CODES AND POLYNOMIALS IN THE STUDY OF CYCLIC DIFFERENCE SETS

Thesis by

Thomas E Norwood

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California

1996

(Submitted May 28, 1996)

Acknowledgements

I wish to thank R.M. Wilson for his unfailing support and guidance throughout my time at Caltech. In addition, I would like to thank all of the people who have helped make this thesis possible through many stimulating discussions. Among those who have made important contributions to the ideas that led to this work are Hunter Snevily, John Blanchard and Wayne Broughton.

Abstract

Let Π_q be the Desarguesian projective plane of order $q = 2^m$. We define an incidence structure as follows. Let $\mathcal{O}$ be a regular oval in Π_q and let $\mathcal{P}$ be the set of exterior points of $\mathcal{O}$. For each $p \in \mathcal{P}$ define B_p to be the sum $(mod\ 2)$ of the exterior blocks through p. Then the B_p are the blocks of a $(q^2 - 1, q^2/2, q^2/4)$ cyclic difference set which we denote $M(q^2)$. It was conjectured by Assmus and Key in [ass3] and [ass1] that $rank_2(C_2(M(q^2))) = m2^{m-1}$. The goal of this paper is to give a proof of that conjecture as well as to discuss certain related results which are suggested by it or by its proof.

There are three central theorems in this paper. The first is theorem 2.2.3: $rank_2(C_2(M(q^2))) = m2^{m-1}$, resolving the conjecture of Assmus and Key. Although the proof of this theorem does not directly involve the cyclic nature of $M(q^2)$, we do utilize some results and a construction of Jackson [jac] on designs with $PSL_2(q)$ acting transitively. Thus, it is of interest to us to undertake a further study of Jackson's construction and its relation to cyclic difference sets. This gives rise to our second major result, that Jackson's construction is equivalent to a classical construction of Gordon, Mills, and Welch [gor]. This is the primary result

of chapter 1 and an immediate consequence is theorem 1.3.5, that $PSL_2(q)$ acts transitively on a Hadamard design D if and only if D arises from the Gordon, Mills, Welch construction. Another particularly interesting consequence of the equivalence of the two constructions is that although the designs $M(q^2)$ and a certain family of the Gordon, Mills, Welch designs are isomorphic, this has apparently not been noticed until now even though both families have been widely studied. The third major theorem of this paper is theorem 3.1.1 which characterizes the generator polynomial of the binary code of $M(q^2)$ by explicitly giving its roots. The proof of this theorem comprises the bulk of chapter 3. The most important application of this theorem is that it allows us to study the code $C_2(M(q^2)))$ as a cyclic code. That is, we may immediately determine, from the roots, exactly which cyclic codes are subcodes of $C_2(M(q^2)))$. In particular, we address the question of whether it contains a cyclic punctured first-order Reed Muller code in theorem 3.2.1. This question was also posed by Assmus and Key in [ass1], and [ass3].

Finally, in chapter 4, we discuss a generalization of the results of the earlier chapters. Specifically, let $C_{rep}(v)$ be the subcode of $\mathbf{F_2^v}$ generated by repetition vectors (i.e. vectors of the form $(\mathbf{c}, \mathbf{c}, \ldots, \mathbf{c})$). If $v = 2^m - 1$, a cyclic code is a subcode of $C_{rep}(v)$ if and only if it does not contain a cyclic punctured first-order Reed Muller code. For this reason, we propose that the question of containment in $C_{rep}(v)$ is of interest for the code of any cyclic difference set, not just those with $v = 2^m - 1$. In chapter 4, we address this question in the case of all known cyclic

Hadamard difference sets, as well as the Singer difference sets. In the latter case, the codes are given by generalized Reed Muller codes, so we determine the relation of these codes to $C_{rep}(v)$.

Table of Contents

0 Introduction

We begin with some basic definitions and concepts from design and coding theory. This section is included mainly for the purpose of standardizing notation and reviewing the relevant topics. For the reader who is unfamiliar with these areas, see [lin], [mac], or [ass1].

0.1 Symmetric Designs and Cyclic Difference Sets

Let $\mathcal{P}$, $\mathcal{B}$ be finite sets. The elements of $\mathcal{P}$ will be called *points* the elements of $\mathcal{B}$ will be called *blocks*. An *incidence structure* is determined by a subset $\mathcal{F}$ of $\mathcal{P} \times \mathcal{B}$ called the flags. If $(p, B) \in \mathcal{F}$ we say p and B are *incident*. Let D be an incidence structure which satisfies:

(1) $|\mathcal{P}| = v$.

(2) *If $B \in \mathcal{B}$, then B is incident with exactly k points.*

(3) *If $S \subseteq \mathcal{P}$ with $|S| = t$, then there are exactly λ blocks incident with every element of S.*

We then say D is a $t - (v, k, \lambda)$ *design*. it is easy to see that the number of blocks incident with a given point is a constant, say r. We will also write $|\mathcal{B}| = b$.

In case $v = b$ (and hence $k = r$) we will say that D is a *Symmetric Design.* It can be shown that this implies that $t = 2$, and we will use the notation (v, k, λ) *design* to refer to a symmetric design. One construction for Symmetric Designs is by using a *Difference Set.* Let G be a (finite) group with $|G| = v$ and let D be a subset of G which satisfies:

(1) $|D| = k$

(2) *Each nonidentity element of* G *occurs exactly* λ *times in the list* $[gh^{-1} : g, h \in D]$

We then say D is a (v, k, λ) *difference set* in G. In this case, the structure with $\mathcal{P} = G$ and $\mathcal{B}$ given by the translates of D is a (v, k, λ) symmetric design. Our primary concern will be in the case when G is cyclic in which case we will call D a *Cyclic Difference Set.*

Let D be a subset of the cyclic group $\mathbf{Z}_v = \{0, 1, 2, \ldots, v-1\}$. We will associate with D a polynomial $\theta \in \mathbf{Z}[x]$ *mod* $(x^v - 1)$ called the *Hall Polynomial* of D. θ is given by:

$$\theta(x) = \sum_{i=0}^{v-1} a_i x^i \qquad \text{where} \qquad a_i = \begin{cases} 1 & \text{if } i \in D \\ 0 & \text{else} \end{cases}$$

By definition, D is a difference set if and only if

$$\theta(x)\theta(x^{-1}) = (k - \lambda) + \lambda(1 + x + x^2 + \cdots + x^{v-1}) \pmod{x^v - 1}$$

0.2 Cyclic Codes

A code of length n is a subspace of the vector space $\mathbf{F_q^n}$ endowed with the Hamming Metric: $d(\mathbf{x}, \mathbf{y})$ is the number of coordinates in which $\mathbf{x}$ and $\mathbf{y}$ differ. The vectors are called *codewords*. The *weight* of a codeword $\mathbf{x}$ is $d(\mathbf{0}, \mathbf{x})$. A matrix whose rows generate C is called a *generator matrix* for C. Two codes are said to be *isomorphic* if one can be obtained from the other by a permutation of the coordinates. The *automorphism group* of C is that group of permutations of the coordinates which fix C as a set (i.e. which map codewords to codewords). We define $C^{\perp} = \{y : y \cdot x = 0 \ for \ all \ x \in C\}$. Notice $dim(C) + dim(C^{\perp}) = n$. A generator matrix for $C^{\perp}$ is called a *parity check matrix* for C. We define the *weight enumerator* of C by

$$W_C(x, y) = \sum_{c \in C} x^{n-wt(c)} y^{wt(c)}$$

Suppose C has M codewords and that C is a vector space over $\mathbf{F_q}$. We then have the following formula called the MacWilliams Relations:

$$W_{C^{\perp}}(x, y) = \frac{1}{M} W_C(x + (q-1)y, x - y)$$

If $C = C^{\perp}$ we will say C is *self dual*. Otherwise, we will call $C^{\perp}$ the *orthogonal* of C.

A *cyclic code* may be broadly defined as a code of length v whose automorphism group contains a cycle of length v. However, we will be more specific and say that a code is cyclic if and only if it satisfies:

$$(c_0, c_1, \ldots, c_{v-1}) \in C \implies (c_{v-1}, c_0, \ldots, c_{v-2}) \in C$$

Now, to each codeword $(c_0, c_1, \ldots, c_{v-1})$ we associate the polynomial $\sum_{k=0}^{(v-1)} c_k x^k$. Notice that the cyclic shift above corresponds to multiplication by x $(mod\ x^v - 1)$. If we then let $\mathbf{R_v(q)}$ be the ring of polynomials with coefficients in $\mathbf{F_q}$ modulo $x^v - 1$, cyclic codes over $\mathbf{F_q}$ are in one to one correspondence with ideals in $\mathbf{R_v(q)}$. As such each cyclic code is generated by a single polynomial. Given a cyclic code C, there is a unique monic polynomial of least degree among all polynomials which generate C called the *generator polynomial* of C. If $g_i(x)$ is the generator polynomial of C_i $(i = 1, 2)$, we have

(1) $g_i(x)$ *divides* $x^v - 1$

(2) $dim(C_i) = v - deg(g_i(x))$

(3) $g_1 | g_2$ *if and only if* $C_1 \supseteq C_2$

Now, let C be a cyclic code of length v and suppose v and q are relatively prime (in our case, v will usually be $q^n - 1$ for some n). The roots of $x^v - 1$ over some extension field are precisely the v^{th} roots of unity in that field. Thus, each monic divisor $g(x)$ of $x^v - 1$ (i.e. each generator polynomial of a cyclic code) may be associated with a set $S \subseteq \{0, 1, \ldots, v-1\}$ such that if α is a primitive v^{th} root of unity, then

$$g(x) = \prod_{i \in S} (x - \alpha^i)$$

One advantage of giving a cyclic code in terms of roots is the *BCH Bound*: Let the cyclic code C be given. Assume that α is a primitive element of $\mathbf{F_{q^2}}$ where $q = 2^m$. Assume also that there is some a so that the distinct elements $\alpha^a, \alpha^{a+1}, \ldots, \alpha^{a+\delta-2}$ are all roots of the generator polynomial of C. Then the

minimum distance of C is at least δ. See [oor] or [mac] for a proof.

Let D be a (v, k, λ) design. Form the matrix $\mathbf{A}$ whose rows are indexed by the blocks of D and whose columns are indexed by the points of D, and with

$$\mathbf{A_{B,p}} = \begin{cases} 1 & \text{if p and B are incident } (p \neq B) \\ 0 & \text{else} \end{cases}$$

The *p-ary code* of D, $C_p(D)$ is defined to be the span of the rows of $\mathbf{A}$. We will almost always assume that 2 divides $k-\lambda$ and consider only the binary code $C_2(D)$.

Notice that if D is a cyclic difference set, then $C_2(D)$ is a cyclic binary code. Assume further that v is odd. Then we may find the generator polynomial of $C_2(D)$ as follows. First, take $\theta(x)$ the Hall polynomial of D and let $\bar{\theta}(x)$ be the same polynomial but with the coefficients now taken to be in $\mathbf{F_2}$ rather than $\mathbf{Z}$ and taken modulo $x^v - 1$. Now, $\bar{\theta}(x)$ generates the cyclic code $C_2(D)$ but may not be the generator polynomial. Let $g(x)$ be the generator polynomial. $g(x)|\bar{\theta}(x)$ since $\bar{\theta}$ is in the ideal generated by g. Moreover, the code must be the smallest cyclic code which contains $\bar{\theta}$. Then applying (1) and (3) above, we see that $g(x) = gcd(\bar{\theta}, x^v - 1)$ which is given by the formula:

$$g(x) = \prod_{i \in S} (x - \alpha^i) \qquad \text{where} \qquad S = \{i : \alpha^i \textit{ is a root of } \bar{\theta} \textit{ over } \mathbf{F_{2^m}}\}$$

0.3 Reed Muller Codes

There are several ways to define the Reed Muller Codes and study their properties. We will give some simple constructions that will be useful in the sequel. For more

on Reed Muller Codes or the equivalence of these constructions, see [mac], [lin], or [ass1].

Consider the $m \times 2^m$ matrix $\mathbf{A}$ whose columns consist of every vector in $\mathbf{F_2}^m$. Now form the matrix

$$\mathbf{R} = \begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ & & \mathbf{A} & & \end{pmatrix} \tag{1}$$

We define the *first-order Reed Muller Code* $R(1,m)$ to be the $\mathbf{F_2}$ span of the rows of $\mathbf{R}$. Clearly, the dimension of this code is $m+1$. $R(1,m)$ may also be defined in the following way. Let the coordinates of the code be labelled by the elements of $\mathbf{F_q}$ where $q = 2^m$. Define a code L as the set of all linear functionals from $\mathbf{F_q}$ to $\mathbf{F_2}$. Then $R(1,m)$ is the code generated by L together with the all ones vector $\mathbf{j}$. In turn, this is equivalent to the code generated by the point-hyperplane incidence vectors in m-dimensional affine geometry over $\mathbf{F_2}$.

Finally, notice that the weight enumerator of $R(1,m)$ is given by:

$$x^{2^m} + (2^{m+1} - 2)x^{2^{m-1}}y^{2^{m-1}} + y^{2^m}$$

we will later need to use the fact that $R(1,m)$ is determined by its weight enumerator. Here is an easy proof:

PROPOSITION 0.3.1: *Let C be a code with the same weight enumerator as $R(1,m)$, then C is isomorphic to $R(1,m)$.*

PROOF: Since C contains the all ones vector, assume C is generated by the rows

of the matrix

$$\begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ & & \mathbf{S} & & \end{pmatrix}$$

For some $m \times 2^m$ matrix $\mathbf{S}$. Now, by the MacWilliams relations,

$$W_{C^\perp}(x,y) = \frac{1}{2^{m+1}}\left[2^{m+1}x^{2^m} + A_4 x^{2^m-4}y^4 + \cdots\right]$$

that is, $C^\perp$ contains no vectors of weight 2. Suppose now that $\mathbf{S}$ had 2 identical columns. The vector with ones in these coordinates and 0 elsewhere would then be in $C^\perp$, so that $C^\perp$ would contain vectors of weight 2. Thus, we conclude that every column of $\mathbf{S}$ is different and therefore, $\mathbf{S}$ differs from the matrix $\mathbf{A}$ of equation (1) only by a permutation of the coordinates □

Now, define the *punctured first-order Reed Muller code*, $R^*(1,m)$ to be the code obtained by removing the coordinate position corresponding to 0 from $R(1,m)$. We may now prove the following:

PROPOSITION 0.3.2: *Let $q = 2^m$. Let α be a primitive element of $\mathbf{F_q}$. Let R be the cyclic code of length $q-1$ whose generator polynomial is the polynomial whose roots are every element of $\mathbf{F_q}$ except $1, \alpha^{-1}, \alpha^{-2}, \alpha^{-4}, \dots, \alpha^{-q/2}$ (i.e., except for 1 and the conjugates of α^{-1}). Then $R \cong R^*(1,m)$.*

PROOF: R has roots $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{q/2-2}$ and thus, by the BCH bound, R must have minimum weight at least $q/2-1$. Consider now the code R_e obtained by adding an overall parity bit to R. Then R_e has minimum weight at least $q/2$. Now,

since 1 is not a root, R contains the code whose generator polynomial has every element except 1 as a root. This code contains only two codewords, the zero vector, and $\mathbf{j}$, the vector of all ones. Thus, R contains $\mathbf{j}$ and it follows that every codeword of R_e has weight 0,q/2, or q. Since R has exactly $m+1$ non-roots, the dimension of R_e is $m+1$. Then by proposition 0.3.1, we have $R_e \cong R(1,m)$ and we have the desired result. □

1 The Family $M(q^2)$

In the three parts of this section, we will discuss a family of difference sets called $M(q^2)$ from three different perspectives. First, we give the simple geometric definition of the family using a regular oval in a Desarguesian projective plane. Second, we review some results of Jackson [jac] which allow us to construct $M(q^2)$ in an alternative manner. Finally, we show that the construction of Jackson is essentially identical to an earlier construction of Gordon, Mills, and Welch [gor] which allows us to compute the Hall polynomial of $M(q^2)$.

1.1 Hadamard Designs, Geometry, $\mathbf{D(q^2)}$, and $\mathbf{M(q^2)}$.

A *Hadamard design* D is a symmetric $(4n-1, 2n, n)$ design. The complementary design $\bar{D}$ has parameters $(4n-1, 2n-1, n-1)$. Moreover, $\bar{D}$ extends to a design with parameters $3-(4n, 2n, n-1)$ which we will denote $\tilde{D}$. The Hadamard designs with these parameters will be said to have *order* n. If n is even, the binary codes of these designs will be related as follows. The code of D denoted $C_2(D)$ is self orthogonal and hence does not contain the all ones vector $\mathbf{j}$. The code of D has codimension 1 in $C_2(\bar{D})$ the difference being that $\mathbf{j} \in C_2(\bar{D})$. $C_2(\bar{D})$ may be extended by an

overall parity bit to obtain the code $C_2(\tilde{D})$. If D is given as a cyclic difference set, the codes may be given by the roots of the generator polynomial. In this case, the difference between $C_2(D)$ and $C_2(\bar{D})$ is the root 1.

From now on, we will write $n = q/4 = 2^{m-2}$. To define the family $D(q)$ of Hadamard designs, we first let the points be the nonzero elements of $\mathbf{F_q}$. The blocks are associated with the linear functionals $L : \mathbf{F_q} \to \mathbf{F_2}$ so that $\gamma \in B_L$ if and only if $L(\gamma) = 1$. The code of $D(q)$ is the code of linear functionals and thus, we have $C_2(\overline{D(q)}) \cong R^*(1, m)$.

A family of designs of order $q^2 = 2^{2m}$ which we will call $M(q^2)$ may be defined by the following simple geometric construction. Let Π be a Desarguesian projective plane of order q. That is Π is the symmetric $(q^2 + q + 1, q + 1, 1)$ design of one- and two-dimensional subspaces of F_q^3. Let $\mathcal{O}$ consist of the points $\{(1, t, t^2) : t \in \mathbf{F_q}\} \bigcup \{(0, 1, 0)\} \bigcup \{(0, 0, 1)\}$. $\mathcal{O}$ is an *oval* in Π, that is, a set of $q + 2$ points such that no 3 are collinear. Blocks of Π meet $\mathcal{O}$ in 0 or 2 points and are called *exterior* or *secant* respectively. Points not on $\mathcal{O}$ are called *exterior points.* The points of $M(q^2)$ are the exterior points. For each exterior point p, we define a block B_p by $B_p = \{q \neq p : \textit{the block through } p \textit{ and } q \textit{ is an exterior block}\}$. It is easily seen that $M(q^2)$ is a symmetric $(q^2 - 1, q^2/2, q^2/4)$ symmetric design, i.e. it has the same parameters as $D(q^2)$. The family $M(q^2)$ has been extensively studied by geometers, see especially the recent work of Maschietti [mas1], [mas2],[mas3], and [mas4]. In [mas1] it is shown using only this definition that $M(q^2) \cong D(q^2)$ if and only if $q = 4$.

We will not give such a proof here, but the result will follow from several of the results in the sequel.

1.2 The Results of Jackson

We will state some of the results in [jac] without proof. The reader may consult this paper for details. Let $\mathbf{M}$ be the matrix whose rows and columns are indexed by the elements of $\mathbf{F_q^2} \setminus (0,0)$. The entry $\mathbf{M_{xy}} = \mathbf{xy^T} = \mathbf{x} \cdot \mathbf{y}$. Let $f : \mathbf{F_q} \to \{0,1\}$. Define $f(\mathbf{M})$ to be the matrix with $\big(f(\mathbf{M})\big)_{\mathbf{xy}} = f(\mathbf{xy^T})$. We then have

CONSTRUCTION 1.2.1 (Jackson [jac]): *Let D be a cyclic Hadamard difference set in $\mathbf{F_q^*}$. Define $f : \mathbf{F_q} \to \{0,1\}$ by $f(x) = 1$ if and only if $x \in D$. Then $f(\mathbf{M})$ is the incidence matrix of a $(q^2-1, q^2/2, q^2/4)$ symmetric design. If two such designs are constructed from D_1 and D_2 they are isomorphic if and only if D_1 is a translate of D_2.*

The main result of Jackson's paper is

THEOREM 1.2.2 (Jackson [jac]): *D is a $(q^2-1, q^2/2, q^2/4)$ design on which $PSL_2(q)$ acts transitively if and only if D arises from construction 1.2.1.*

Notice that as a corollary of theorem 1.2.2, we have that all the designs constructed by Jackson are, in fact, cyclic difference sets. Also, since $PSL_2(q)$ acts as a subgroup of the automorphism group of the projective plane Π which fixes the oval $\mathcal{O}$ (see [dic]), $M(q^2)$ must arise from Jackson's construction. In fact, we have the following

PROPOSITION 1.2.3 *(Jackson [jac]): $D(q^2)$ arises from Jackson's construction with $D = D(q)$. Moreover, $M(q^2)$ arises from Jackson's construction with $D = 1/D(q) = \{1/x \ : \ x \in D(q)\}$.*

1.3 The Hall Polynomial of $\mathbf{M(q^2)}$

We will adopt the following notational conventions throughout the rest of the paper:

NOTATION 1.3.1: *$q = 2^m$. β is a primitive element of $\mathbf{F_q}$. α is a primitive element of $\mathbf{F_{q^2}}$ such that $\beta = \alpha^{q+1}$. $\Theta(x)$ is the Hall polynomial of $D(q^2)$. $\Xi_0(x)$ is the Hall polynomial of $M(q^2)$. $\theta_0(y)$ is the Hall polynomial of $D(q)$. We will also write $y = x^{q+1}$.*

Now, any element of $\mathbf{F_{q^2}}$ may be written uniquely in the form $t_1 + t_2\alpha$ where $t_1, t_2 \in \mathbf{F_q}$. We define the linear functional $L_0 : \mathbf{F_{q^2}} \to \mathbf{F_q}$ by $L_0(t_1 + t_2\alpha) = t_1$. Now, let the columns of $\mathbf{M}$ be ordered $1, \alpha, \alpha^2, \ldots, \alpha^{q-2}$. The rows of $\mathbf{M}$ may then be ordered so that $\mathbf{M}$ is circulant. Let $\mathbf{r}$ be the row corresponding to (1,0) (i.e. $\mathbf{r}$ is the row associated with L_0). Let $\mathbf{x}$ be the vector of the first $q+1$ entries in $\mathbf{r}$. Then $\mathbf{r} = (\mathbf{x}, \beta\mathbf{x}, \beta^2\mathbf{x}, \ldots, \beta^{q-2}\mathbf{x})$. Let $f : \mathbf{F_q} \to \{0,1\}$ with $f(0) = 0$. To find the Hall polynomial of any difference set whose incidence matrix is of the form $f(\mathbf{M})$ (for example $\Xi_0(x)$ or $\Theta(x)$), we must simply find the polynomial associated with $f(\mathbf{r})$. To this end, we define:

$$\phi(y) = \sum_{i=0}^{q-2} a_i y^i \qquad \text{where} \qquad a_i = \begin{cases} 1 & \text{if } f(\beta^i) = 1 \\ 0 & \text{else} \end{cases}$$

$$\Psi(x) = \sum_{i=0}^{q^2-2} b_i x^i \qquad \text{where} \qquad b_i = \begin{cases} 1 & \text{if } f(L_0(\alpha^i)) = 1 \\ 0 & \text{else} \end{cases}$$

$$\Omega_0(x) = \sum_{i=0}^{q^2-2} c_i x^i \qquad \text{where} \qquad c_i = \begin{cases} 1 & \text{if } L_0(\alpha^i) = 1 \\ 0 & \text{else} \end{cases}$$

We then have the following

THEOREM 1.3.2: $\Psi(x) = \Omega_0(x)\phi(y) \ (mod\ x^{q^2-1})$ *where* $y = x^{q+1}$.

PROOF: It suffices to prove the result in the case where ϕ is monomial, so assume that $\phi(y) = y^k$. Then

$$\Omega_0(x)\phi(y) = \sum_{i=0}^{q^2-2} c_i y^k x^i = \sum_{i=0}^{q^2-2} c_i x^{k(q+1)+i}$$

But if $L_0(\alpha^i) = 1$, then $L_0(\alpha^{k(q+1)+i}) = L_0(\beta^k \alpha^i) = \beta^k$. Thus,

$$\Omega_0(x)\phi(y) = \sum_{i=0}^{q^2-2} d_i x^i \qquad (mod\ \ x^{q^2-1} - 1)$$

$$\text{where} \qquad d_i = \begin{cases} 1 & \text{if } L_0(\alpha^i) = \beta^k \\ 0 & \text{else} \end{cases}$$

The result follows □

We may now establish the following corollary which is an immediate consequence of theorem 1.3.2 and proposition 1.2.3.

COROLLARY 1.3.3: $\Theta(x) = \Omega_0(x)\theta_0(y)$. $\Xi_0(x) = \Omega_0(x)\theta_0(y^{-1})$.

The family $D(q^2)$ was first discovered by Singer in 1939 ([sin] see also [hal1] and [hal2]), and for quite some time it was unknown whether there was another infinite

family of cyclic difference sets with the same parameters as $D(q^2)$ but not isomorphic to it. This question was eventually answered in the affirmative by Gordon, Mills, and Welch [gor] who observed that $\Theta(x) = \Omega_0(x)\theta_0(y)$ and gave the following construction.

CONSTRUCTION 1.3.4: *(Gordon, Mills, Welch [gor]) Let D be a cyclic Hadamard difference set in $\mathbf{F}_q^*$ and let $\hat{\theta}(y)$ be its Hall polynomial. Then $\Omega_0(x)\hat{\theta}(y)$ is the Hall polynomial of a $(q^2-1, q^2/2, q^2/4)$ cyclic difference set. If two such designs are constructed from D_1 and D_2, they are isomorphic if and only if D_1 is a translate of D_2.*

Thus, Jackson's theorem may be restated

THEOREM 1.3.5: *D is a $(q^2-1, q^2/2, q^2/4)$ design on which $PSL_2(q)$ acts transitively if and only if it is of Gordon, Mills, Welch type.*

The construction given in [gor] is actually much more general than that given above, but we are only interested in this special case for the purpose of this discussion. It was noted in that paper that the difference set $G(q^2)$ whose Hall polynomial is $\Xi_0(x)$ is never isomorphic to $D(q^2)$ provided $q > 4$. Thus, $G(q^2)$ became the first infinite family known with the same parameters as $D(q^2)$ but not isomorphic to $D(q^2)$. Since both $G(q^2)$ and $M(q^2)$ are classically known designs known to have this property, it is perhaps surprising that, until now, it has not been noticed that $G(q^2) \cong M(q^2)$.

2 The Code of $M(q^2)$

In this section we will mainly be concerned with computing the rank of $C_2(M(q^2))$, thus solving a conjecture of Assmus and Key ([ass1],[ass3]). Also, we will investigate the existence of subcodes of $C_2(M(q^2))$ isomorphic to $R^*(1, 2m)$.

2.1 Preliminary Lemmas

We will first prove some technical lemmas which will be needed in the sequel. It may be, however, that some of these results are interesting in their own right. Our first lemma was communicated to the author by A. Brouwer via R.M. Wilson. It has evidently been known in the folklore for some time. (The earliest published use of this technique known to this author is [smi] where it is used to compute the rank of the point-hyperplane incidence matrix of $PG(n, q)$, where $q = p^m$.) In some sense, it is a generalization of the fact that a circulant matrix can be diagonalized by a Vandermonde matrix.

LEMMA 2.1.1: Let α be a primitive element of $\mathbf{F_q}$ $(q = 2^m)$, and let $f : (\mathbf{F_q^*}, \mathbf{F_q^*}) \to \mathbf{F_q}$ be given by $f(x, y) = \sum_{i,j=0}^{q-2} a_{ij} x^i y^j$. Let the matrix $\mathbf{A}$ be defined

$(\mathbf{A})_{ij} = a_{ij}$ and define the matrix $\mathbf{F}$ by $(\mathbf{F})_{\mathbf{ij}} = f(\alpha^i, \alpha^j)$. Then $Rank(\mathbf{A}) = Rank(\mathbf{F})$.

PROOF: Let $\mathbf{V}$ be the Vandermonde matrix

$$\mathbf{V} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(q-2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{q-2} & \alpha^{2(q-2)} & \cdots & \alpha^{(q-2)(q-2)} \end{pmatrix}$$

Then direct computation shows that $\mathbf{VAV^T} = \mathbf{F}$. Since $\mathbf{V}$ is nonsingular, we have the result $Rank(\mathbf{A}) = Rank(\mathbf{F})$ □

LEMMA 2.1.2: Let $\mathbf{F_q} = \{\alpha_1, \ldots, \alpha_q\}$. Let $\mathbf{B}$ be the matrix with $\mathbf{B}_{i,j} = (\alpha_i + \alpha_j)^{q-2}$ then,

$$Rank \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ & & \mathbf{B} & & \end{pmatrix} = q/2$$

PROOF: First note that

$$(\mathbf{B^2})_{ij} = \sum_{k=1}^{q} (\alpha_i + \alpha_k)^{q-2} (\alpha_k + \alpha_j)^{q-2}$$
$$= \sum_{k=1}^{q} [\alpha_k^2 + (\alpha_i + \alpha_j)\alpha_k + \alpha_i \alpha_j]^{q-2}$$

This last sum is 0 if $i = j$ since it then runs through all elements of $\mathbf{F_q}$. If $i \neq j$, the sum is 0 since the function $\alpha_k \mapsto \mu\alpha_k$ is 2-1 on $\mathbf{F_q}$. Thus, $\mathbf{B^2} = 0$ and we conclude that $Rank(\mathbf{B}) \leq q/2$. Now, let $\mathbf{B}'$ be the principal submatrix of B obtained by deleting the row and column corresponding to 0. We may apply lemma 2.1.1 to this

matrix with $f(x,y) = (x+y)^{q-2} = x^{q-2} + x^{q-4}y^2 + x^{q-6}y^4 + \cdots + y^{q-2}$. Clearly, then, the matrix of coefficients has rank $q/2$ and by lemma 2.1.1, $Rank(\mathbf{B}') = q/2$. Hence, $Rank(\mathbf{B}) = q/2$. Now, since $\mathbf{B^2} = 0$ and $\mathbf{B}$ is symmetric, the rows of $\mathbf{B}$ span a self orthogonal code. Since $Rank(\mathbf{B}) = q/2$, this code is in fact self dual. Since $(1,1,1,\ldots,1)$ is orthogonal to every row of $\mathbf{B}$, it is in this code and we have the desired result. □

Recall that the trace map $Tr(x) = x + x^2 + x^4 + \cdots + x^{q/2}$ is a linear functional mapping $\mathbf{F_q} \to \mathbf{F_2}$, and has the property that every linear functional $L : \mathbf{F_q} \to \mathbf{F_2}$ is of the form $L(x) = Tr(\mu x)$ for some $\mu \in \mathbf{F_q}$. Let $\mathbf{M}$ be the matrix of section 1.2. except now appended with a row and column corresponding to $(0,0)$ with every new entry equal to 0. Let $f(x) = Tr(x^{q-2})$, so that $f(\mathbf{M})$ is an "extended" incidence matrix of $M(q^2)$. Clearly, this matrix has the same rank as the ordinary incidence matrix. Let R_∞ be the set of rows of $\mathbf{M}$ indexed by multiples of (0,1). For $\alpha \in \mathbf{F_q}$ let R_α be the set of rows indexed by multiples of $(1,\alpha)$. Note that the R_i partition the rows of $\mathbf{M}$ except that $0 \in R_i$ for each i. Finally, define $f(R_i)$ in the obvious way, so that if z is an entry of R_i, then $f(z)$ is the corresponding entry of $f(R_i)$

LEMMA 2.1.3: The code generated by $f(R_i) \cup \{\mathbf{j}\}$, where $\mathbf{j}$ is the all ones vector, is equivalent to $\{(\mathbf{c},\mathbf{c},\ldots,\mathbf{c}) : \mathbf{c} \in R(1,m)\}$. The rows of $f(R_i)$ are equivalent to $\{(\mathbf{c},\mathbf{c},\ldots,\mathbf{c}) : \mathbf{c}$ *is a linear functional* $\}$.

PROOF: It suffices to prove the latter assertion. Consider R_γ. Let α generate $\mathbf{F_q^*}$.

Permute the columns of $\mathbf{M}$ so that row $(1,\gamma)$ is

$$(0,1,\alpha,\alpha^2,\ldots,\alpha^{q-2},0,1,\alpha,\ldots,\alpha^{q-2})$$

Now, label the columns of R_γ by $(0,1,\alpha^{q-2},\alpha^{q-3},\ldots,\alpha,0,1,\alpha^{q-2},\ldots,\alpha)$ (note that this labelling does not correspond to that of $\mathbf{M}$) and label row $\mu(1,\gamma)$ with μ. Then the entry in row μ column σ is $Tr(\mu\sigma)$. As μ runs through all elements of $\mathbf{F_q}$, this lists all linear functionals. The case of R_∞ is identical. □

2.2 The Rank of $\mathbf{C_2(M(q^2))}$

It is conjectured in [ass1] and [ass3] that $rank(C_2(M(q^2))) = m2^{m-1}$ where $q = 2^m$ as usual. We can now prove this by using the lemmas in section 2.1 to exhibit a basis for $C_2(M(q^2))$. Let $\mathbf{B}$ be as in lemma 2.1.2, and let $H \subseteq \mathbf{F_q}$ with $|H| = q/2$ such that the rows and columns of $\mathbf{B}$ indexed by the elements of H form a nonsingular principal submatrix of $\mathbf{B}$. Now, by lemma 2.1.3, $rank(f(R_i)) = m$ for each i. For each $\beta \in H$, let B_β be a set of m vectors in $f(R_\beta)$ such that B_β is a basis for $f(R_\beta)$. Let $B = \bigcup_{\beta\in H} B_\beta$. Notice that $|B| = m2^{m-1}$. We claim that B is a basis for $C_2(M(q^2))$. To show this, we will first show that B is linearly independent. Write $B = \{\mathbf{b_1},\mathbf{b_2},\ldots,\mathbf{b_{m2^{m-1}}}\}$ and suppose $\sum_{i=1}^{m2^{m-1}} a_i\mathbf{b_i} = \mathbf{0}$ for some scalars $\{a_i\}_{i=1}^{m2^{m-1}}$ (in this case, of course, a scalar is an element of $\mathbf{F_2}$). Then, if we write $H = \{\beta_1,\ldots,\beta_{q/2}\}$ we may rewrite this expression as

$$\sum_{\mathbf{b_i}\in R_{\beta_1}} a_i\mathbf{b_i} + \sum_{\mathbf{b_i}\in R_{\beta_2}} a_i\mathbf{b_i} + \cdots + \sum_{\mathbf{b_i}\in R_{\beta_{q/2}}} a_i\mathbf{b_i} = \mathbf{0}$$

which, in turn, may be rewritten as $c_1\mathbf{x_1} + c_2\mathbf{x_2} + \cdots + c_{q/2}\mathbf{x_{q/2}}$ where $c_i \in \mathbf{F_2}$ and $\mathbf{x_i} \in span(f(R_{\beta_i})) = f(R_{\beta_i})$. If $c_i = 0$, let $\mathbf{y_i} = \mathbf{0} \in f(R_{\beta_i})$. Otherwise, let $\mathbf{y_i} = \mathbf{x_i}$. The above sum now becomes $\mathbf{y_1} + \mathbf{y_2} + \cdots + \mathbf{y_{q/2}} = \mathbf{0}$ where $\mathbf{y_i} \in f(R_{\beta_i})$. It therefore suffices to prove

PROPOSITION 2.2.1: *Let* $H = \{\beta_1, \ldots, \beta_{q/2}\}$ *be as above. For each* i *with* $1 \leq i \leq q/2$, *pick* $\mathbf{y_i} \in f(R_{\beta_i})$. *Then* $\sum_{i=1}^{q/2} \mathbf{y_i} = \mathbf{0}$ *if and only if* $\mathbf{y_i} = \mathbf{0}$ *for all* i

PROOF: Assume $\sum_{i=1}^{q/2} \mathbf{y_i} = \mathbf{0}$. Suppose $\mathbf{y_i}$ is the row of $f(\mathbf{M})$ associated with $\alpha_i(1, \beta_i)$ (possibly $\alpha_i = 0$). The entries in the corresponding row of $\mathbf{M}$ are those elements of the form $(\alpha_i, \alpha_i\beta_i)(x_1, x_2)^T$ where (x_1, x_2) runs through every element of $\mathbf{F_q^2}$. Thus, we conclude that the columns of $\mathbf{M}$ restricted to the rows corresponding to $\mathbf{y_i}$ form the subspace of $\mathbf{F_q^{q/2}}$ generated by $(\alpha_1, \alpha_2, \ldots, \alpha_{q/2})^T$ and $(\alpha_1\beta_1, \alpha_2\beta_2, \ldots, \alpha_{q/2}\beta_{q/2})^T$. Now, let $(\sigma_1, \sigma_2, \ldots, \sigma_{q/2})$ be any element of this subspace. Then

$$\mathbf{0} = \sum_{i=1}^{q/2} Tr[(\sigma_i)^{q-2}] = Tr[\sum_{i=1}^{q/2} (\sigma_i)^{q-2}]$$

since this sum is just the entry in one coordinate position of $\sum_{i=1}^{q/2} \mathbf{y_i}$. Notice that the above equation must also hold for every scalar multiple of $(\sigma_1, \sigma_2, \ldots, \sigma_{q/2})$ and so it must be the case that $\sum_{i=1}^{q/2} (\sigma_i)^{q-2} = 0$. More specifically, we have shown that

$$\sum_{i=1}^{q/2} (\alpha_i)^{q-2} = \sum_{i=1}^{q/2} (\gamma\alpha_i + \alpha_i\beta_i)^{q-2} = 0$$

for every $\gamma \in \mathbf{F_q}$. Thus, $(\alpha_1^{q-2}, \alpha_2^{q-2}, \ldots, \alpha_{q/2}^{q-2})$ is orthogonal to $\big((\gamma + \beta_1)^{q-2}, (\gamma + \beta_2)^{q-2}, \ldots, (\gamma + \beta_{q/2})^{q-2}\big)$ for every $\gamma \in \mathbf{F_q}$. It then follows from lemma 2.1.2 and

the definition of H that $(\alpha_1^{q-2}, \alpha_2^{q-2}, \ldots, \alpha_{q/2}^{q-2})$ is orthogonal to every element of $\mathbf{F_q^{q/2}}$, so that $\alpha_i = 0$ for all i. Which is equivalent to saying that $\mathbf{y_i} = \mathbf{0}$ for all i, as desired. □

Proposition 2.2.1 shows that the set B is linearly independent. It remains to show

PROPOSITION 2.2.2: $span(B) = C_2(M(q^2))$

PROOF: We will show this by showing that each $f(R_i)$ is in the span of B. Clearly, $f(R_\beta) \subseteq span(B)$ if $\beta \in H$. Now, suppose that $\beta_0 \in \mathbf{F_q} \backslash H$ and let $\mathbf{y} \in f(R_{\beta_0})$. Say $\mathbf{y}$ is the is the row indexed by $\alpha_0(1, \beta_0)$, note $\alpha_0 \neq 0$. Let $\mathbf{B_2}$ be the submatrix of $\mathbf{B}$ with columns indexed by $\{\beta_0\} \cup \{\beta \ : \ \beta \in H\}$ and with rows indexed by $\mathbf{F_q}$. By lemma 2.1.2, there exists a nonzero vector, $(\hat{\alpha}_0, \alpha_1, \ldots, \alpha_{q/2})$ which is orthogonal to every row of the matrix

$$\begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ & & \mathbf{B_2} & & \end{pmatrix}$$

But clearly we have $\hat{\alpha}_0 \neq 0$, so we may assume $\alpha_0 = \hat{\alpha}_0$. Thus,

$$\sum_{i=0}^{q/2} (\alpha_i)^{q-2} = \sum_{i=0}^{q/2} (\alpha_i)^{q-2} (\gamma + \beta_i)^{q-2} = 0$$

for all $\gamma \in \mathbf{F_q}$ and $\beta_i \in \{\beta_0\} \cup \{\beta \ : \ \beta \in H\}$. Multiplying the latter sum by an appropriate scalar, we have that

$$\sum_{i=0}^{q/2} (\alpha_i)^{q-2} (\gamma_1 + \gamma_2 \beta_i)^{q-2} = \sum_{i=0}^{q/2} [(\gamma_1, \gamma_2) \cdot (\alpha_i, \alpha_i \beta_i)]^{q-2} = 0$$

For any $(\gamma_1, \gamma_2) \in \mathbf{F_q^2}$. Hence,

$$\sum_{i=0}^{q/2} Tr\Big([(\gamma_1, \gamma_2) \cdot (\alpha_i, \alpha_i\beta_i)]^{q-2}\Big) = 0$$

But this is exactly the entry in the column labelled (γ_1, γ_2) in the sum $\mathbf{y} + \mathbf{y_1} + \cdots + \mathbf{y_{q/2}}$ where $\mathbf{y_i}$ is the row of $f(\mathbf{M})$ associated with $\alpha_i(1, \beta_i)$. So $\mathbf{y} = \sum_{i=1}^{q/2} \mathbf{y_i}$ but since for $1 \leq i \leq q/2$, $\mathbf{y_i} \in span(B)$ we have that $\mathbf{y} \in span(B)$.

This leaves only the case of $f(R_\infty)$ to consider. Because of the above,we may show that $f(R_\infty) \in span(B)$ by showing that it is in the span of the other $f(R_i)$. In fact, it is not difficult to show that any of the $f(R_i)$ is in the span of the rest using the transitive action of $GL_2(q)$ on $M(q^2)$. Let $\mathbf{y} \in f(R_\infty)$, as above pick $\mathbf{z_0}, \mathbf{z_1}, \ldots, \mathbf{z_{q/2}}$ such that $\mathbf{z_i} \in f(R_{\alpha_i})$ and $\sum_{i=0}^{q/2} \mathbf{z_i} = 0$. Then take some element of $GL_2(q)$ which maps $\mathbf{z_0}$ to $\mathbf{y}$ and let $\mathbf{y_i}$ be the image of $\mathbf{z_i}$ under this map. Then clearly, since $GL_2(q)$ maps linearly independent vectors to linearly independent vectors, we have that $\mathbf{y_i} \notin f(R_\infty)$ for $1 \leq i \leq q/2$. In other words, $\mathbf{y} = \sum_{i=1}^{q/2} \mathbf{y_i}$ where each $\mathbf{y_i} \in span(B)$. We conclude that $F(R_\infty) \subseteq span(B)$ and we are done.□

An immediate consequence of Propositions 2.2.1 and 2.2.2 is that we have proved the conjecture of Assmus and Key stated as conjecture 7.12.1 in [ass1] and as conjecture 1 on page 288 of [ass3]. We record this in the following

THEOREM 2.2.3: $Rank(C_2(M(q^2))) = m2^{m-1}$

We will see some applications of theorem 2.2.3 in chapter 3.

2.3 Some Reed Muller Codes in $C_2(M(q^2))$

In addition to allowing us to exhibit a basis for $C_2(M(q^2))$, lemma 2.1.3 will allow us to determine whether the code $C_2(M(q^2))$ contains a copy of $R^*(1,2m)$ in the coding theoretic sense. Of course, it cannot, since it does not contain $\mathbf{j}$, but we will abuse notation and say that $R^*(1,2m) \leq C_2(M(q^2))$ if $\mathbf{j} \cup C_2(M(q^2))$ contains $R^*(1,2m)$. Note, however, that if the code of a $(q^2-1, q^2/2, q^2/4)$ design contains $R^*(1,2m)$ in the above sense, then the code of the complementary $(q^2-1, q^2/2-1, q^2/4-1)$ design actually contains $R^*(1,2m)$.

We will pause briefly to explain why this question may be of interest. There are three reasons. First, it was conjectured in [ass1] that the code of every $(q^2-1, q^2/2-1, q^2/4-1)$ design contains a copy of $R^*(1,2m)$ although this conjecture was shown using an exhaustive computer search to be false (see [ass4]), several weaker versions of the conjecture remain open. Thus, it is still important to examine $C_2(M(q^2))$ with respect to this property. Second, in the general theory of codes of designs, it is obviously preferable if no two nonisomorphic designs with the same parameters have isomorphic codes. In fact, we would even like to avoid the situation where two nonisomorphic designs with the same parameters generate codes one of which is a subcode of the other. This is, in fact the situation with projective planes which is why most of the applications of the theory occur there. The result below will show that in contrast to this situation, $C_2(M(q^2))$ contains the codes of many other designs with the same parameters as $M(q^2)$ (although the ones that we will find are

all isomorphic to $R^*(1,2m)$). Finally, we will see that a cyclic difference set whose code contains no cyclic copies of $R^*(1,2m)$ will have some very interesting combinatorial properties. We will discuss this situation further in chapter 4. With this in mind, let us show

PROPOSITION 2.3.1: *$C_2(M(q^2))$ contains a copy of $R^*(1,2m)$ as a subcode.*

PROOF: Reorder the columns of **M** so that they are labelled in the order

$$(0,0),(0,1),(0,\alpha),\ldots(0,\alpha^{q-2}),(1,0),(1,1),(1,\alpha),\ldots$$

$$\ldots,(\alpha^{q-2},0),(\alpha^{q-2},1),\ldots,(\alpha^{q-2},\alpha^{q-2})$$

Now, consider the subcodes $f(R_\infty)$ and $f(R_0)$. Let Q be the code of linear functionals so that $< Q, \mathbf{j} >= R(1,m)$. In this form, it is easy to see that $f(R_\infty) = \{(\mathbf{c},\mathbf{c},\ldots,\mathbf{c}) \ : \ \mathbf{c} \in Q\}$. We also see that the vectors in $f(R_0)$ are precisely those of the following type. Let $(x_1,\ldots,x_q)$ be any element of Q. Define vectors $\mathbf{y_i}$ $(1 \leq i \leq q)$ by the rule

$$\mathbf{y_i} = \begin{cases} \mathbf{j} \quad (\in \mathbf{F_2^q}) & \text{if } x_i = 1 \\ \mathbf{0} & \text{if } x_i = 0 \end{cases}$$

then every vector in $f(R_0)$ is of the form $(\mathbf{y_1},\mathbf{y_2},\ldots,\mathbf{y_q})$ for some $(x_1,x_2,\ldots,x_q) \in Q$. This leads us to observe that every element of $\langle f(R_\infty), f(R_0)\rangle$ has weight 0 or $q^2/2$. Moreover, it shows that $f(R_\infty) \cap f(R_0) = \{\mathbf{0}\}$ and that $\mathbf{j} \notin \langle f(R_\infty), f(R_0)\rangle$. This means that $\langle f(R_\infty), f(R_0), \mathbf{j}\rangle$ has dimension $2m+1$ and that every vector it contains has weight $0, q^2/2$, or q^2. It therefore follows from proposition 0.3.1 that

$\langle f(R_\infty), f(R_0), \mathbf{j}\rangle \cong R(1, 2m)$. Omitting the extra column of $\mathbf{M}$ corresponding to $(0, 0)$ gives the desired result $\square$

There are two things worth noting about proposition 2.3.1. First, since the automorphism group of $M(q^2)$ acts twofold transitively on the $f(R_i)$, the result is true for any two of the $f(R_i)$. Thus, $C_2(M(q^2))$ may contain as many as $\binom{q+1}{2}$ copies of $R^*(1, 2m)$. However, none of them is cyclic. This follows easily from the proof since each of these copies of $R^*(1, 2m)$ must contain vectors in common with $C_2(M(q^2))$. Thus, if any of them were cyclic, it would necessarily imply that $C_2(M(q^2)) \subseteq R^*(1, 2m)$, an impossibility. Since we are mainly interested in cyclic codes for the purpose of this paper, we have still not fully answered the question whether $R^*(1, 2m) \leq C_2(M(q^2))$.

3 The Code of $M(q^2)$ as a Cyclic Code

In the previous section, we determined that $C_2(M(q^2))$ contains copies of $R^*(1, 2m)$, but none of these codes was cyclic. This motivates the question whether $C_2(M(q^2))$ contains such subcodes. To answer this question (in the affirmative) we will first determine the roots of the generating polynomial for $C_2(M(q^2))$. In addition, this determination will allow us to estimate the minimum distance of the code using the BCH bound.

3.1 The Roots of $\Xi(\mathbf{x})$

We know that $C_2(M(q^2))$ has dimension $m2^{m-1}$. This means that its generator polynomial has exactly $m2^{m-1}$ non-roots. Since the orbit of a primitive element of $\mathbf{F_{q^2}}$ contains $2m$ elements, this may lead us to suspect that the non-roots consist of $q/4$ orbits of primitive elements. This, as we shall see, is not entirely true. In fact, the non-roots do comprise exactly $q/4$ orbits, but they are not all primitive. We will show this in this section along with giving a simple way to determine which non-roots are primitive. Before we begin, though, we will need to clarify some

preliminary notation.

We will use notation 1.3.1. In chapters 0 and 1, we characterized the non-roots of $\Theta(x)$ as being α^{-1} and its conjugates where α is any primitive element of $\mathbf{F_{q^2}}$. Notice that for any element $\gamma \in \mathbf{F_{q^2}}$, $\gamma^q + \gamma \in \mathbf{F_q}$ where we are viewing $\mathbf{F_q}$ as a subfield of $\mathbf{F_{q^2}}$. For our particular α as above, we will write $\alpha^q + \alpha = c \in \mathbf{F_q} \setminus \{0\}$.

THEOREM 3.1.1: *The non-roots of* $\Xi_0(x)$ *are the elements of the form* $\alpha^{\ell(q-1)+1}$ *with* $0 < \ell \leq q$ *and* ℓ *even, and their conjugates.*

Before proving the theorem, we will illustrate it by examining the examples $M(16)$ and $M(64)$. Let γ be of the form $\gamma = \alpha^{\ell(q-1)+1}$. The conjugates of γ are $\gamma, \gamma^2, \gamma^4, \ldots, \gamma^{q^2/2}$. These $2m$ elements are not necessarily distinct, but the first m of them are clearly distinct. We therefore define the *half-orbit* of γ to be $\{\gamma, \gamma^2, \ldots, \gamma^{q/2}\}$. The non-roots can then be given as $\alpha^{\ell(q-1)+1}$, $, 0 < \ell \leq q$, together with their half-orbits. In this way, each non-root is counted exactly once. In the case of $M(16)$, we have $q = 4$ and the corresponding half-orbits of non-roots are $\{\alpha^7, \alpha^{14}\}$ and $\{\alpha^{13}, \alpha^{11}\}$. Thus, the code of $M(16)$ has non-roots exactly α^{-1} and its conjugates, as we expected since $M(16) \cong D(16)$. The case of $M(64)$ is more interesting. Here, $q = 8$ and the half-orbits of non-roots are $\{\alpha^{15}, \alpha^{30}, \alpha^{60}\}$, $\{\alpha^{29}, \alpha^{58}, \alpha^{53}\}$, $\{\alpha^{43}, \alpha^{23}, \alpha^{46}\}$, and $\{\alpha^{57}, \alpha^{51}, \alpha^{39}\}$. Notice that the first and fourth of these form an orbit as do the second and third. But notice also that α^{15} is not primitive. Thus, the code of $M(64)$ contains exactly one cyclic copy of $R^*(1, 6)$. These examples show that using the half-orbits gives an easy way to use the the-

orem to write down the half-orbits of non-roots of the generating polynomial of $C_2(M(q^2)$. The reader may use this method to verify that every non-root of the generator polynomial of $C_2(M(256))$ is primitive. Thus, $C_2(M(256))$ contains exactly 4 cyclic copies of $R^*(1,8)$. In section 3.2, we will see how to easily determine exactly how many cyclic copies of $R^*(1,2m)$ are contained in $C_2(M(q^2))$. We will also see that this number is at least one.

We need to make one more notational change before beginning the proof of theorem 3.1.1. $\Xi_0(x)$ may be replaced with any of its translates: $x^j\Xi_0(x) \ mod(x^{q^2-1}-1)$ and the resulting polynomial will still be a Hall polynomial of $M(q^2)$ and will have the same roots as $\Xi_0(x)$ over $\mathbf{F_{q^2}}$ (except possibly for 0 roots, which we ignore). It is shown in [gor] that 2 is a multiplier of $M(q^2)$ and hence, there is a translate $\Xi(x)$ of $\Xi_0(x)$ which is fixed by this multiplier. Thus, $\Xi(x)$ has the property that $\Xi(x) \in \{0,1\}$ for every $x \in \mathbf{F_{q^2}}$. We will therefore replace $\Xi_0(x)$ with $\Xi(x)$. Similarly, there is a translate $\theta(x) = x^i\theta_0(y^{-1})$ of $\theta_0(y^{-1})$ which is fixed by the multiplier 2 of $D(q)$, so that $\theta(y^{-1})$ always takes the value 0 or 1. Now, let $\Omega(x) = x^{j-i}\Omega_0(x)$. We then have $\Xi(x) = x^j\Xi_0(x) = (x^{j-i}\Omega_0(x))(x^i\theta(y^{-1}) = \Omega(x)\theta(y^{-1})$. If $\Xi(x) \neq 0$, then $1 = \Xi(x) = \Omega(x)\theta(y^{-1}) = \Omega(x)$. So that $\Omega(x)$ always takes the value 0 or 1 provided $\theta(y^{-1}) \neq 0$. We will also define $L(x) = L_0(\alpha^{i-j}x)$. Note $L(x)$ is a linear functional mapping $\mathbf{F_{q^2}}$ to $\mathbf{F_q}$. We may easily verify that theorem 1.3.2 remains valid with $\Omega_0(x)$ replaced by $\Omega(x)$ and with $L_0(x)$ replaced by $L(x)$. With these preliminaries, we are able to give the

PROOF OF THEOREM 3.1.1: We have $\Xi(x) = \Omega(x)\theta(y^{-1})$ in the above notation. So the non-roots of $\Xi(x)$ are precisely those elements which are non-roots of both $\Omega(x)$ and $\theta(y^{-1})$. By proposition 0.3.2, the non-roots of $\theta(y^{-1})$ over $\mathbf{F_q}$ are β and its conjugates. Thus, over $\mathbf{F_{q^2}}$, the non-roots of $\theta(y^{-1})$ are those elements α^i such that $(\alpha^i)^{q+1} = \beta$ or a conjugate of β. These are precisely those elements of the form $\alpha^{\ell(q-1)+1}$ where $0 \leq \ell \leq q$ and their conjugates.

Each element of the form $\alpha^{\ell(q-1)+1}$ corresponds to a half-orbit so by our above discussion, we only need to determine those ℓ for which $\alpha^{\ell(q-1)+1}$ is a non-root of $\Omega(x)$ and then extend to the half-orbits. Now, consider the cases where $\ell = 0$ or $\ell = 1$. These correspond to the cases where $\alpha^{\ell(q-1)+1} = \alpha$ or $\alpha^{\ell(q-1)+1} = \alpha^q$. We claim that these elements must be roots of $\Omega(x)$. Since they are conjugates, it will suffice to show that α is a root of Ω.

For the rest of this proof, we will assume that $L(x)$ has the following form. Express an element $\gamma \in \mathbf{F_{q^2}}$ as $\gamma = t_1 + t_2\alpha$ where $t_1, t_2 \in \mathbf{F_q}$. Then there are elements $a_1, a_2 \in \mathbf{F_q}$ such that $L(t_1 + t_2\alpha) = a_1t_1 + a_2t_2$. We will assume that $a_2 \neq 0$, but the case where $a_2 = 0$ can be treated in a virtually identical manner . Now,

$$\Omega(\alpha^j) = \sum_{i=0}^{q^2-2} c_i(\alpha^j)^i \qquad \text{where} \qquad c_i = \begin{cases} 1 & \text{if } L(\alpha^i) = 1 \\ 0 & \text{else} \end{cases}$$

but if $\alpha^i = t_1 + t_2\alpha$, $L(\alpha^i) = 1$ means that $a_1t_1 + a_2t_2 = 1$ so that

$$t_2 = \frac{1 + a_1t_1}{a_2}$$

We then let

$$a = \frac{a_1}{a_2},\ b = \frac{1}{a_2},\ t = t_1$$

And we have $\alpha^i = t(1 + a\alpha) + b\alpha$. Thus,

$$\Omega(\alpha^j) = \sum_{t \in \mathbf{F_q}} [t(1 + a\alpha) + b\alpha]^j$$

We now have $\Omega(\alpha) = \sum_{t \in \mathbf{F_q}} [t(1 + a\alpha) + b\alpha] = 0$, and it follows that α (and α^q) are roots of $\Omega(x)$ as claimed.

There are $m(q-1)$ possibilities left for the non-roots of $\Xi(x)$. By theorem 2.2.3, we know that exactly $m2^{m-1} = m(q/2)$ of them are actually non-roots, and by the above, we know that these non-roots are either elements of the form $\alpha^{\ell(q-1)+1}$ $(2 \leq \ell \leq q)$ or in a half-orbit of such an element. Also, it will suffice to exhibit those ℓ, $(2 \leq \ell \leq q)$ for which $\alpha^{\ell(q-1)+1}$ is not a root. There are $q/2$ such ℓ. Suppose we can show that for any ℓ with $2 \leq \ell \leq q-1$ that $\alpha^{\ell(q-1)+1}$ and $\alpha^{(\ell+1)(q-1)+1}$ cannot both be non-roots. Then the theorem would follow by the pigeonhole principle.

Therefore, assume for the sake of a contradiction, that for some ℓ in the range $2 \leq \ell \leq q-1$ we have $\Omega(\alpha^{\ell(q-1)+1}) = \Omega(\alpha^{(\ell+1)(q-1)+1}) = 1$. Replacing ℓ with $\ell - 1$ if necessary, we may assume that $\Omega(\alpha^{(\ell-1)(q-1)+1}) = 0$. This gives the equations:

$$\sum_{t \in \mathbf{F_q}} [t(1 + a\alpha) + b\alpha]^{(\ell-1)(q-1)} [t(1 + a\alpha) + b\alpha] = 0 \qquad (1)$$

$$\sum_{t \in \mathbf{F_q}} [t(1 + a\alpha) + b\alpha]^{\ell(q-1)} [t(1 + a\alpha) + b\alpha] = 1 \qquad (2)$$

$$\sum_{t \in \mathbf{F_q}} [t(1 + a\alpha) + b\alpha]^{(\ell-1)(q-1)} [t(1 + ac + a\alpha) + b(c + \alpha)] = 1 \qquad (3)$$

$$\sum_{t\in\mathbf{F_q}}[t(1+a\alpha)+b\alpha]^{(\ell+1)(q-1)}[t(1+a\alpha)+b\alpha]=1 \tag{4}$$

$$\sum_{t\in\mathbf{F_q}}[t(1+a\alpha)+b\alpha]^{\ell(q-1)}[t(1+ac+a\alpha)+b(c+\alpha)]=1 \tag{5}$$

where equations (3) and (5) follow directly from equations (2) and (4) by noting that

$$[t(1+a\alpha)+b\alpha]^q=[t(1+ac+a\alpha)+b(c+\alpha)] \tag{6}$$

equation (6) also allows us to write

$$[t(1+a\alpha)+b\alpha]^{j(q-1)}=\left[\frac{t(1+ac+a\alpha)+b(c+\alpha)}{t(1+a\alpha)+b\alpha}\right]^j$$

For $j=\ell-1,\ell,\ell+1$. Thus, (1), (2), (3), and (5) may be viewed as four equations in the unknowns

$$S_{0j}=\sum_{t\in\mathbf{F_q}}\left(\frac{t(1+ac+a\alpha)+b(c+\alpha)}{t(1+a\alpha)+b\alpha}\right)^j$$

$$S_{1j}=\sum_{t\in\mathbf{F_q}}t\left(\frac{t(1+ac+a\alpha)+b(c+\alpha)}{t(1+a\alpha)+b\alpha}\right)^j$$

where $j=\ell-1,\ell$. In particular, we rewrite

$$(b\alpha)S_{0(\ell-1)}+(1+a\alpha)S_{1(\ell-1)}=0 \tag{1}$$

$$(b(c+\alpha))S_{0(\ell-1)}+(1+ac+a\alpha)S_{1(\ell-1)}=1 \tag{3}$$

$$(b\alpha)S_{0\ell}+(1+a\alpha)S_{1\ell}=1 \tag{2}$$

$$(b(c+\alpha))S_{0\ell}+(1+ac+a\alpha)S_{1\ell}=1 \tag{5}$$

which we solve to obtain

$$\begin{array}{ll} S_{0(\ell-1)}=(1+a\alpha)/bc & S_{1(\ell-1)}=\alpha/c \\ S_{0\ell}=a/b & S_{1\ell}=1 \end{array} \tag{7}$$

We now turn to a different method for computing the same sums. Notice that $\alpha^{-\ell(q-1)-1}$ is a root of $\Theta(x)$ but is not a root of $\theta(y)$. So we have

$$\begin{aligned} 0 &= \sum_{t\in\mathbf{F_q}} \left(\frac{t(1+a\alpha)+b\alpha}{t(1+ac+a\alpha)+b(c+\alpha)}\right)^{\ell} \left(\frac{1}{t(1+a\alpha)+b\alpha}\right) \\ &= \sum_{t\in\mathbf{F_q}} \left(\frac{t(1+ac+a\alpha)+b(c+\alpha)}{t(1+a\alpha)+b\alpha}\right)^{\ell} \left(\frac{1}{t(1+ac+a\alpha)+b(c+\alpha)}\right) \end{aligned} \tag{8}$$

where the latter equality follows by raising the first to the power q. We compute:

$$\begin{aligned} 0 &= \sum_{t\in\mathbf{F_q}} \left(\frac{t(1+a\alpha)+b\alpha}{t(1+ac+a\alpha)+b(c+\alpha)}\right)^{\ell} \left(\frac{b\alpha}{t(1+a\alpha)+b\alpha}\right) \\ &= \sum_{t\in\mathbf{F_q}} \left(\frac{t(1+a\alpha)+b\alpha}{t(1+ac+a\alpha)+b(c+\alpha)}\right)^{\ell} \left(1+\frac{t(1+a\alpha)}{t(1+a\alpha)+b\alpha}\right) \\ &= \left(\sum_{t\in\mathbf{F_q}} \left(\frac{t(1+ac+a\alpha)+b(c+\alpha)}{t(1+a\alpha)+b\alpha}\right)^{\ell}\right)^{q} \\ &\quad + (1+a\alpha) \sum_{t\in\mathbf{F_q}} \left(\frac{t(1+a\alpha)+b\alpha}{t(1+ac+a\alpha)+b(c+\alpha)}\right)^{\ell} \left(\frac{t}{t(1+a\alpha)+b\alpha}\right) \\ &= a/b + (1+a\alpha) \sum_{t\in\mathbf{F_q}} \left(\frac{t(1+a\alpha)+b\alpha}{t(1+ac+a\alpha)+b(c+\alpha)}\right)^{\ell} \left(\frac{t}{t(1+a\alpha)+b\alpha}\right) \end{aligned}$$

where the last equation follows by (7). Thus, we have

$$\sum_{t\in\mathbf{F_q}} \left(\frac{t(1+a\alpha)+b\alpha}{t(1+ac+a\alpha)+b(c+\alpha)}\right)^{\ell} \left(\frac{t}{t(1+a\alpha)+b\alpha}\right) = \frac{a}{b(1+a\alpha)} \tag{9}$$

Now, putting this all together, starting from equation (1), we have

$$
\begin{aligned}
0 &= \sum_{t\in\mathbf{F_q}} \left(\frac{t(1+a\alpha)+b\alpha}{t(1+ac+a\alpha)+b(c+\alpha)}\right)^{\ell-1} (t(1+a\alpha)+b\alpha) \\
&= (1+a\alpha)S_{1(\ell-1)} \\
&\quad + b\alpha \sum_{t\in\mathbf{F_q}} \left(\frac{t(1+ac+a\alpha)+b(c+\alpha)}{t(1+a\alpha)+b\alpha}\right)^{\ell} \left(\frac{t(1+a\alpha)+b\alpha}{t(1+ac+a\alpha)+b(c+\alpha)}\right) \\
&= \alpha(1+a\alpha)\left[\frac{1}{c}+b\sum_{t\in\mathbf{F_q}}\left(\frac{t(1+ac+a\alpha)+b(c+\alpha)}{t(1+a\alpha)+b\alpha}\right)^{\ell}\left(\frac{t}{t(1+ac+a\alpha)+b(c+\alpha)}\right)\right] \\
&\quad + (b\alpha)^2 \sum_{t\in\mathbf{F_q}} \left(\frac{t(1+ac+a\alpha)+b(c+\alpha)}{t(1+a\alpha)+b\alpha}\right)^{\ell} \left(\frac{1}{t(1+ac+a\alpha)+b(c+\alpha)}\right) \\
&= \alpha(1+a\alpha)\left[\frac{1}{c}+b\left(\sum_{t\in\mathbf{F_q}}\left(\frac{t(1+a\alpha)+b\alpha}{t(1+ac+a\alpha)+b(c+\alpha)}\right)^{\ell}\left(\frac{t}{t(1+a\alpha)+b\alpha}\right)\right)^{q}\right] \\
&= \frac{1}{c}+b\left(\frac{a}{b(1+a\alpha)}\right)^{q} \\
&= \frac{1+a\alpha}{c(1+a+a\alpha)}
\end{aligned}
$$

where the last three lines follow from (8), (9), and since $\alpha(1+a\alpha) \neq 0$. We conclude that $1+a\alpha = 0$, a contradiction. □

3.2 Consequences of the Theorem

Theorem 3.1.1 is important in its own right since it is always better to give a cyclic code in terms of its generator polynomial. For example, this makes $C_2(M(q^2))^{\perp}$ somewhat easier to compute than it would be given the characterization of the code in chapter 2. In this section, we will determine two properties of $C_2(M(q^2))$ which

could probably not be found using the methods of section 2. However, we will see that the second has a simple geometric proof based on the definitions of section 1.

First, recall that we have shown that $C_2(M(q^2))$ contains many codes isomorphic to $R^*(1,2m)$, but we haven't found any that are cyclic. To determine whether $C_2(M(q^2))$ contains a cyclic copy of $R^*(1.2m)$ we must simply determine whether any non-roots of $\Xi(x)$ are primitive and apply proposition 0.3.2. We will first observe that the non-roots of $\Xi(x)$ do, in fact, comprise exactly $q/4$ orbits. Actually, this is easy, since $\alpha^{\ell(q-1)+1}$ and $\alpha^{(q+2-\ell)(q-1)+1}$ are conjugate, so that their corresponding half-orbits together form an orbit. The only way this could fail is if $\ell = q+2-\ell$, i.e. $\ell = q/2+1$, but $\alpha^{(q/2-1)(q-1)+1}$ is not a root by the theorem. We may now give a method for counting the number of cyclic copies of $R^*(1,2m)$ contained in $C_2(M(q^2))$.

THEOREM 3.2.1: *Let N be the number of $k \in \mathbf{N}$ satisfying*

(1) $0 \leq k \leq 2q$

(2) $k = 3 \ (mod\ 4)$

(3) k is relatively prime to $q+1$.

Then $C_2(M(q^2))$ contains exactly $N/2$ distinct cyclic copies of $R^*(1,2m)$. Moreover, $C_2(M(q^2))$ always contains at least one cyclic copy of $R^*(1,2m)$.

PROOF: By theorem 3.1.1 and the above discussion, the number of cyclic copies of $R^*(1,2m)$ in $C_2(M(q^2))$ is half the number of ℓ with ℓ even, $2 \leq \ell \leq q$, and $gcd(\ell(q-1)+1, q^2-1) = 1$. Notice $gcd(\ell(q-1)+1, q^2-1) = gcd(\ell(q-1)+1, q+1)$.

Now, assume $a|(q+1)$, then $a|\ell(q-1)+1$ if and only if $a|(2\ell-1)$. So $gcd(\ell(q-1)+1, q^2-1) = gcd(2\ell-1, q+1)$ and the number of ℓ with $gcd(\ell(q-1)+1, q^2-1) = 1$ is equal to the number of elements of the set $\{3, 7, 11, \ldots, 2q-1\}$ which are relatively prime to $q+1$, as desired. As for the second assertion, take $k = q+3$. Then k satisfies all three conditions of the theorem. □

As an easy consequence of the theorem, we see that if $q+1$ is prime, then every non-root of $\Xi(x)$ is primitive. So, for example, $C_2(M(256))$ contains exactly four cyclic copies of $R^*(1, 2m)$.

Finally, we would like to determine the minimum weight of $C_2(M(q^2))$. Given the theorem, the obvious way to do this is to use the BCH bound. We then have

PROPOSITION 3.2.2: *The minimum weight of $C_2(M(q^2))$ is at least $2q$.*

PROOF: The set of elements of the form $\alpha^{\ell(q-1)+1}$, with $2 \leq \ell \leq q$, ℓ even, contains the gap $\alpha, \alpha^2, \ldots, \alpha^{2(q-1)}$ of $2q-2$ elements. To apply the BCH bound, we must show that none of these elements is in the half-orbit of a non-root of the form $\alpha^{\ell(q-1)+1}$. But $\ell(q-1)+1 = 2k(q-1)+1$ for some k and so $2^i(2k(q-1)+1) = 2^i \ (mod\ 2(q-1))$. So that if $(\alpha^{\ell(q-1)+1})^{2^i} \in \{\alpha, \alpha^2, \ldots, \alpha^{2(q-1)}\}$, then $\alpha^{(\ell(q-1)+1)2^i} \in \{\alpha, \alpha^2, \alpha^4 \ldots, \alpha^{2q}\}$ which is impossible. Thus, the result follows by the BCH bound. □

We wish to emphasize at this point that we do not conjecture that the minimum distance of $C_2(M(q^2))$ is $2q$. In fact, it is probably significantly greater. To show

why we suspect this, we will give another proof of proposition 3.2.2 based on the geometric definitions in section 1 and some well known facts about the codes of Desarguesian projective planes which may be found in [ass1].

ALTERNATE PROOF OF PROPOSITION 3.2.2: Recall that the incidence vectors of $M(q^2)$ are associated with exterior points $p \in \Pi_q$, the Desarguesian projective plane of order q. In particular, the block $B_p \in M(q^2)$ is the sum of all exterior blocks through p in Π_q (we ignore the $q+2$ coordinates corresponding to the oval since they are always 0). Since there are $q/2$ such exterior blocks, and every block of Π_q meets each once, $B_p \in C_2(\Pi_q)^{\perp}$. Thus, $C_2(M(q^2)) \leq Hull(\Pi_q) = C_2(\Pi_q) \cap C_2(\Pi_q)^{\perp}$. It is shown in [ass1] that the minimum weight of $Hull(\Pi_q)$ is $2q$. □

In fact, if $C_2(M(q^2))$ contains any vectors of weight $2q$, they must necessarily correspond to the sum of two exterior blocks of Π_q. We therefore conclude that, in all probability, the minimum weight of $C_2(M(q^2))$ is greater than $q/2$ in order of magnitude. However, the determination of the exact minimum weight seems to be a very difficult problem.

4 From Algebra to Combinatorics

We show in this section that for a cyclic code of length $2^m - 1$, there is a simple combinatorial condition which is equivalent to the statement that the code does not contain a cyclic copy of $R^*(1, m)$. This condition can be defined for codes of any length, and for any prime field $\mathbf{F_p}$. Thus, this condition generalizes the concept of "containing a cyclic $R^*(1, m)$". We finish by giving a short example where we analyze the cyclic code of a cyclic difference set arising from a Singer cycle in a projective geometry.

4.1 Repetition Vectors and $\mathbf{C_{rep}(v)}$

Let $v \in \mathbf{N}$ and let k divide v, $k \neq v$ and let $\ell = v/k$. We define a *repetition vector* in $\mathbf{F_2^v}$ to be a vector of the form $(\mathbf{c}, \mathbf{c}, \ldots, \mathbf{c})$ where $\mathbf{c} \in \mathbf{F_2^k}$ is repeated ℓ times. Note that $\mathbf{F_2^v}$ contains at least 2 repetition vectors: $\mathbf{0}$ and $\mathbf{j}$. We define the code $C_{rep}(v)$ to be $\langle \mathbf{x} \in \mathbf{F_2^v} : \mathbf{x}$ *is a repetition vector*$\rangle$. If $C = \{(\mathbf{c}, \mathbf{c}, \ldots, \mathbf{c}) : \mathbf{c} \in \mathbf{F_2^k}\} \leq C_{rep}(v)$, we call C the *k-repetition subcode of* $C_{rep}(v)$, and the vectors in C will be called *k-repetition vectors*. We record some facts about $C_{rep}(v)$ in the following proposition whose proof is obvious.

PROPOSITION 4.1.1: *$C_{rep}(v)$ satisfies the following:*

(1) *$C_{rep}(v)$ is a cyclic code*

(2) *For each prime divisor p of v, let C_p be the v/p-repetition subcode of $C_{rep}(v)$. Then if $\mathbf{x}$ is any repetition vector in $C_{rep}(v)$ besides $\mathbf{0}$ and $\mathbf{j}$, then $\mathbf{x} \in C_p$ for some p dividing v.*

(3) *$C_{rep}(v) = \{\mathbf{0}, \mathbf{j}\}$ if and only if v is prime.*

(4) *$C_{rep}(v)$ consists entirely of repetition vectors if and only if v is a prime power.*

Since $C_{rep}(v)$ is cyclic, it may be given in the form of its generator polynomial. If v is odd, the polynomial can be given in terms of its roots. We then have

THEOREM 4.1.2: *Let $g(x)$ be the generator polynomial of $C_{rep}(v)$, where v is odd. Then*

$$g(x) = \prod_{\alpha \in S} (x - \alpha)$$

where S=$\{\alpha$: α is a primitive v^{th} root of $1\}$.

PROOF: Let k divide v,$k \neq v$, let $\ell = v/k$, and let C be the cyclic code whose generator polynomial is

$$h_k(x) = \prod_{\beta \,:\, \beta^k \neq 1} (x - \beta)$$

The non-roots of $h_k(x)$ are those elements which satisfy $(x^k - 1) = 0$. So we have

$$h_k(x) = \frac{x^v - 1}{x^k - 1} = 1 + x^k + x^{2k} + \cdots + x^{(\ell-1)k}$$

Then $h_k(x)$ is the generator polynomial of the k-repetition subcode of $C_{rep}(v)$. By definition, $g(x)$ is the gcd of all the $h_k(x)$ as k runs through all divisors of v. Thus, $g(x)$ has the desired form. □

COROLLARY 4.1.2: *let $v = 2^m - 1$, then a code C of length v contains $R^*(1, m)$ if and only if C is not a subcode of $C_{rep}(v)$*

It would clearly be of interest to find a cyclic Hadamard difference set whose code is contained entirely in $C_{rep}(v)$ or to show that no such difference set can exist. We will state this formally as

QUESTION 4.1.3: *Is there a $(4n-1, 2n, n)$ difference set D, such that $C_2(d) \leq C_{rep}(4n-1)$?*

We cannot give a full answer to question 4.1.3 at this time, but we may put some restrictions on D. In particular, we have

PROPOSITION 4.1.4: *Let D be a $(4n-1, 2n, n)$ cyclic difference set such that $C_2(D) \leq C_{rep}(4n-1)$. Then $4n-1$ is divisible by at least 3 distinct primes.*

PROOF: Note that no repetition vector can have weight $2n$. But the weight of any incidence vector or the sum of any two incidence vectors of blocks in D is $2n$. Thus, the incidence vector of a block in D must be the sum of at least three repetition vectors from different repetition subcodes. The result then follows by proposition 4.1.1 (2). □

Although proposition 4.1.4 is very easy to prove, it has some interesting consequences. The following is a list of every cyclic Hadamard difference set known to the author:

(1) *Quadratic residues in* F_p, *where* $v = p$ *a prime.*

(2) *Difference sets with* $v = p$, *a prime of the form* $p = 4x^2 + 27$

(3) *If* p *and* $p + 2$ *are primes, a cyclic Hadamard difference set with* $v = p(p + 2)$.

(4) *D(q).*

(5) $M(q^2)$.

(6) *Other recursive applications of the Gordon, Mills, Welch construction.*

(7) *Two sporadic examples with* $v = 255$.

For a discussion of (1), (2) and (3), see [hal1]. We remark that the code of (1) is the well known *quadratic residue code* (see [ass1]). By (6), we mean using difference sets isomorphic to those obtained from (4), (5), or (6) in construction 1.3.3.

Now, suppose D is a difference set which satisfies the condition of question 4.1.3. D cannot be of type (1), (2) or (3) by proposition 4.1.4. Obviously, D is not of type (4). That D is not of type (5) is one of the results proved in chapter 3 of this paper. We have verified using the computer that D cannot be one of the two difference sets of type (7). This leaves only (6). To show that question 4.1.3 has no affirmative answer for these difference sets, it would suffice to show that $\Omega_0(x)\theta_0(y^i)$ always has a primitive non-root whenever $gcd(i, 2^m - 1) = 1$.

Finally, we note that if there exists a cyclic Hadamard difference set with

parameters $(2^m - 1, 2^{m-1}, 2^{m-2})$, which satisfies the condition of question 4.1.3, having Hall polynomial $\theta_1(x)$, then $\theta_2(x) = \Omega_0(x)\theta_1(y)$ is the Hall polynomial of another difference set which satisfies question 4.1.3 as is $\theta_3(x) = \Omega_0(x)\theta_2(y)$, and so on. Thus, we conclude that if there is a cyclic difference set with parameters $(2^m - 1, 2^{m-1}, 2^{m-2})$ which answers question 4.1.3 in the affirmative, then there is a cyclic difference set E_1 with parameters $(2^{2m} - 1, 2^{2m-1}, 2^{2m-2})$ which also satisfies question 4.1.3 and also having the property that $\Gamma L_2(2^m)$ acts transitively on E_1. Moreover, E_1 is just the first member of a family $E_1, E_2, E_3, \ldots$ of cyclic Hadamard difference sets with semilinear automorphism groups each of which satisfies question 4.1.3. Although we consider the existence of such a family to be unlikely, we remark that their nonexistence would answer question 4.1.3 only in the case where $v = 2^m - 1$ leaving the general question open.

4.2 A Generalization of Question 4.1.3

Although the code of a cyclic Hadamard difference set provides the most interesting case, we may extend the observations of section 4.1 to apply to any cyclic difference set. We first define the p-ary analogue $C^p_{rep}(v) \leq \mathbf{F_p^v}$ in the obvious manner and note that the result of theorem 4.1.2 holds for $C^p_{rep}(v)$ provided $gcd(v, p) = 1$. We may thus restate some of the results of section 4.1 in the following theorem.

THEOREM 4.2.1 *Let D be a cyclic (v, k, λ) difference set. Let $p|(k - \lambda)$ and let $g(x)$ be the generator polynomial of $C_p(D)$. Then*

(1) *If* $p = 2$ *and* $v = 2^m - 1$, *then* $C_2(D)$ *contains a cyclic copy of* $R^*(1,m)$ *if and only if* $C_2(D) \not\leq C^2_{rep}(v)$

(2) *If* $gcd(p,v) = 1$, *then there exists a primitive* v^{th} *root of* 1 *which is not a root of* $g(x)$ *if and only if* $C_2(D) \not\leq C^p_{rep}(v)$

Notice that the question of whether a cyclic code C of length v is contained in $C^p_{rep}(v)$ makes sense even when neither hypothesis of theorem 4.2.1 holds. We therefore will view non-containment in $C^p_{rep}(v)$ as the appropriate combinatorial generalization of the concept of containing a cyclic copy of $R^*(1,m)$. The remainder of this section will be devoted to justifying this view. First, however, we formally state the following which generalizes question 4.1.3 and (for cyclic difference sets), generalizes the question of p.270 of [ass1].

QUESTION 4.2.2: *Is there a cyclic* (v,k,λ) *difference set* D *and a prime* p *such that* $C_p(D) \leq C^p_{rep}(v)$?

Note that if question 4.2.2 has an affirmative answer, then necessarily $p|(k-\lambda)$.

In light of our view that non-containment in $C^p_{rep}(v)$ is the appropriate combinatorial generalization of containing a cyclic $R^*(1,m)$, we must mention that for some values of v which are not of the form $2^m - 1$, there are already cyclic codes of length v which generalize the family $R^*(1,m)$. In this case, $v = \frac{q^{N+1}}{q-1}$ for $q = p^m$ and the codes are known as *non-primitive, subfield subcodes of the punctured, first-order generalized Reed-Muller code over* $\mathbf{F_q}$. The theory of these codes may be found

in [ass2] or in chapter 5 of [ass1]. Rather than go through the rather complicated details, we will simply define the codes as codes of certain cyclic difference sets and state some results that can be found in these references.

Let D be the design of 1 and N dimensional subspaces of $\mathbf{F_q}$ where $q = p^m$. Then D is a cyclic difference set with parameters

$$\left(\frac{q^{N+1}-1}{q-1}, \frac{q^N-1}{q-1}, \frac{q^{N-1}-1}{q-1}\right)$$

In this case, D will be called a *Singer difference set.* We are interested in determining $C_p(D)$, which is the aforementioned generalization of $R^*(1,m)$. Note that if $q = 2$, then D is the complement of a cyclic Hadamard difference set. Then since the codes $C_p(D)$ are a generalization of the $R^*(1,m)$, we will denote them by $C_p(D) = R_q^*(1, N+1)$. Ideally, we would like the analogue of theorem 4.2.1 to hold for $R_q^*(1, N+1)$, however, it does not. For example, if γ is a primitive 21^{st} root of 1 over $\mathbf{F_2}$, the non-roots of $R_4^*(1,3)$ (which is the code of the Desarguesian projective plane of order 4), are $1, \gamma^5, \gamma^9, \gamma^{10}, \gamma^{13}, \gamma^{15}, \gamma^{17}, \gamma^{18}, \gamma^{19}, \gamma^{20}$. So that the cyclic code of length 21 whose generator polynomial has non-roots exactly $\gamma^5, \gamma^{10}, \gamma^{13}, \gamma^{17}, \gamma^{19}, \gamma^{20}$ is not contained in $C_{rep}^2(21)$ but it also does not contain $R_4^*(1,3)$.

Even though this shows that the exact analogue of theorem 4.2.1 does not hold for $R_q^*(1, N+1)$, we may still show that if a cyclic code C contains $R_q^*(1, N+1)$, then C is not contained in $C_{rep}^p(\frac{q^{N+1}}{q-1})$. This will partially justify our view that question 4.2.2 is the appropriate generalization of the theory in the Hadamard case. Of course, it will suffice to show that $R_q^*(1, N+1) \not\leq C_{rep}^p(\frac{q^{N+1}}{q-1})$. We first

make a preliminary definition. If $i = \sum a_j q^j$ is the q-ary expansion of i, we define $wt_q(i) = \sum a_j$. The main theorem we will need may now be stated. Its proof may be found in [ass1] or [ass2] (see also [kas], [ber], or [cha]).

THEOREM 4.2.3: $R_q^*(1, N+1)$ *is cyclic with generator polynomial*

$$g(x) = \prod_{i(q-1) \in S} (x - \gamma^i)$$

where γ *is a primitive* $\left(\frac{q^{N+1}-1}{q-1}\right)^{st}$ *root of* 1 *in* $\mathbf{F_{q^{N+1}}}$ *and* $S = \{u : 0 < u \leq q^{N+1} - 1,\ (q-1)|u,$ *and* $wt_q(up^j) < N(q-1)$ *for* $j = 0, 1, \ldots m-1$ *and* up^j *is reduced mod* $q^{N+1} - 1\}$.

Notice that theorem 4.2.3 is a direct generalization of proposition 0.3.2. We may now prove

THEOREM 4.2.4: *Let* $g(x)$ *be the generator polynomial of* $R_q^*(1, N+1)$, *and let* v *be the length of* $R_q^*(1, N+1)$. *Then there is a primitive* v^{th} *root of* 1 *over* $\mathbf{F_p}$ *which is not a root of* $g(x)$.

PROOF: Let $t = q - 1$. Then if $0 \leq j < m$, we have $tp^j = p^j(p^m - 1) = (p^j - 1)p^m + (p^m - p^j)$. So $wt_q(tp^j) = q - 1$. Now, let $u = (q^{N+1} - 1) - (q - 1)$. Note $wt_q(u) + wt_q(t) = (N+1)(q-1)$ so $wt_q(u) = N(q-1)$. Thus, $u \in S$ and γ^{-1} is a non-root of $g(x)$ (where γ is as in theorem 4.2.3). □

Note that the above theorem may be used to verify our previous example where we

used the generator polynomial of $R_4^*(1,3)$. We have now shown what we intended, namely

COROLLARY 4.2.5: *Assume C is a cyclic code which contains $R_q^*(1, N+1)$. Then C is not contained in $C_{rep}^p\left(\frac{q^{N+1}-1}{q-1}\right)$*

Thus, in general, non-containment in $C_{rep}^p(v)$ is a slightly weaker condition than containing $R_q^*(1, N+1)$. For this reason, we would be extremely interested in obtaining the answer to question 4.2.2.

Bibliography

[ass1] E.F. Assmus, Jr. and J.D. Key. *Designs and their Codes.* Cambridge University Press, 1992. Cambridge Tracts in Mathematics, Vol. 103.

[ass2] E.F. Assmus, Jr. and J.D. Key. Polynomial Codes and Finite Geometries. preprint.

[ass3] E.F. Assmus, Jr. and J.D. Key. Hadamard Matrices and their Designs: A Coding Theoretic Approach. *Trans. Amer. Math. Soc.*, 330: 269–293, 1992.

[ass4] E.F. Assmus, Jr. and J.D. Key. Designs and Codes: an Update. Unpublished.

[ber] S.D. Berman. On the Theory of Group Codes. *Kibernetika*, 3: 31–39, 1967.

[cha] P. Charpin. Codes Cycliques Étendus Affines-Invariants et Antichaines d'un Ensemble Partiellement Ordonne. *Discrete Math.*, 80: 229–247, 1990.

[dic] L.E. Dickson. *Linear Groups With an Exposition of the Galois Field Theory.* New York: Dover Publications, 1958.

[gor] B. Gordon, W.H. Mills, and L.R. Welch. Some New Difference Sets. *Canadian J. Math.*, 14: 614–625, 1962.

[hal1] M. Hall, Jr. *Combinatorial Theory.* New York: Wiley, Second Edition, 1986.

[hal2] M. Hall, Jr. A Survey of Difference Sets. *Proc. Amer. Math. Soc.*, 7: 975–986, 1956.

[jac] Wen-Ai Jackson. A Characterization of Hadamard Designs with $SL(2,q)$ Acting Transitively. *Geom. Dedic.*, 46: 197–206, 1993.

[kas] T. Kasami, S. Lin, and W. W. Peterson. Some Results on Cyclic Codes which are Invariant Under the Affine Group and Their Applications. *Inform. and Control*, 11: 475–496, 1967.

[lin] J.H. van Lint, and R.M. Wilson. *A Course in Combinatorics.* Cambridge University Press, 1992.

[mac] F.J. MacWilliams and N.J.A. Sloan *The Theory of Error Correcting Codes.* Amsterdam: North-Holland, 1983.

[mas1] A. Maschietti. Hyperovals and Hadamard Designs. *J. Geometry*, 44: 107–116, 1992.

[mas2] A. Maschietti. On $q^2/4$-sets of Type $(0, q/4, q/2)$ in Projective Planes of Order $q \equiv 0 \ (mod\ 4)$. *Discrete Math.*, 129: 149–158, 1994.

[mas3] A. Maschietti. Regular Triples with Respect to a Hyperoval. *Ars Comb.*, 39: 75–88, 1995.

[mas4] A. Maschietti. On Hadamard Designs Associated with a Hyperoval. *J. Geometry*, 53: 122–130, 1995.

[oor] P.C. van Oorschot, and S.A. Vanstone. *An Introduction to Error Correcting Codes with Applications.* Norwell: Kluwer, 1989.

[sin] J. Singer. A Theorem in Finite Projective Geometry and Some Applications to Number Theory. *Trans Amer. Math. Soc.* 43: 377–385, 1938.

[smi] K.J.C. Smith. On the p-rank of the Incidence Matrix of Points and Hyperplanes in a Finite Projective Geometry. *J. Combin. Theory*, 7: 122–129, 1969.