) a set $\mathcal{B}$ of size b whose elements are called *blocks*;

(c) an *incidence* relation $\mathcal{I} \subset \mathcal{P} \times \mathcal{B}$ such that:

  (i) every block is incident with exactly k points;

  (ii) every point is incident with exactly r blocks; and

  (iii) any two distinct points in $\mathcal{P}$ are simultaneously incident with exactly λ blocks;

where the parameters k, r, and λ are constant. It turns out that the existence of the constant r in (c) (ii) follows from the other conditions, and the values of the parameters b and r are given by $r = \lambda(v-1)/(k-1)$ and $b = rv/k$, so such a design is often called a (v, k, λ)-BIBD. It is normally assumed that $k < v$ (this is

the "incompleteness" part), to avoid degeneracy. Notice that each block determines a subset of the points, namely those with which it is incident. A design where distinct blocks are incident with distinct subsets of the points is called *simple*, and in a simple design we often identify the blocks with these subsets.

An example of a $(13,4,1)$-BIBD on the point set

$$\mathcal{P} = \{0,1,2,3,4,5,6,7,8,9,10,11,12\}$$

consists of blocks identified with the following subsets:

$$\begin{array}{cccc} \{0,1,3,9\} & \{4,5,7,0\} & \{7,8,10,3\} & \{10,11,0,6\} \\ \{1,2,4,10\} & \{5,6,8,1\} & \{8,9,11,4\} & \{11,12,1,7\} \\ \{2,3,5,11\} & \{6,7,9,2\} & \{9,10,12,5\} & \{12,0,2,8\} \\ \{3,4,6,12\}. & & & \end{array} \tag{1.1}$$

Notice that indeed any two distinct points $0 \leq i,j \leq 12$ occur together in exactly one of these blocks.

The *complement* of a given BIBD is the incidence structure with the complementary incidence relation $(\mathcal{P} \times \mathcal{B}) \setminus \mathcal{I}$, or, equivalently, the structure whose blocks are identified with the complements of the subsets (i.e., blocks) of the original BIBD. It can be shown that the complement is also a BIBD. So, for example, the complement of the $(13,4,1)$-BIBD above is a $(13,9,6)$-BIBD.

1.2. Symmetric Designs

Sir R.A. Fisher proved in [F] that for a (v,k,λ)-BIBD with $k < v$, one must have $b \geq v$. This motivates interest in the extremal case, where $b = v$. It turns out that in this case we must also have $r = k$, and

(iv) any two distinct blocks are simultaneously incident with exactly λ points.

In other words, the *dual* structure (with point set $\mathcal{B}$, block set $\mathcal{P}$, and the same incidence relation) is also a (v,k,λ)-BIBD. So a BIBD with $b = v\,(> k)$ is usually called a *symmetric design*. Observe that (1.1) is in fact a $(13,4,1)$-symmetric design, since there are 13 blocks (and each point is contained in exactly 4 blocks, and the

intersection of any two distinct blocks consists of exactly 1 point). Symmetric designs thus have a lot of regular structure. A symmetric design is necessarily simple.

The *order* of a (v, k, λ)-symmetric design is defined to be $n = k - \lambda$, and is a very useful parameter for classifying symmetric designs, often more so than k or λ. Notice that for any two distinct points of the design, n counts the number of blocks containing the first, but not the second, of the two points. Likewise, for any two distinct blocks, n is the size of the intersection of the first block with the complement of the second.

The most important question about symmetric designs remains only partially solved: given v, k, λ, does there exist a symmetric design with these parameters? Of course, an answer of "yes" usually involves exhibiting an actual construction of such a design.

The simplest necessary condition on the parameters of a symmetric design is easily obtained by counting the pairs of incident points and blocks in two different ways, and is sometimes called the *basic parametric equation*:

$$\lambda(v-1) = k(k-1). \tag{1.2}$$

This can also be easily expressed in a form involving $n = k - \lambda$:

$$\lambda v + n = k^2. \tag{1.3}$$

The only other known general condition required of the parameters of a symmetric design is the *Bruck-Ryser-Chowla theorem* (see [vLW] for a proof):

BRC Theorem. *If a (v, k, λ)-symmetric design of order n exists, then*

(i) *if v is even, then n is a square (actually due to Schützenberger);*

(ii) *if v is odd, then there exist integers x, y, z, not all 0, such that*

$$nx^2 + (-1)^{(v-1)/2}\lambda y^2 = z^2.$$

The complement of a symmetric (v, k, λ)-design is a $(v,\ v-k,\ v-2n-\lambda)$-symmetric design, since $\mu = v-2n-\lambda = v-2k+\lambda$ is the number of blocks containing *neither* of a given pair of distinct points. Notice that the order of the complementary design is the same as that of the original, since $(v-k)-(v-2k+\lambda) = k-\lambda$. So when considering the question of existence, we normally assume that $k \leq v/2$, and it is convenient to classify symmetric designs in terms of their order.

If $n = 1$, then (1.2) implies that the symmetric design must have parameters $(v, 1, 0)$ (or the complementary $(v, v-1, v-2)$), and such a symmetric design is called *trivial*.

We can use the basic parametric equation to derive nice bounds on v in terms of n for non-trivial symmetric designs (see [BJL]). Let $\mu = v - 2n - \lambda$ as above, then from (1.3) we easily derive that

$$\lambda + \mu = v - 2n$$

$$\lambda\mu = n(n-1).$$

Now assume that $n > 1$, so that in particular $\mu, \lambda \geq 1$ (from equation (1.2) and its complementary equivalent). Thus

$$\begin{aligned} & (\mu-1)(\lambda-1) \geq 0 \\ \Rightarrow\ & \mu\lambda - (\mu+\lambda) + 1 \geq 0 \\ \Rightarrow\ & n(n-1) - (v-2n) + 1 \geq 0 \\ \Rightarrow\ & n^2 + n + 1 \geq v. \end{aligned}$$

Again assuming that $n > 1$, we use the arithmetic-geometric mean inequality:

$$\begin{aligned} & (\mu+\lambda)^2 \geq 4\mu\lambda \\ \Rightarrow\ & (v-2n)^2 \geq 4n(n-1) = (2n-1)^2 - 1 \\ \Rightarrow\ & v - 2n \geq 2n - 1 \qquad \text{since } n > 1, \\ \Rightarrow\ & v \geq 4n - 1. \end{aligned}$$

Thus, in summary, for a non-trivial symmetric design of order n,

$$4n - 1 \leq v \leq n^2 + n + 1.$$

The extremal cases of these inequalities have been much studied. When $v = n^2 + n + 1$ (which occurs if and only if $\lambda = 1$), the symmetric design is called a *projective plane of order* n. These have been constructed when n is a power of a prime, and for no other values of n. As an example, the $(13, 4, 1)$-symmetric design (1.1) is a projective plane of order 3. A massive computer search by C. Lam and others showed that projective planes of order 10 do not exist, the only symmetric designs that have been eliminated by something other than the necessary conditions given above.

The case $v = 4n - 1$ corresponds to *Hadamard 2-designs* with parameters $(4n-1,\ 2n-1,\ n-1)$. These exist if and only if a $4n \times 4n$ Hadamard matrix exists (and hence they are conjectured to exist for all n). These parameters always satisfy the BRC condition (with $x = y = z = 1$).

Symmetric designs with $v = 4n$ have also been greatly studied, and give rise to so-called regular Hadamard matrices. In this case BRC (i) implies that $n = u^2$ is a square, and the parameters must be $(4u^2,\ 2u^2 - u,\ u^2 - u)$.

Finally, we come to consider symmetric designs satisfying $v = 4n + 1$. These have been studied far less than the families described above, and these are the common theme to this dissertation. We derive their parameters as follows: assuming $k \leq v/2$, let $t = n - \lambda$, so that with $k = n + \lambda$ we have

$$n = (k + t)/2, \qquad \lambda = (k - t)/2;$$

using $v - 1 = 4n$ and equation (1.2) we obtain

$$\begin{aligned} & 4n\lambda = k^2 - k \\ \Rightarrow\ & k^2 - t^2 = k^2 - k \\ \Rightarrow\ & k = t^2, \quad \lambda = t(t-1)/2, \quad n = t(t+1)/2, \quad v = 2t(t+1) + 1. \end{aligned} \tag{1.4}$$

Observe that (1.1) is such a symmetric design (corresponding to $t = 2$), and $t = 1$ gives the trivial $(5, 1, 0)$-design. We also see that these parameters always satisfy BRC (ii) (with $x = y = 1,\ z = t$). In fact, these designs are a special

case ("$h = 2$") of a more general construction of A.E. Brouwer in [Br]; he gives a construction whenever t is an odd prime power. Another version of this construction is provided in Chapter 5 of this thesis. In addition, Bridges, Hall, and Hayden constructed a $(41, 16, 6)$-symmetric design in [BHH] (this is the $t = 4$ case). No constructions have been found for other values of the parameter t.

Before considering these designs further, however, we turn to one of the most important construction methods for symmetric designs.

1.3. Automorphisms and Difference Sets

Two (v, k, λ)-symmetric designs are said to be *isomorphic* if there is a bijection between their point sets and a bijection between their block sets that preserve the incidence relation. Another way of saying this is that there is a bijection between their point sets which induces a bijection between blocks by the incidence relation. Designs with the same parameters can certainly be non-isomorphic; indeed, a symmetric design need not be isomorphic to its own dual.

An isomorphism of a symmetric design with itself is called an *automorphism* of the design. It is simply a permutation of the points that takes blocks to blocks. A group of automorphisms is *sharply transitive*, or regular, if for any two distinct points there exists *exactly* one automorphism in the group that takes the first point to the second. It can be shown (see [vLW]) that the number of orbits of points under the action of the group is equal to the number of orbits of the blocks under the group action; in particular, if the group is sharply transitive on the points, then it is sharply transitive on the blocks also.

If a symmetric design admits a sharply transitive group G of automorphisms, we can fix a point x_0 of the design and identify the group G with the point set $\mathcal{P}$ by the correspondence $g \in G \leftrightarrow gx_0 \in \mathcal{P}$. We can then fix a block $D \in \mathcal{B}$, thought of as a subset of G, so that, under the induced sharply transitive action of the group of automorphisms on the blocks, the other blocks are simply the left translates of D in G, i.e., of the form gD for a $g \in G$.

The properties of the symmetric design can then be shown without difficulty to imply that for every non-identity element $g \in G$, there are exactly λ pairs $x, y \in D$ satisfying $xy^{-1} = g$.

DEFINITION. A (v, k, λ)-*difference set* is a subset D (of size k) of a group G (of size v), such that for every non-identity element $g \in G$, there are exactly λ pairs $x, y \in D$ satisfying $xy^{-1} = g$ (or $x - y = g$ if using additive notation). The difference set is called *cyclic* (respectively, *abelian, non-abelian*) if the group G is.

Conversely, given a (v, k, λ)-difference set D in a group G, form an incidence structure with point set G and blocks given by the set $\{gD : g \in G\}$ of all left translates of D. This is called the *development* of D (or dev$D$ for short), and is a (v, k, λ)-symmetric design admitting a sharply transitive group of automorphisms isomorphic to G. Note that each of the translates of D is also a difference set in G.

As an example, identify the point set $\mathcal{P}$ of (1.1) with the cyclic group $\mathbf{Z}_{13}$. Then the first block, $\{0, 1, 3, 9\}$, is a $(13, 4, 1)$-difference set in $\mathbf{Z}_{13}$, since each non-zero element of the group is represented exactly once as a difference of elements in D. For example, $1 = 1 - 0,\ 2 = 3 - 1,\ 4 = 0 - 9$, etc. The other blocks of the design are simply the translates of this set in $\mathbf{Z}_{13}$.

Thus the existence of symmetric designs admitting a sharply transitive group of automorphisms is equivalent to the existence of difference sets. Due to their algebraic structure and simpler description, the search for the latter is generally easier than the search for symmetric designs, and difference sets have become one of the most fruitful sources of symmetric designs. As we shall see in subsequent chapters, the increased structure also makes it easier to prove the non-existence of certain difference sets. However, this does *not* imply the non-existence of all symmetric designs with the same parameters. For a good survey of the theory of difference sets, see [J].

The algebraic structure of difference sets is often exploited by using the *group ring* formulation. Given a group G, let $\mathbf{Z}G$ be the free $\mathbf{Z}$-module with basis G. For any subset $A \subset G$, we abuse notation and also denote the group ring element

$\sum_{g\in A} g$ by A. For any $A = \sum_{g\in G} a_g g \in \mathbf{Z}G$, we write $A^{(-1)} = \sum_{g\in G} a_g g^{-1}$. Finally, in the group ring we use an integer m to denote the element $m1_G$. With this formalism, the defining condition for a subset $D \subset G$ to be a difference set is equivalent to the following equation in the group ring:

$$DD^{(-1)} = n + \lambda G. \tag{1.5}$$

This allows the use of algebraic techniques such as character theory; we shall see some of this in Chapter 2.

Difference sets corresponding to the three cases $v = n^2+n+1$, $v = 4n-1$, and $v = 4n$ have again been the object of a great deal of study. In fact, interest in difference sets seems to have been growing recently, and several surprising new results have been published in the last few years. A considerable amount of attention has been given to the latter of these three cases, the $(4u^2, 2u^2 - u, u^2 - u)$-difference sets, variously called Menon difference sets, Hadamard difference sets, or H-sets. The existence question seems to be quite complex in this case. Most work in difference set theory has been done with abelian groups, but constructions of new examples of these difference sets are being found in non-abelian groups (e.g., see [Sm]). It is widely conjectured that non-trivial ($u > 1$) *cyclic* examples of this case do not exist. This point is visited again in Chapter 4.

However, very little work has been done in the $v = 4n + 1$ case. The first explicit reference is [T], where R.J. Turyn remarks that cyclic difference sets with parameters (1.4) (namely, $(2t(t + 1) + 1, t^2, t(t - 1)/2)$) exist for $t = 1, 2$, but not for $3 \leq t \leq 11$. The only extensive reference is [EK], where the authors have a table showing the non-existence of these difference sets in cyclic groups for $3 \leq t \leq 100$, with the possible exception of $t = 50$. In [B] I also eliminated the case $t = 50$, and observed that no difference set, even non-abelian, exists for $3 \leq t \leq 100$. The former result is demonstrated in Chapter 2 of this work.

As a result it seems reasonable to conjecture that abelian difference sets with these parameters do not exist at all for $t \geq 3$. Towards this, we prove in Chapter 3

the non-existence of difference sets with these parameters for a set of values of t having density 1 in the positive integers.

In Chapter 4, we consider the connection of cyclic difference sets with auto-correlations of finite binary sequences $x_1, x_2, \ldots, x_v$, defined by $c_r = \sum_{i=1}^{v-r} x_i x_{i+r}$ and $p_r = \sum_{i=1}^{v} x_i x_{i+r}$, with subscripts read modulo v. We prove a bound on $|c_r|$ given a sequence with constant values of p_r.

Finally, in Chapter 5 we return to symmetric designs and present an alternative to Brouwer's construction of a family of symmetric designs.

2. MULTIPLIERS AND DIFFERENCE SETS

2.1. Multipliers

If D is a difference set in G and α is a group automorphism of G, then dev $\alpha(D)$ is isomorphic as a symmetric design to dev$D$. Two (v, k, λ)-difference sets D_1, D_2 in the same group G are said to be *equivalent* if there is a group automorphism α of G such that D_1 is a translate of $\alpha(D_2)$.

DEFINITION. An automorphism α of G is a *multiplier* of the difference set D in G if $\alpha(D)$ is a translate of D. If G is abelian and written additively, and α is multiplication by an integer z relatively prime to $\exp(G)$ (the exponent of G), then we also say that z is a (*numerical*) *multiplier* of D.

From now on, we only consider numerical multipliers. Most of the background information in this section is from [J].

Multipliers are among the most powerful tools in the study of difference sets, and were first introduced by M. Hall in [H1]. A multiplier puts tremendous restrictions on a difference set, making it much easier to construct one (when it exists) or to prove non-existence (when it does not). One fact that makes them so useful is the following theorem of McFarland and Rice (see [BJL]):

Theorem. *Let D be a difference set in an abelian group G. Then there exists a translate of D that is fixed by every numerical multiplier of D.*

So given a multiplier z of an abelian difference set D, we can always assume that D is fixed by z. But then this implies that D must be a union of orbits of the action of multiplication by z, often rendering the existence of D susceptible to a computer search or algebraic techniques, or both.

What makes multipliers most useful, however, is the fact that it is often not difficult to show that a difference set has one, by means of one of several multiplier theorems. One of the most general is the following due to P.K. Menon (see [M]):

"Second" Multiplier Theorem. *Let D be an abelian (v, k, λ)-difference set in G, and let $m > \lambda$ be a divisor of n which is relatively prime to v. Suppose that z is an integer relatively prime to v which satisfies the following condition: for every prime p dividing m, there is an $f \geq 1$ such that $z \equiv p^f \pmod{\exp(G)}$. Then z is a numerical multiplier for D.*

Another one, due to McFarland ([Mc]), is more complicated. We first define a function M as follows:

$$M(1) = 1, \qquad M(2) = 2 \cdot 7, \qquad M(3) = 2 \cdot 3 \cdot 11 \cdot 13, \qquad M(4) = 2 \cdot 3 \cdot 7 \cdot 31,$$

and for $z \geq 5$, $M(z)$ is defined recursively to be the product of the distinct prime factors of the numbers

$$z,\ M(z^2/p^{2e}),\ p-1,\ p^2-1,\ \ldots,\ p^{u(z)}-1,$$

where p is a prime divisor of z with $p^e \parallel z$ (i.e., p^e exactly divides z) and where $u(z) = z(z-1)/2$. Notice that the "definition" of M actually depends on the choice of p for each z.

Then the theorem is as follows:

McFarland's Multiplier Theorem. *For every positive integer z, the Second Multiplier Theorem remains true if the condition $m > \lambda$ is replaced by the condition that $M(n/m)$ and v are relatively prime.*

As Jungnickel points out in [J], this result is difficult to apply! However, we use it to eliminate the case $t = 50$ from Table I of [EK].

It is conjectured that in fact the condition "$m > \lambda$" can be dropped altogether from the Multiplier Theorem (this is called the Multiplier Conjecture).

2.2. Use of McFarland's Multiplier Theorem

In this section we apply McFarland's Theorem to eliminate the one gap in Table I of [EK], which shows the non-existence of cyclic $(2t(t+1)+1,\ t^2,\ t(t-1)/2)$-difference sets for $3 \leq t \leq 100$, $t \neq 50$. This result has appeared in [B].

Theorem 2.1. *There does not exist a* $(5101, 2500, 1225)$*-difference set.*

Proof. The stated parameters are the $t = 50$ case. We have $v = 5101$, a prime, (so $G = \mathbf{Z}_{5101}$), and $n = 1275 = 3 \cdot 5^2 \cdot 17$. Let $m = 3 \cdot 17$. So $n/m = 5^2$, and $M(5^2)$ has as factors the prime factors of

$$5^2, M(1), 5-1, 5^2-1, 5^{300}-1\,,$$

since $u(25) = 300$. But the multiplicative order of 5 modulo 5101 is 425, so $M(25)$ is not divisible by $v = 5101$. Moreover,

$$3^{1088} \equiv 17^1 \pmod{5101}\,,$$

and so by McFarland's Theorem $d = 17$ is a multiplier of any $(5101, 2500, 1225)$-difference set.

But the non-trivial orbits of multiplication by 17 in $\mathbf{Z}_{5101}$ are all of size 75, so it is impossible for a union of orbits to have size 2500 and hence no such difference set exists. □

2.3. Multipliers and the Group Ring

In [B] it is also shown that there are no *non*-cyclic difference sets with parameters (1.4) in the range $3 \leq t \leq 100$. These are mostly eliminated with the "Semi-Primitivity Theorem" (see Chapter 3), but there is one non-cyclic case which must be handled differently, namely $t = 49$. In this section, we prove that there is no non-cyclic difference set when $t = 49$, using the Multiplier Theorem and the group ring equation (1.5). The method is analogous to that used by Eliahou and Kervaire in eliminating the cyclic case (see [EK]).

As described in [B], this result also follows from Theorem 4.18 in [L], which in turn can be shown to follow from a stronger version of the Semi-Primitivity Theorem.

Theorem 2.2. *There does not exist a non-cyclic* $(4901, 2401, 1176)$*-difference set.*

Proof. These are the parameters at $t = 49$. Since $v = 4901 = 13^2 \cdot 29$, the only non-cyclic group of this order is $G = \mathbf{Z}_{13} \times \mathbf{Z}_{13} \times \mathbf{Z}_{29}$. Its exponent is $\exp(G) = 377$.

We have $n = 1225 = 5^2 \cdot 7^2$. But since $7^6 \equiv 5^2 \equiv 25 \pmod{377}$, the Second Multiplier Theorem given above guarantees that 25 would be a multiplier of any such difference set. (McFarland's Multiplier Theorem does no better.)

Now assume that we have a difference set D in G with these parameters. We can assume that it is fixed by the multiplier 25, and hence that it is the union of orbits of the action of this automorphism.

Represent the elements of G as $\{(i,j,k) : i,j \in \mathbf{Z}_{13}, k \in \mathbf{Z}_{29}\}$. We will also use integer representatives of i,j,k. Then the orbits of multiplication by 25 in G are:

$$\begin{aligned}
1 \quad & \{(0,0,0)\} \\
X_{ij} \quad & \{(i,j,0), (-i,-j,0)\}, \qquad \text{for } (i,j) \neq (0,0) \\
Y_1 \quad & \{(0,0,1),(0,0,-4),(0,0,-13),(0,0,-6),(0,0,-5),(0,0,-9),(0,0,7)\} \\
Y_2 \quad & \{(0,0,2),(0,0,-8),(0,0,3),(0,0,-12),(0,0,-10),(0,0,11),(0,0,14)\} \\
Y_1^{(-1)} \quad & \{(0,0,-1),(0,0,4),(0,0,13),\ldots\} \\
Y_2^{(-1)} \quad & \{(0,0,-2),(0,0,8),(0,0,-3),\ldots\},
\end{aligned}$$

(where we identify $X_{i,j} = X_{-i,-j}$), and another 336 orbits of size 14 each, given by

$$X_{ij}Y_1,\ X_{ij}Y_2,\ X_{ij}Y_1^{(-1)},\ X_{ij}Y_2^{(-1)} \qquad \text{for } (i,j) \neq (0,0).$$

We are abusing notation and identifying subsets of G with their corresponding elements in the group ring $\mathbf{Z}G$, and so multiplication above is in the group ring. Observe that $X_{ij}^{(-1)} = X_{ij}$ for all i,j.

So since D is a union of these orbits, it can be written in the following form in $\mathbf{Z}G$:

$$D = C + AY_1 + BY_2 + PY_1^{(-1)} + QY_2^{(-1)},$$

where C, A, B, P, Q are each of the form

$$\varepsilon + \sum_{i,j} x_{ij} X_{ij},$$

and the coefficients ε, x_{ij} are each 0 or 1.

Now by (1.5) we can write

$$DD^{(-1)} = 1225 + 1176G \qquad \text{in } \mathbf{Z}G. \tag{2.1}$$

Let $G = G_1 \times G_2$ with $G_1 = \mathbf{Z}_{13} \times \mathbf{Z}_{13}$ and $G_2 = \mathbf{Z}_{29}$, and let $\pi\colon \mathbf{Z}G \to \mathbf{Z}G_1$ be the canonical projection onto the group ring of G_1.

Then $\pi(Y_1) = \pi(Y_2) = \pi(Y_1^{(-1)}) = \pi(Y_2^{(-1)}) = 7$, so reducing modulo 7 we have from (2.1),

$$\pi(DD^{(-1)}) = \pi(CC^{(-1)}) = 0 \qquad \text{in } \mathbf{F}_7 G_1 \tag{2.2}$$

(where $\mathbf{F}_7$ is the Galois field of order 7), since $1225 \equiv 1176 \equiv 0 \pmod 7$.

We also see that $C^{(-1)} = C$, so from (2.2) we have

$$\pi(C)^2 = 0 \qquad \text{in } \mathbf{F}_7 G_1. \tag{2.3}$$

We now need the following lemma:

Lemma. ([vLW], Lemma 28.6) *Let G be an abelian group of order v and p a prime, $p \not| v$. If $A \in \mathbf{Z}G$ and $A^m \equiv 0 \pmod{p, G}$ for some positive integer m, then $A \equiv 0 \pmod{p, G}$.*

Since 7 does not divide $|G_1| = 13^2$, we apply the Lemma to (2.3) to get

$$\pi(C) = 0 \quad \text{in } \mathbf{F}_7 G_1 \qquad \Rightarrow \qquad C = 0 \quad \text{in } \mathbf{F}_7 G.$$

But the coefficients of C are all 0 or 1, so in fact $C = 0$ in $\mathbf{Z}G$. Thus

$$D = AY_1 + BY_2 + PY_1^{(-1)} + QY_2^{(-1)},$$

and $\pi(D) = 7S$, where

$$S = \pi(A + B + P + Q) = r + \sum_{i,j} s_{ij}\pi(X_{ij})$$

and the coefficients of S satisfy $0 \leq r, s_{ij} \leq 4$, and $S^{(-1)} = S$.

Now by (2.1) we have $\pi(DD^{(-1)}) = 1225 + 1176 \cdot 29G_1$, where $G_1 = \sum_{h \in G_1} h$ in $\mathbf{Z}G_1$, so

$$S^2 = 25 + 696G_1 \qquad \text{in } \mathbf{Z}G_1. \tag{2.4}$$

Notice that two possible solutions of this equation for S are $\pm(5 + 2G_1) \in \mathbf{Z}G_1$ since $G_1^2 = 169G_1$. We will show that there can be no more than two solutions, which will complete the proof, since in that case $r = \pm 7$, contradicting $0 \leq r \leq 4$.

We first find solutions to equation (2.4) in $\mathbf{C}G_1$. We use some elementary character theory.

Let $\zeta = e^{2\pi i/13}$ be a primitive 13^{th} root of unity in $\mathbf{C}$. Then the irreducible characters of G_1 are

$$\chi_{ij} \colon G_1 \to \mathbf{C}^*, \quad \chi_{ij}(k, l) = \zeta^{ik+jl}, \qquad \text{for } 0 \leq i, j \leq 12.$$

These extend by linearity to maps $\chi_{ij} \colon \mathbf{C}G_1 \to \mathbf{C}$.

It is not hard to show that

$$\chi_{00}(G_1) = 169,$$
$$\chi_{ij}(G_1) = 0 \qquad \text{for } (i, j) \neq (0, 0)$$

with $G_1 \in \mathbf{C}G_1$.

Given $S \in \mathbf{C}G_1$ such that $S^2 = 25 + 696G_1$, it follows that

$$\chi_{00}(S^2) = 117649 = 343^2,$$
$$\chi_{ij}(S^2) = 25 = 5^2 \qquad \text{for } (i, j) \neq (0, 0)$$

which implies

$$\chi_{00}(S) = \pm 343,$$
$$\chi_{ij}(S) = \pm 5 \qquad \text{for } (i, j) \neq (0, 0).$$

We now consider possible solutions $Z \in \mathbf{Z}G_1$ to equation (2.4). By replacing Z by $-Z$ if necessary, we may assume that $\chi_{00}(Z) = 343$.

One sees that the restriction of χ_{ij} to $\mathbf{Z}G_1$ maps into the ring $\mathbf{Z}[\zeta]$. We have a map

$$\phi\colon \mathbf{Z}[\zeta] \to \mathbf{F}_{13}$$

induced by $\zeta \mapsto \overline{1} \in \mathbf{F}_{13}$, so that

$$\phi\left(\sum_{i,j} a_{ij}\zeta^{ik+jl}\right) = \sum_{i,j} \overline{a}_{i,j}.$$

But this is also the image of $\sum a_{ij} \in \mathbf{Z}$ under the canonical projection $\mathbf{Z} \to \mathbf{F}_{13} = \mathbf{Z}_{13}$.

So the following diagram commutes:

$$\begin{array}{ccc} \mathbf{Z}G_1 & \xrightarrow{\chi_{ij}} & \mathbf{Z}[\zeta] \\ \downarrow{\scriptstyle \chi_{00}} & & \downarrow{\scriptstyle \phi} \\ \mathbf{Z} & \xrightarrow{\text{mod } 13} & \mathbf{F}_{13} \end{array}$$

Now the image of $Z \in \mathbf{Z}G_1$ along the left and bottom arrows is

$$\overline{343} = \overline{5} \qquad \text{in } \mathbf{F}_{13},$$

and since $5 \not\equiv -5 \pmod{13}$, we must also have

$$\chi_{ij}(Z) = 5 \qquad \text{for all } (i,j) \neq (0,0).$$

But by the standard Inversion Formula for characters (e.g., see Lemma 3.2 in [J]) this determines Z uniquely. So, with negation, there are only two solutions to equation (2.4) in $\mathbf{Z}G_1$, as claimed. □

Although these multiplier methods are powerful, their use is very dependent on the specific parameters involved. In Chapter 3 we apply a more easily used theorem to show that "most" difference sets satisfying $v = 4n + 1$ do not exist.

3. SEMI-PRIMITIVITY AND DIFFERENCE SETS

3.1. Semi-primitivity

One of the most powerful theorems available to prove the non-existence of putative difference sets uses the notion of semi-primitivity.

DEFINITION. A prime p is said to be *semi-primitive* modulo w with $(p, w) = 1$ if there exists some $f \geq 1$ such that $p^f \equiv -1 \pmod{w}$. A number m is semi-primitive modulo w if $(m, w) = 1$ and each of its prime factors is semi-primitive modulo w.

A rather specialized version of the semi-primitivity theorem, originally due to H.B. Mann, appears below; for a more general and complete version, see Theorem 7.1 in [J].

Semi-Primitivity Theorem. *Suppose an abelian group G admits a non-trivial (v, k, λ)-difference set, with $n = k - \lambda$, and suppose that for some factor w of v with $w \neq 1$, and some prime $p \not| w$, p is semi-primitive modulo w. Then*

(i) *p does not divide the square-free part of n , say $p^{2j} \parallel n$;*

(ii) *$p^j \leq v/w$. In particular, if p is semi-primitive modulo v, then $p \not| n$.*

Lander has also shown in [L] that under the same hypotheses for *any* group G, even non-abelian, conclusion (i) still holds; see Theorem 7.6 in [J].

Now consider the (v, k, λ)-difference sets that satisfy $v = 4n + 1$. As shown in the introduction, such difference sets must have parameters of the form:

$$\begin{gathered} \big(t^2 + (t+1)^2, \quad t^2, \quad t(t-1)/2\big), \\ n = \frac{t(t+1)}{2}. \end{gathered} \tag{3.1}$$

$t = 1$ gives the trivial $(5, 1, 0)$-difference set, and $t = 2$ gives the parameters $(13, 4, 1)$ of the design shown in (1.1). But in [EK] and [B] it has been shown that no such difference sets exist for $3 \leq t \leq 100$. A quick look at Table I of [EK] shows that the great majority of these cases are eliminated by means of the semi-primitivity theorem quoted above. It turns out that this is not entirely a quirk of small values

of t. In [EK] Eliahou and Kervaire use the fact that $4n \equiv -1 \pmod{v}$ to show that the semi-primitivity theorem eliminates abelian difference sets with parameters (3.1) in the following cases:

(i) v is a prime power;

(ii) every prime factor of n divides the square-free part of n.

Unfortunately it is very difficult to know how often the above cases occur for the various values of t. However, semi-primitivity relations do indeed hold for "most" values of t, as shown in the next few propositions.

Proposition 3.1. *Abelian difference sets with parameters* (3.1) *do not exist for* $t = 2^m$ *or* $t = 2^m - 1, \quad m > 1$.

Proof. We first establish some easy relations. From (3.1) we see that $v = 2t^2 + 2t + 1 = 2(t+1)^2 - 2(t+1) + 1$. So

$$4t^4 + 1 = \big(2t^2 + 2t + 1\big)\big(2t^2 - 2t + 1\big) \equiv 0 \pmod{v},$$

$$4(t+1)^4 + 1 = \big(2(t+1)^2 - 2(t+1) + 1\big)\big(2(t+1)^2 + 2(t+1) + 1\big) \equiv 0 \pmod{v}.$$

Thus $4t^4 \equiv 4(t+1)^4 \equiv -1 \pmod{v}$. This also follows easily from the alternative form of the basic parametric equation, $\lambda v + n = k^2$, whence $4t^4 = 4k^2 \equiv 4n \equiv -1 \pmod{v}$.

Now by hypothesis either $t = 2^m$ or $(t+1) = 2^m$, so the above relations show that $2^{4m+2} \equiv -1 \pmod{v}$; i.e., that 2 is semi-primitive modulo v. But $m > 1 \Longrightarrow n = t(t+1)/2$ is divisible by 2, so by part (ii) of the semi-primitivity theorem, no abelian difference set with parameters (3.1) exists. □

We now try to establish some more general situations where semi-primitivity holds. For this we use well-known facts from elementary number theory. First, for distinct primes p and q we say that p is a *quadratic residue* modulo q if there is some integer x with $p \equiv x^2 \pmod{q}$, and a *quadratic nonresidue* otherwise. Similarly we say that p is *biquadratic* (or *quartic*) modulo q if there is some integer x such that $p \equiv x^4 \pmod{q}$.

FACTS. Suppose that q is odd.

(a) $p^{(q-1)/2} \equiv 1 \pmod{q}$ if p is quadratic modulo q;
$p^{(q-1)/2} \equiv -1 \pmod{q}$ otherwise;

(b) if $q \equiv -1 \pmod{4}$ then p is biquadratic modulo q iff p is quadratic modulo q;

(c) if $q \equiv 1 \pmod{4}$ and p is quadratic modulo q, then
$p^{(q-1)/4} \equiv 1 \pmod{q}$ if p is biquadratic modulo q, and
$p^{(q-1)/4} \equiv -1 \pmod{q}$ otherwise.

So in particular p is semi-primitive modulo q if it is not biquadratic modulo q.

Thus we would like to know necessary and sufficient conditions for a prime p to be quadratic or biquadratic modulo q. We consider first $p = 2$.

Lemma 3.2. *Let q be an odd prime.*

(i) *2 is quadratic modulo q for $q \equiv 1$ or $7 \pmod{8}$, and non-quadratic for $q \equiv 3$ or $5 \pmod{8}$;*

(ii) *Assume $q \equiv 1 \pmod{8}$, and write $q = x^2 + 4y^2$. Then 2 is biquadratic modulo q iff $y \equiv 0 \pmod{4}$.*

See, e.g., [IR] for a proof. In particular, part (ii) occurs as exercise 28 in chapter 5 of [IR], and is also explicitly stated in [G].

Like the first proposition, the next one also uses semi-primitivity of the prime 2, but part (i) of the semi-primitivity theorem instead. Proposition 3.1 dealt with the case that one of t and $t + 1$ is purely a power of 2, while the next proposition considers the case where n is divisible by only one factor of 2.

Remark 3.3. *If $w, z \in \mathbf{Z}[i]$ both have imaginary parts divisible by some integer d, then so does their product wz.*

This follows immediately from $(x + yi)(a + bi) = (xa - yb) + (xb + ya)i$; if $d|y$ and $d|b$, then $d|(xb + ya)$.

Proposition 3.4. *There does not exist any (v, k, λ)-difference set, with $n = k - \lambda$, satisfying $v = 4n + 1$ and $n \equiv 2 \pmod{4}$.*

Proof. We show that, under the hypotheses, 2 must be semi-primitive modulo some factor of v, and so by (i) of the semi-primitivity theorem and the fact that $2^1 \parallel n$, no such difference set can exist (not even a non-abelian one, by Lander's result).

We first observe that if $q \mid v$, q a prime, then $q \equiv 1 \pmod 4$, since from the proof of Proposition 3.1, $4t^4 \equiv -1 \pmod q \implies -1$ is quadratic modulo q.

Now if v has a prime factor $q \equiv 5 \pmod 8$, then by Lemma 3.2 (i), 2 is non-quadratic modulo q and hence semi-primitive modulo q. So now assume that $q \equiv 1 \pmod 8$ for every prime $q \mid v$. If 2 is not biquadratic modulo q, then again it is semi-primitive modulo q. So we can now assume that 2 is biquadratic modulo every $q \mid v$, and will arrive at a contradiction.

Expand $v = t^2 + (t+1)^2$ into its Gaussian prime factors in $\mathbf{Z}[i]$. Each prime $q \mid v$ can be factored as $q = (x + 2yi)(x - 2yi)$, say. By Lemma 3.2 (ii), we have $y \equiv 0 \pmod 4$.

But v can also be written as $v = \big(t+(t+1)i\big)\big(t-(t+1)i\big)$. The factor $t+(t+1)i$ is a unit (i.e., ± 1 or $\pm i$) times a product of Gaussian primes $x+2yi$, with each $y \equiv 0 \pmod 4$. By Remark 3.3, we observe that any product of these Gaussian primes will still have its imaginary part divisible by 8. So by induction on the Gaussian prime factors of $t + (t+1)i$, we conclude that either $t \equiv 0 \pmod 8$ or $(t+1) \equiv 0 \pmod 8$. But in either case we then have $n = t(t+1)/2 \equiv 0 \pmod 4$, contradicting the hypothesis. □

We note that $n \equiv 2 \pmod 4$ iff $t \equiv 3$ or $4 \pmod 8$, and that in some sense this eliminates one quarter of all putative difference sets with parameters (3.1).

We now use a biquadratic approach for odd primes p. However, this will require more preparation.

3.2. Biquadratic Reciprocity

The law of biquadratic reciprocity goes back to Gauss, although Eisenstein

published the first proof. All of the number-theoretic information in this section before the lemmas is drawn from Chapter 9 of [IR].

As usual we define the norm on the Gaussian integers $\mathbf{Z}[i]$ as $N(a+bi) = a^2+b^2$. Let π be an irreducible in this ring. Then the quotient ring $\mathbf{Z}[i]/(\pi)$ is a field with $N(\pi)$ elements.

Now also let $\alpha \in \mathbf{Z}[i]$, with $\pi \not| \alpha$ and assume $N(\pi)$ odd. Then $\chi_\pi(\alpha)$, the biquadratic character, denotes the unique element of $\{1, -1, i, -i\}$ such that

$$\alpha^{(N(\pi)-1)/4} \equiv \chi_\pi(\alpha) \pmod{\pi}.$$

Then it is easy to check that $\chi_\pi(\alpha\beta) = \chi_\pi(\alpha)\chi_\pi(\beta)$, and that $\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$.

Let q be an odd prime. Since we only consider the case that q divides $v = t^2 + (t+1)^2$, we assume that $q \equiv 1 \pmod 4$. Let $q = \lambda\overline{\lambda}$, where $\lambda = x + 2yi$ is a Gaussian prime. For $p \in \mathbf{Z}$, notice that

$$\begin{aligned} \chi_\lambda(p) \neq 1 &\Rightarrow p^{(q-1)/4} \not\equiv 1 \pmod{\lambda} \\ &\Rightarrow p^{(q-1)/4} \not\equiv 1 \pmod{q} \\ &\Rightarrow p \text{ is not biquadratic modulo } q \\ &\Rightarrow p \text{ is semi-primitive modulo } q. \end{aligned}$$

We say that a non-unit $\alpha = a+bi \in \mathbf{Z}[i]$ is *primary* if either $a \equiv 1 \pmod 4$, $b \equiv 0 \pmod 4$, or $a \equiv 3 \pmod 4$, $b \equiv 2 \pmod 4$. For any non-unit α with $N(\alpha)$ odd, there is a unique unit u such that $u\alpha$ is primary.

Biquadratic Reciprocity Law ([IR], Chapter 9, Section 9). *Let π and λ be relatively prime primary elements of $\mathbf{Z}[i]$. Then*

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{((N(\lambda)-1)/4)((N(\pi)-1)/4)}.$$

We now derive (relatively) useful criteria for determining when an odd prime p is biquadratic modulo $q \equiv 1 \pmod 4$.

For a complex number z, let $\Re(z)$ and $\Im(z)$ be its real and imaginary parts, respectively.

Lemma 3.5. *Let $p \equiv 1 \pmod 4$ and $q \equiv 1 \pmod 4$ be distinct primes, with $q = \lambda\overline{\lambda}$, where $\lambda \in \mathbf{Z}[i]$ is a primary Gaussian irreducible. Then $\chi_\lambda(p) = 1$ if and only if $\Im(\lambda^{(p-1)/4}) \equiv 0 \pmod p$.*

Proof. Write $p = \pi\overline{\pi}$ where π is a primary irreducible in $\mathbf{Z}[i]$. Then

$$\chi_\lambda(p) = \chi_\lambda(\pi)\chi_\lambda(\overline{\pi}) = \chi_\pi(\lambda)\chi_{\overline{\pi}}(\lambda)$$

by the Biquadratic Reciprocity Law. So $\chi_\lambda(p) = 1$ if and only if

$$\begin{aligned}
&\chi_\pi(\lambda) = \overline{\chi_{\overline{\pi}}(\lambda)} \\
\iff &\chi_\pi(\lambda) = \chi_\pi(\overline{\lambda}) \\
\iff &\lambda^{(p-1)/4} \equiv \overline{\lambda}^{(p-1)/4} \pmod{\pi} \\
\iff &\lambda^{(p-1)/4} \equiv \overline{\lambda}^{(p-1)/4} \pmod{\overline{\pi}} \\
\iff &\lambda^{(p-1)/4} \equiv \overline{\lambda}^{(p-1)/4} \pmod{p} \\
\iff &\Im(\lambda^{(p-1)/4}) \equiv 0 \pmod p.
\end{aligned}$$

□

Lemma 3.6. *Let $p \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$ be primes, with $q = \lambda\overline{\lambda}$, where $\lambda \in \mathbf{Z}[i]$ is a primary Gaussian irreducible. Then $\chi_\lambda(p) = 1$ if and only if*

$$\lambda^{(p^2-1)/4} \equiv (-1)^{(q-1)/4} \pmod p.$$

Proof. In this case, $-p$ is a primary Gaussian irreducible, and $N(p) = p^2$. Then by the Biquadratic Reciprocity Law,

$$\begin{aligned}
\chi_\lambda(p) &= \chi_\lambda(-1)\chi_\lambda(-p) \\
&= (-1)^{(q-1)/4}\chi_{-p}(\lambda) \\
&= (-1)^{(q-1)/4}\chi_p(\lambda).
\end{aligned}$$

So then $\chi_\lambda(p) = 1$ if and only if

$$\chi_p(\lambda) = (-1)^{(q-1)/4}$$
$$\iff \lambda^{(p^2-1)/4} \equiv (-1)^{(q-1)/4} \pmod{p}.$$

□

We remark that the condition given by Lemma 3.6 for $\chi_\lambda(p) = 1$ is equivalent to the following:

(i) $\Im(\lambda^{(p+1)/4}) \equiv 0 \pmod{p}$ *if* $q \equiv 1 \pmod{8}$,

(ii) $\Re(\lambda^{(p+1)/4}) \equiv 0 \pmod{p}$ *if* $q \equiv 5 \pmod{8}$.

3.3. Main Non-existence Theorem

Theorem 3.7. *Let $n = t(t+1)/2$ and suppose that p is an odd prime dividing the square-free part of n. Then there does not exist a difference set with parameters* (3.1) *in the following cases:*

(i) $p \equiv 3 \pmod{8}$ *and either*

  (a) *n is even, and t or $t+1 \equiv p \pmod{2p}$, or*

  (b) *n is odd, and t or $t+1 \equiv 0 \pmod{2p}$;*

(ii) $p \equiv 5 \pmod{8}$ *and t or $t+1 \equiv p \pmod{2p}$;*

(iii) $p \equiv 7 \pmod{8}$ *and n is odd.*

Proof. By the semi-primitivity theorem it suffices to show that p is semi-primitive modulo some factor of v, and so it suffices to show that p is not biquadratic modulo some factor of v. We assume the contrary and arrive at a contradiction. Recall that the prime factors of v are congruent to $1 \pmod{4}$.

Consider first the case $p \equiv 1 \pmod{4}$.

Suppose that p is biquadratic modulo every prime factor q of v, and write $q = \lambda\overline{\lambda}$, where λ is a primary Gaussian irreducible. By Lemma 3.5, we have

$$\Im(\lambda^{(p-1)/4}) \equiv 0 \pmod{p}.$$

Now, as in the proof of Proposition 3.4, we write the factor $t + (t+1)i$ of v as a product of a unit and Gaussian irreducibles λ. So $(t + (t+1)i)^{(p-1)/4}$ is a product of a unit and factors $\lambda^{(p-1)/4}$, each of which has imaginary part divisible by p. By Remark 3.3 and the fact that each λ is primary, each of these factors also has even imaginary part. So again by Remark 3.3, we see that any product of such factors has imaginary part divisible by $2p$. Unfortunately, the presence of an unknown unit in the factorization of $t + (t+1)i$ undermines this knowledge. But we can at least conclude that either

$$\begin{aligned} \Re\left((t + (t+1)i)^{(p-1)/4}\right) &\equiv 0 \pmod{2p}, \quad \text{or} \\ \Im\left((t + (t+1)i)^{(p-1)/4}\right) &\equiv 0 \pmod{2p}. \end{aligned} \tag{3.2}$$

Since $p \mid n$, one of t or $t+1$ is divisible by p, and of course one of them is even. This allows four possibilities modulo $2p$.

First suppose that t or $t+1 \equiv 0 \pmod{2p}$. Then $(t + (t+1)i)^{(p-1)/4} \equiv i^{(p-1)/4}$ or $(-1)^{(p-1)/4} \pmod{2p}$, which does not contradict (3.2).

If instead, without loss of generality, $t \equiv p \pmod{2p}$, then

$$\begin{aligned} (t + (t+1)i)^{(p-1)/4} &\equiv i^{(p-1)/4} \pmod{p}, \\ (t + (t+1)i)^{(p-1)/4} &\equiv 1^{(p-1)/4} \pmod{2}, \end{aligned}$$

which can only satisfy (3.2) if $(p-1)/4$ is even, i.e. $p \equiv 1 \pmod{8}$.

So for $p \equiv 1 \pmod{4}$, we get a contradiction exactly under the hypothesis (ii). In particular, the case $p \equiv 1 \pmod{8}$ gives us no contradiction at all.

Now consider the case $p \equiv 3 \pmod{4}$.

By Lemma 3.6, we have

$$\lambda^{(p^2-1)/4} \equiv (-1)^{(q-1)/4} \pmod{p}$$

for every prime $q = \lambda\overline{\lambda}$ dividing v.

As usual, write the factor $t + (t+1)i$ as a unit, say u, times a product of Gaussian irreducibles. Since t and $t+1$ are relatively prime, exactly one of λ and $\overline{\lambda}$

must appear in this product for each prime $q = \lambda\overline{\lambda}$ dividing v, counting multiplicity. So we have

$$\begin{aligned}(t+(t+1)i)^{(p^2-1)/4} &\equiv u^{(p^2-1)/4}\prod_{q\,|\,v}(-1)^{(q-1)/4} \pmod{p}\\ &\equiv u^{(p^2-1)/4}(-1)^n \pmod{p}; \qquad (3.3)\end{aligned}$$

the last equivalence follows from the observations that $(q_1-1)/4+(q_2-1)/4 \equiv (q_1q_2-1)/4 \pmod 2$ and $(v-1)/4 = n$.

We also have t or $t+1$ divisible by p, which gives two possibilities for the left hand side of (3.3). But what about u? Recall that each λ is chosen to be primary, so that in particular it has even imaginary part. So by Remark 3.3, the product of the Gaussian primes dividing $t+(t+1)i$ has even imaginary part, whence: t odd $\iff$ u real .

Now we specialize further to $p \equiv 3 \pmod 8$. Then $p^2 \equiv 9 \pmod{16}$, and $(p^2-1)/4 \equiv 2 \pmod 4$. So (3.3) reduces to:

$$p\,|\,t \Longrightarrow i^2 \equiv u^2(-1)^n \pmod{p}$$
$$p\,|\,(t+1) \Longrightarrow (-1)^2 \equiv u^2(-1)^n \pmod{p}.$$

Combined with the previous observation, we have: if $t \equiv 0 \pmod p$ and n even then u is imaginary, which implies $t \equiv 0 \pmod{2p}$, and if n odd then u is real, so $t \equiv p \pmod{2p}$; similarly, if $(t+1) \equiv 0 \pmod p$ and n even then u is real, so $t+1 \equiv 0 \pmod{2p}$, and if n odd then u is imaginary, so $t+1 \equiv p \pmod{2p}$. But these are exactly the cases which contradict the hypotheses given by (i) in the statement of the Theorem.

Finally, consider the special case $p \equiv 7 \pmod 8$. Then we have $p^2 \equiv 1 \pmod{16}$ and $(p^2-1)/4 \equiv 0 \pmod 4$. So (3.3) reduces to:

$$1 \equiv (-1)^n \pmod{p}$$

(since $u^4 = 1$). This obviously implies n is even, which contradicts hypothesis (iii).

□

The following corollary spells out a little more explicitly which values of t are eliminated by Proposition 3.4 and Theorem 3.7:

Corollary 3.8. *Let $t \geq 1$. Then a difference set with parameters (3.1) does not exist if: $t \equiv 3$ or $4 \pmod 8$, or if $p^{2j+1} \parallel n$ for an odd prime p and one of the following holds:*

(i) $p \equiv 3 \pmod 8$ *and* $t \equiv p, 2p-1, 2p,$ *or* $3p-1 \pmod{4p}$;

(ii) $p \equiv 5 \pmod 8$ *and* $t \equiv p$ *or* $p-1 \pmod{2p}$; *or*

(iii) $p \equiv 7 \pmod 8$, *and* $t \equiv 0$ *or* $3 \pmod 4$.

This follows easily from the statements of Proposition 3.4 and Theorem 3.7 using the fact that n even $\iff$ $t \equiv 0$ or $3 \pmod 4$.

This description of eliminated cases is amenable to a search by computer. The consequences of such a search are presented in the next section.

3.4. Consequences of the Theorem

In this section, we show that Theorem 3.7 is successful in eliminating "most" of the difference sets with parameters given by (3.1). In particular, we prove:

Proposition 3.9. *The set of values of $t \geq 1$ for which difference sets with parameters (3.1) are eliminated by Theorem 3.7 has density 1 in the set of positive integers. That is,*

$$\lim_{x \to \infty} \frac{\textit{number of } t \leq x \textit{ eliminated by Thm. 3.7}}{x} = 1.$$

We actually show that the values of t eliminated by case (ii) of Theorem 3.7 already have density 1 in the positive integers.

Lemma 3.10. *Fix an odd prime p. The set of values of t for which p divides the square-free part of $n = t(t+1)/2$ has density $\delta_p = 2/(p+1)$ in the positive integers.*

Proof. We first calculate the density $\delta_p(j)$ of values of t for which $p^{2j-1} \parallel n$, for a

fixed $j \geq 1$. This condition occurs if and only if

$$t \equiv p^{2j-1}, 2p^{2j-1}, \ldots, \text{ or } (p-1)p^{2j-1} \pmod{p^{2j}}, \quad \text{or}$$
$$t+1 \equiv p^{2j-1}, 2p^{2j-1}, \ldots, \text{ or } (p-1)p^{2j-1} \pmod{p^{2j}}.$$

This accounts for exactly $2(p-1)$ residue classes modulo p^{2j}, so $\delta_p(j) = 2(p-1)/p^{2j}$. Thus

$$\begin{aligned}\delta_p &= \sum_{j\geq 1} \delta_p(j) \\ &= 2(p-1)\sum_{j\geq 1} 1/p^{2j} \\ &= \left(\frac{2(p-1)}{p^2}\right)\left(\frac{1}{1-1/p^2}\right) \\ &= \frac{2}{(p+1)}.\end{aligned}$$

□

Now for a fixed prime $p \equiv 5 \pmod 8$, what fraction of the values of t are eliminated by Theorem 3.7 (ii)? The set of t for which p divides $n = t(t+1)/2$ is equally partitioned into four subsets, according to whether t or $t+1$ is divisible by p and which one is odd. Theorem 3.7 explicitly eliminates two of those classes, so that the set of t eliminated by part (ii) of this Theorem with respect to the prime p has density $(1/2)\delta_p = 1/(p+1)$ in the positive integers. Note that the same conclusion can also be reached for a prime $p \equiv 3$ or $7 \pmod 8$, since 3.7 (i) eliminates four of eight classes and 3.7 (iii) eliminates one of two.

Now we find the density of the union of the sets of values of t eliminated with respect to primes $p \equiv 5 \pmod 8$. Consider the complements of these sets, with densities $1 - 1/(p+1)$. Now the membership of t in one of these complementary sets is determined only by the reduction of t modulo 2 and a power of p in such a way that, by the Chinese Remainder Theorem, the intersection of these sets has density given by the product of the densities of the individual sets. So the density of the union of the sets of t that are eliminated by Theorem 3.7 (ii) with respect to

primes $p \equiv 5 \pmod 8$ is given by

$$1 - \prod_{\substack{p \text{ prime} \\ p \equiv 5 \pmod 8}} \left(1 - \frac{1}{p+1}\right).$$

Proof of Proposition 3.9. We need to show that the product given above diverges to 0. Equivalently we want to show that

$$\sum_{\substack{p \text{ prime} \\ p \equiv 5 \pmod 8}} \log\left(1 - \frac{1}{p+1}\right) = -\infty.$$

But $\log(1 - \frac{1}{(p+1)}) < -1/(p+1)$, and

$$p^2 - 1 < p^2 \Rightarrow -\frac{1}{p+1} < -\frac{p-1}{p^2} = \frac{1}{p^2} - \frac{1}{p}$$
$$\Longrightarrow \quad -\sum_{\substack{p \text{ prime} \\ p \equiv 5 \pmod 8}} \frac{1}{p+1} = -\infty$$

by Dirichlet's theorem ([D, p.36] or [S]) and the fact that $\sum(1/p^2)$ converges. □

Proposition 3.9 tells us that the fraction of the set of values of $t \leq x$ which are *not* eliminated by Corollary 3.8 approaches 0 as $x \to \infty$. We did a computer search to get an idea of how quickly this happens, and obtained the following results (where S_M = the number of $t \leq M$ which are not eliminated):

Table 3.1

M	S_M	S_M/M
10	6	0.6 $\approx 1/2$
100	36	0.36 $\approx 1/3$
1000	248	0.248 $\approx 1/4$
10,000	1978	0.1978 $\approx 1/5$
100,000	16,702	0.16702 $\approx 1/6$

As the table shows, the fraction of values of t not eliminated by these results only slowly approaches 0 — apparently like $1/\log M$.

These results lend strong support to the following conjecture:

Conjecture 3.11. *There do not exist any abelian* $\left(2t(t+1)+1, t^2, t(t-1)/2\right)$*-difference sets for* $t \geq 3$.

I would not necessarily conjecture the non-existence of non-abelian difference sets, since much less is known about these than abelian difference sets, and for other parameters non-abelian difference sets have been found where abelian difference sets do not exist.

4. AUTOCORRELATIONS OF FINITE BINARY SEQUENCES

4.1. Autocorrelations

The study of correlations of binary sequences has important applications in digital communications and radar signal design. For example, see [Go], [SP], and [T]. The basic idea is that a signal in the form of a finite sequence of 1's and -1's (or of 0's and 1's) is transmitted, and it is desired that it should not closely resemble other such sequences or time-shifted versions of itself. A nice way of computing such a resemblance is with a *correlation* function. A correlation of one sequence with another is called a *crosscorrelation.* However, in this chapter we concern ourselves with *autocorrelations.* These are of use, for instance, when a signal can reach its destination by several different paths at once (as in the case of radio signals), creating so-called multipath noise. Since some of these signals can arrive with a time-lag compared to the others, there may be interference between the signal and time-shifted versions of itself. It is desired to keep this to a minimum, and this in turn means keeping the autocorrelation function small.

In fact, we define two autocorrelation functions. Most of the terminology follows [EK]. Let $x_1, \ldots, x_v$ be a binary sequence (each $x_i = \pm 1$).

DEFINITIONS. For $1 \leq r \leq v-1$, we define the r^{th} *aperiodic correlation* of the sequence to be

$$c_r = \sum_{i=1}^{v-r} x_i x_{i+r},$$

and the r^{th} *periodic correlation* to be

$$p_r = \sum_{i=1}^{v} x_i x_{i+r},$$

where the subscripts are read modulo v.

The following simple relations hold:

$$p_r = c_r + c_{v-r}, \qquad p_r \equiv v \pmod 4. \tag{4.1}$$

We now show a connection between binary sequences and cyclic difference sets. To every binary sequence there corresponds a subset D of the cyclic group $\mathbf{Z}_v = \{1, 2, \ldots, v\}$ (and vice versa), given by $D = \{i : x_i = -1\}$. For example, the sequence $--+-+++$ corresponds to the subset $D = \{1, 2, 4\}$ of $\mathbf{Z}_7$.

We then have the following equivalence:

$$p_r = \gamma \text{ a constant } \forall r \iff D \text{ is a } (v, k, \lambda)\text{-difference set in } \mathbf{Z}_v \text{ with } \gamma = v - 4n.$$

If in this case $\gamma = -1, 0$,or 1, then we call the sequence a *periodic Barker sequence.* If $\gamma = 0$, it is also called a *perfect binary sequence.*

DEFINITION. A *Barker sequence* has $|c_r| \leq 1$ for $1 \leq r \leq v - 1$.

Every Barker sequence is in fact a periodic Barker sequence, with γ determined by v mod 4 (see [TS]; this follows from the relations (4.1).)

That is, "Barker sequence of length v" $\implies$ "cyclic (v, k, λ)- difference set with $v - 4n = \gamma = -1, 0$, or 1."

For example, $--+-+++$ is a periodic Barker sequence with $\gamma = -1$ but is not a Barker sequence since $c_5 = -2$. On the other hand, $+++--+-$ is a (true) Barker sequence since $c_r = 0$ or -1 for every r.

Turyn and Storer showed in [TS] that Barker sequences of odd length v can only exist for $v = 3, 5, 7, 11, 13$. The only known Barker sequences of even length occur at $v = 2, 4$. It is conjectured that there are no others. A stronger conjecture is that are no perfect binary sequences of even length greater than 4; this is equivalent to the conjecture that there are no non-trivial cyclic $(4u^2, 2u^2 - u, u^2 - u)$-difference sets.

In the next section we prove a general bound on the aperiodic autocorrelations of a periodic Barker sequence.

4.2. Bound on c_r for Periodic Barker Sequences

We assume we have a periodic Barker sequence $x_1, \ldots, x_v$ with $p_r = \gamma = v - 4n$, a constant, for $1 \leq r \leq v-1$.

For now, consider only the case $\gamma = 0$. Then the following inequality is easy to prove: $|c_r| \leq 2n$ for all r. This is because $|c_r| \leq 4n - r$ by the triangle inequality, and $c_r + c_{4n-r} = p_r = 0$, so $|c_r| \leq \min\{r, 4n-r\} \leq 2n$. We improve this to:

Theorem 4.1. *$|c_r| \leq \frac{3}{2}n$ for all r.*

Proof. Fix $r \neq v/2$. (Note that $c_{v/2} = 0$ necessarily.) Define

$$c_r(a) = \sum_{i=1+a}^{v-r+a} x_i x_{i+r} \qquad \text{for } a = 1, \ldots, v$$

where here and everywhere else subscripts should be read modulo v. This is the r^{th} aperiodic correlation of the sequence "rotated" by a places (which corresponds to a translate of the cyclic difference set in $\mathbf{Z}_v$; see the table in the Appendix for a list of aperiodic correlations of the translates of the $(13, 4, 1)$-difference sets.)

We first have

FACT 1. $$\sum_{a=1}^{v} c_r(a) = \sum_{a=1}^{v} \sum_{i=1+a}^{v-r+a} x_i x_{i+r} = (v-r) \sum_{i=1}^{v} x_i x_{i+r} = (v-r)p_r = 0.$$

Now define

$$\begin{aligned} \delta_r(a) &= c_r(a) - c_r(a-1) \\ &= \sum_{i=a+1}^{v-r+a} x_i x_{i+r} - \sum_{i=a}^{v-r+a-1} x_i x_{i+r} \\ &= x_{v-r+a} x_a - x_a x_{a+r} \\ &= x_a (x_{a-r} - x_{a+r}). \end{aligned}$$

So

$$\delta_r(a) = \begin{cases} \pm 2, & \text{if } x_{a-r} \neq x_{a+r}; \\ 0, & \text{if } x_{a-r} = x_{a+r}. \end{cases} \tag{4.2}$$

Let

$$\alpha = |\{a : \delta_r(a) = 0\}|, \qquad \beta = |\{a : \delta_r(a) \neq 0\}|.$$

So $\alpha + \beta = v = 4n$.

Now (4.2) $\Longrightarrow \alpha - \beta = \sum_{a=1}^{v} x_{a-r}x_{a+r} = \sum_{j=1}^{v} x_j x_{j+2r} = p_{2r} = 0.$

Therefore $\alpha = \beta = 2n$.

Also clearly $\sum_{a=1}^{v} \delta_r(a) = \sum_{a=1}^{v}(c_r(a) - c_r(a-1)) = 0$, so

FACT 2. $$|\{a : \delta_r(a) = +2\}| = |\{a : \delta_r(a) = -2\}| = n$$
$$|\{a : \delta_r(a) = 0\}| = 2n.$$

Now let $c = c_r = c_r(v)$, for convenience. So the sequence $c_r(1), c_r(2), \ldots, c_r(v)$ is given by

$$c + \delta_r(1),\ c + \delta_r(1) + \delta_r(2),\ \ldots,\ c + \delta_r(1) + \cdots + \delta_r(v) = c.$$

Thus FACT 1 implies

$$vc + v\delta_r(1) + (v-1)\delta_r(2) + \cdots + 2\delta_r(v-1) + \delta_r(v) = 0$$

which implies

$$vc = -[v\delta_r(1) + \cdots + \delta_r(v)].$$

So finally FACT 2 guarantees that

$$\begin{aligned} |vc| &\leq +2[(v) + (v-1) + \cdots + (v-n+1)] - 2[n + (n-1) + \cdots + 1] \\ &= 2[3n]n \qquad\qquad \text{since } v = 4n \\ &= 6n^2, \end{aligned}$$

which implies

$$|c| \leq \frac{3}{2}n,$$

as claimed. □

An analogous argument in general ($r \neq v/2$, and $v = 4n + \gamma$) gives the bounds

$$-\frac{3}{2}n + \gamma - \frac{(\frac{1}{2}n + r)\gamma}{4n + \gamma} \leq c_r \leq \frac{3}{2}n + \gamma + \frac{(\frac{1}{2}n - r)\gamma}{4n + \gamma}.$$

Indeed, FACT 1 becomes

$$\sum_{a=1}^{v} c_r(a) = (v - r)p_r = (v - r)\gamma,$$

and FACT 2 becomes

$$|\{a : \delta_r(a) = +2\}| = |\{a : \delta_r(a) = -2\}| = n$$
$$|\{a : \delta_r(a) = 0\}| = 2n + \gamma,$$

and the rest of the proof is similar to that of Theorem 4.1.

Unfortunately this bound suffers from being too general and weak. It would be desirable to show that given a periodic Barker sequence, there *exists* a sequence with very good (small) aperiodic correlations. In particular, if the existence of a Barker sequence could be deduced from that of a periodic Barker sequence this would be a big step in showing the non-existence of the corresponding cyclic difference sets. Indeed, in the case of $v = 4n + 1$, the result of [TS] would show the non-existence of a cyclic difference set with parameters (3.1).

5. CONSTRUCTION OF SYMMETRIC DESIGNS

5.1. A.E. Brouwer's Symmetric Designs

In this chapter we return to general symmetric designs. As mentioned in the Introduction, A.E. Brouwer has constructed symmetric designs in [Br] of which the $v = 4n + 1$ designs are a special case (these designs were first known to R.M. Wilson, as pointed out by Brouwer). Brouwer's construction is given in terms of the *incidence matrices* of symmetric designs; an incidence matrix is a $(0, 1)$-matrix with rows indexed by the points, columns indexed by the blocks, and a "1" in row x and column B if and only if $x \in B$. We present a different formulation of the construction, suggested by Wilson, using the designs themselves. For this construction we need to use several different types of structures, so we begin by introducing these ingredients.

Hadamard 2-designs were described in the Introduction as $(4n-1, 2n-1, n-1)$-symmetric designs. We remark here that if q is an odd prime power, then Hadamard 2-designs with parameters $(2q + 1,\ q,\ (q - 1)/2)$ are known to exist (see Chapter 18 of [vLW]).

Another type of BIBD can be found in the *affine geometry* $AG(h, q)$ which is any h-dimensional vector space over the finite field $\mathbf{F}_q$ along with its subspaces. The point set simply consists of the q^h points of $AG(h, q)$, and the blocks are the hyperplanes (cosets of the $(h - 1)$-dimensional subspaces), with the incidence relation being inclusion of the points in the hyperplanes. Any two distinct points lie in exactly $(q^{h-1} - 1)/(q - 1)$ blocks. Notice that the blocks of this BIBD can be naturally partitioned into *parallel classes* of mutually disjoint blocks.

Now the dual of the affine points and hyperplanes design in $AG(h, q)$ is a structure called a *λ-transversal design* (see [BJL]). Its points are partitioned into equivalence classes commonly, but confusingly, called "*groups*," each of size q. Two points in the same "group" do not lie on a common block. This λ-transversal design

has

$$\frac{q(q^h-1)}{(q-1)} \text{ points}$$

$$\frac{(q^h-1)}{(q-1)} \text{ points per block}$$

$$\frac{(q^{h-1}-1)}{(q-1)} \text{ points in any two distinct blocks}$$

$$q^h \text{ blocks}$$

$$q^{h-1} \text{ blocks on any one point}$$

$$q^{h-2} \text{ blocks on any two points from distinct "groups."}$$

Note that consequently any block intersects each "group" in exactly one point.

Finally, we need a *balanced weighing matrix*, denoted $BW(w,m)$. This is a $w \times w$ $(0,1,-1)$-matrix $M = ((m_{ij}))$ that satisfies $MM^t = mI$ and whose "underlying" $(0,1)$-matrix $((|m_{ij}|))$ is the incidence matrix of a $(w,\ m,\ \lambda)$-symmetric design. In other words, it is the incidence matrix of a symmetric design that has been "signed" in such a way that distinct rows are orthogonal. When $w = (q^h-1)/(q-1)$ and $m = q^{h-1}$, then the complement of the points and hyperplanes design of the so-called *projective geometry* $PG(h-1,q)$ is a $(w,\ q^{h-1},\ q^{h-1}-q^{h-2})$-symmetric design which is known to have a "decomposition" of its incidence matrix into a balanced weighing matrix (see [GS]).

Theorem 5.1. *Let q be an odd prime power and let $h \geq 1$. Then there exist symmetric designs with parameters*

$$v = 2q\frac{(q^h-1)}{(q-1)} + 1, \quad k = q^h, \quad \lambda = \frac{1}{2}q^{h-1}(q-1).$$

(Note: $h = 2$ gives the parameters (1.4) of $v = 4n+1$ designs.)

Proof. Let $w = (q^h-1)/(q-1)$. First, take w many Hadamard 2-designs with parameters $(2q+1,\ q,\ (q-1)/2)$. Call them (and by abuse, their point sets also) $X_1, \ldots, X_w$ and identify them at a point ∞. That is, let $X_i \cap X_j = \{\infty\}$ for all $i \neq j$. Let $X := \cup_{i=1}^{w} X_i$; this will be the point set of the (v,k,λ) design $\mathcal{D}$.

Let $\{A_j^{(i)} : 1 \leq j \leq q\}$ be the blocks of X_i that contain the point ∞.

Let $\{B_j^{(i)} : 1 \leq j \leq q+1\}$ be the blocks of X_i that do *not* contain ∞.

Now we will construct the blocks of $\mathcal{D}$ that contain ∞. We will use the dual of the affine points and hyperplanes design in $AG(h,q)$, which is a λ-transversal design as described above.

Impose the structure of this design on the set of objects $\{A_j^{(i)} : 1 \leq i \leq w,\ 1 \leq j \leq q\}$ such that the "groups" of the transversal design are exactly the sets $\{A_j^{(i)} : 1 \leq j \leq q\}$, for $i = 1, \ldots, w$. So each block of the transversal design consists of w different $A_j^{(i)}$'s (one for each i). Form a block of $\mathcal{D}$ for each block L of the transversal design by letting $\mathcal{A}_L$ be the union of the $A_j^{(i)}$'s that lie on L. We thus get q^h blocks $\mathcal{A}_L$, each of size $(q-1)w + 1 = q^h$, that contain the point ∞.

Now we must describe the blocks of $\mathcal{D}$ that do not contain ∞. For this part we need a balanced weighing matrix $BW(w, q^{h-1})$, called $M = ((m_{ij}))$.

Define the following notation:

$$(+1)B_j^{(i)} := B_j^{(i)},$$
$$(-1)B_j^{(i)} := (X_i \backslash \{\infty\}) \backslash B_j^{(i)},$$
$$(0)B_j^{(i)} := \emptyset.$$

Then for each $1 \leq j \leq q+1, \quad 1 \leq t \leq w$ we define the block $\mathcal{B}_{jt}$ of $\mathcal{D}$ as follows:

$$\mathcal{B}_{jt} := \cup_{i=1}^{w} m_{it} B_j^{(i)}.$$

We now check that there are v blocks of $\mathcal{D}$, that they all have the right size, and that any two of them intersect in the right number of points. By Theorem 19.10 of [vLW], this suffices to prove that the structure is a symmetric design.

To begin with, there are $q^h = (q-1)w + 1$ blocks $\mathcal{A}_L$ and $(q+1)w$ blocks $\mathcal{B}_{jt}$, for a total of $2qw + 1 = v$ blocks.

As mentioned above, the blocks $\mathcal{A}_L$ each have size $k = q^h$. To find the size of a $\mathcal{B}_{jt}$, we note that $\left|(+1)B_j^{(i)}\right| = \left|(-1)B_j^{(i)}\right| = q$ and that for each t exactly q^{h-1} values of i give non-zero m_{it}, so $\left|\mathcal{B}_{jt}\right| = q^{h-1}q = q^h = k$.

Consider two blocks of $\mathcal{D}$ of the form $\mathcal{A}_{L_1}$ and $\mathcal{A}_{L_2}$ for distinct blocks L_1 and L_2 of the transversal design. Their intersection is the union over $1 \le i \le w$ of $A_{j_1}^{(i)} \cap A_{j_2}^{(i)}$. This latter intersection has size q if $A_{j_1}^{(i)} = A_{j_2}^{(i)} \in L_1 \cap L_2$, and size $(q-1)/2$ otherwise. Since $|L_1 \cap L_2| = (q^{h-1}-1)/(q-1)$, and taking into account the common point ∞, we find that $\left|\mathcal{A}_{L_1} \cap \mathcal{A}_{L_2}\right| = (q-1)(q^{h-1}-1)/(q-1) + \big((q-1)/2-1\big)\big((q^h-q^{h-1})/(q-1)\big) + 1 = q^{h-1}(q-1)/2 = \lambda$.

Now consider two blocks of $\mathcal{D}$ of the form $\mathcal{B}_{j_1 t}$ and $\mathcal{B}_{j_2 t}$ for $j_1 \ne j_2$. Their intersection is the union of $m_{it}B_{j_1}^{(i)} \cap m_{it}B_{j_2}^{(i)}$ over $1 \le i \le w$. But these latter intersections have size $(q-1)/2$ for $m_{it} = \pm 1$, so $\left|\mathcal{B}_{j_1 t} \cap \mathcal{B}_{j_2 t}\right| = q^{h-1}(q-1)/2 = \lambda$.

Two blocks $\mathcal{B}_{j_1 t_1}$ and $\mathcal{B}_{j_2 t_2}$ with $t_1 \ne t_2$ correspond to two distinct columns of the balanced weighing matrix $M = ((m_{ij}))$. As above, $m_{it_1}B_{j_1}^{(i)} \cap m_{it_2}B_{j_2}^{(i)}$ has size $(q-1)/2$ if $m_{it_1} = m_{it_2} \ne 0$; it has size $q-(q-1)/2 = (q+1)/2$ if $m_{it_1} = -m_{it_2} \ne 0$. Because M is a $BW(w, q^{h-1})$, these cases each occur for half of the number of times that $m_{it_1}m_{it_2} \ne 0$, that is, $(q^{h-1}-q^{h-2})/2$ times. So $\left|\mathcal{B}_{j_1 t_1} \cap \mathcal{B}_{j_2 t_2}\right| = (q-1)(q^{h-1}-q^{h-2})/4 + (q+1)(q^{h-1}-q^{h-2})/4 = (q^h - q^{h-1})/2 = \lambda$.

Finally, we consider two blocks of the form $\mathcal{B}_{jt}$ and $\mathcal{A}_L$. For $1 \le i \le w$, the set $A_l^{(i)} \cap m_{it}B_j^{(i)}$ has size $(q-1)/2$ if $m_{it} = \pm 1$ (because $\infty \notin (-1)B_j^{(i)}$), so $\left|\mathcal{A}_L \cap \mathcal{B}_{jt}\right| = q^{h-1}(q-1)/2 = \lambda$. □

We make one more interesting observation. It is known (see [GS]) that a necessary condition for a $BW(v,k)$ to exist when v is odd is that k is a perfect square, and if the $BW(v,k)$ is *regular* (i.e., has a constant number of -1's per row) then λ is even. But the parameters of the $v = 4n+1$ designs given by (1.4), i.e., the case $h = 2$ of Theorem 5.1, have the property that k is always a square both for the design and its complement, and either the design or its complement have λ even. This leads to the question of whether or not the incidence matrices of these designs can be signed to produce balanced weighing matrices. To the best of my knowledge, this has not yet been done.

APPENDIX

Aperiodic Autocorrelations of Periodic Barker Sequences of Length 13

The table on the next page is a listing of the aperiodic autocorrelations c_r for the periodic Barker sequences of length 13, that is, the cyclic $(13, 4, 1)$-difference sets under the correspondence described in Section 4.1. In the left column are the cyclic $(13, 4, 1)$-difference sets; in each of the two groupings the difference sets are translates of each other. That is, they correspond to *rotations* of the first sequence. For each r, the value of c_r is listed for the corresponding periodic Barker sequence. For example, the difference set $\{0, 1, 3, 9\}$ corresponds to the binary sequence

$$--+-++++++-+++.$$

The translate $\{1, 2, 4, 10\}$ corresponds to the cyclic rotation of the first sequence by one position:

$$+--+-++++++-++.$$

Observe that $c_r + c_{v-r} = +1$ always (where $v = 13$), and that within each grouping the sum of the entries in the r^{th} column is $v - r$, as explained in the remarks following the proof of Theorem 4.1.

Table A.1

r =	1	2	3	4	5	6	7	8	9	10	11	12
$\{0,1,3,9\}$	2	3	2	1	0	3	-2	1	0	-1	-2	-1
$\{1,2,4,10\}$	0	1	4	-1	0	3	-2	1	2	-3	0	1
$\{2,3,5,11\}$	0	1	2	-1	-2	3	-2	3	2	-1	0	1
$\{3,4,6,12\}$	2	1	0	-3	-2	1	0	3	4	1	0	-1
$\{4,5,7,0\}$	2	1	0	-1	0	-1	2	1	2	1	0	-1
$\{5,6,8,1\}$	0	1	0	-1	0	-3	4	1	2	1	0	1
$\{6,7,9,2\}$	0	-1	0	1	0	-3	4	1	0	1	2	1
$\{7,8,10,3\}$	0	-1	0	1	2	-1	2	-1	0	1	2	1
$\{8,9,11,4\}$	0	1	0	1	4	-1	2	-3	0	1	0	1
$\{9,10,12,5\}$	2	1	2	3	2	-1	2	-1	-2	-1	0	-1
$\{10,11,0,6\}$	2	-1	0	3	2	1	0	-1	-2	1	2	-1
$\{11,12,1,7\}$	2	1	0	3	2	3	-2	-1	-2	1	0	-1
$\{12,0,2,8\}$	0	3	0	3	0	3	-2	1	-2	1	-2	1
$\{0,2,6,5\}$	2	1	2	1	0	1	0	1	0	-1	0	-1
$*\{1,3,7,6\}$	0	1	0	1	0	1	0	1	0	1	0	1
$\{2,4,8,7\}$	0	-1	0	-1	2	3	-2	-1	2	1	2	1
$\{3,5,9,8\}$	0	-1	-2	1	2	3	-2	-1	0	3	2	1
$\{4,6,10,9\}$	0	-1	0	1	2	1	0	-1	0	1	2	1
$\{5,7,11,10\}$	0	1	2	1	0	3	-2	1	0	-1	0	1
$\{6,8,12,11\}$	2	3	2	1	2	1	0	-1	0	-1	-2	-1
$\{7,9,0,12\}$	0	3	2	-1	2	-1	2	-1	2	-1	-2	1
$\{8,10,1,0\}$	2	3	0	-1	0	-1	2	1	2	1	-2	-1
$\{9,11,2,1\}$	0	3	0	1	0	-1	2	1	0	1	-2	1
$\{10,12,3,2\}$	2	1	0	1	0	-1	2	1	0	1	0	-1
$\{11,0,4,3\}$	2	-1	2	3	0	-1	2	1	-2	-1	2	-1
$\{12,1,5,4\}$	2	-1	2	1	-2	-1	2	3	0	-1	2	-1

$*$ Notice that this corresponds to a (true) "Barker sequence". The binary sequence here is:

$$+-+-++--+++++.$$

REFERENCES

[AK] E.F. ASSMUS, JR. AND J.D. KEY, Designs and their Codes. Camb. Tracts in Math., Vol. 103, Cambridge University Press, 1992.

[BJL] T. BETH, D. JUNGNICKEL, AND H. LENZ, Design Theory. Cambridge University Press, 1986.

[BHH] W.G. BRIDGES, M. HALL, AND J.L. HAYDEN, *Codes and Designs*, Jour. Comb. Theory, Series A, 31 (1981), pp.155–174.

[B] W.J. BROUGHTON, *A Note on Table I of "Barker Sequences and Difference Sets,"* L'Ens. Math., 40 (1994), pp.105–107.

[Br] A.E. BROUWER, *An Infinite Series of Symmetric Designs*, Stichting Mathematisch Centrum (Amsterdam), ZW 202/83.

[CvL] P.J. CAMERON AND J.H. VAN LINT, Graphs, Codes and Designs. Lond. Math. Soc. Lect. Note Series, Vol. 43, Cambridge University Press, 1980.

[D] H. DAVENPORT, Multiplicative Number Theory, 2nd ed. Graduate Texts in Math. Vol. 74, Springer-Verlag, 1980.

[EK] S. ELIAHOU AND M. KERVAIRE, *Barker Sequences and Difference Sets*, L'Ens. Math., 38 (1992), pp.345–382.

[G] C.F. GAUSS, *Theoria Residuorum Biquadraticorum, Commentatio secunda*, (Apr. 1831), in Carl Friedrich Gauss Werke, Band 2. Königlichen Gesellschaft der Wissenschaften, Göttingen, 1876.

[GS] A.V. GERAMITA AND J. SEBERRY, Orthogonal Designs: Quadratic Forms and Hadamard Matrices. Lect. Notes in Pure and Appl. Math., Vol.45, Marcel Dekker, 1979.

[Go] S.W. GOLOMB, *Construction of Signals with Favourable Correlation Properties*, in Surveys in Combinatorics, 1991 (A.D. Keedwell, ed.). Lond. Math. Soc. Lect. Note Series, Vol. 166, Cambridge University Press, 1991, pp.1–39.

[H1] M. HALL, JR., *Cyclic Projective Planes*, Duke Jour. Math., 14 (1947), pp.1079–1090.

[H2] M. HALL, JR., Combinatorial Theory, 2nd ed. Blaisdell Publishing Company, 1986.

[HP] D.R. HUGHES AND F.C. PIPER, Design Theory. Cambridge University

Press, 1985.

[IR] K. IRELAND AND M. ROSEN, A Classical Introduction to Modern Number Theory, 2nd ed. Graduate Texts in Math. Vol. 84, Springer-Verlag, 1990.

[J] D. JUNGNICKEL, *Difference Sets*, in Contemporary Design Theory: A Collection of Surveys (J.H. Dinitz and D.R. Stinson, eds.). Wiley-Interscience, John Wiley & Sons, 1992, pp.241–324.

[L] E.S. LANDER, Symmetric Designs: An Algebraic Approach. Lond. Math. Soc. Lect. Note Series, Vol. 74, Cambridge University Press, 1983.

[M] P.K. MENON, *Difference Sets in Abelian Groups*, Proc. Amer. Math. Soc., 11 (1960), pp.368–376.

[Mc] R.L. MCFARLAND, On Multipliers of Abelian Difference Sets. Ph.D. thesis, Ohio State University, 1970.

[SP] D.V. SARWATE AND M.B. PURSLEY, *Crosscorrelation Properties of Pseudorandom and Related Sequences*, Proc. IEEE, 68 (1980), pp.593–619.

[S] J.P. SERRE, A Course in Arithmetic. Graduate Texts in Math. Vol. 7, Springer-Verlag, 1973.

[Sm] K.W. SMITH, *Non-abelian Hadamard Difference Sets*, Jour. Comb. Theory, Series A, 70 (1995), pp.144–156.

[Ste] J. STEINER, *Combinatorische Aufgabe*, Jour. Reine Angew. Math., 45 (1853), pp.181–182.

[St] D.R. STINSON, *Combinatorial Designs and Cryptography*, in Surveys in Combinatorics, 1993 (K. Walker, ed.). Lond. Math. Soc. Lect. Note Series, Vol. 187, Cambridge University Press, 1993, pp.257–287.

[T] R. TURYN, *Sequences with Small Correlation*, in Error Correcting Codes (H.B. Mann, ed.). John Wiley & Sons, 1968, pp.195–228.

[TS] R. TURYN AND J. STORER, *On Binary Sequences*, Proc. A.M.S., 12 (1961), pp.394–399.

[vLW] J.H. VAN LINT AND R.M. WILSON, A Course in Combinatorics. Cambridge University Press, 1992.

[Y] F. YATES, *Incomplete Randomized Blocks*, Annals of Eugenics, 7 (1936), pp.121–140.