# ALGEBRAIC CODING THEORY

Thesis by

Robert Calderbank

In Partial Fulfillment of the Requirements

for the Degree of

Doctor of Philosophy

California Institute of Technology

Pasadena, California 91125

1980

(Submitted May 16, 1980)

# ACKNOWLEDGEMENTS

I wish to thank Professor Marshall Hall, Jr., my thesis advisor, for encouraging my interest in coding theory. I benefited a great deal from his generous support.

I am grateful to Professor David B. Wales for many ideas and suggestions and for the time and interest he has devoted to my work.

I wish to thank Mrs. F. J. MacWilliams for inviting me to spend August 1979 at Bell Laboratories. I appreciated her illuminating conversation and her generous hospitality.

I am grateful to the mathematics faculty at Caltech for their support and interest, to my fellow graduate students, and to the secretaries in the mathematics department. I particularly want to thank Mrs. Lillian Chappelle who typed this thesis so proficiently.

Thanks are also due to the California Institute of Technology and to the National Science Foundation for financial support.

ABSTRACT

The present investigation concerns quadratic residue codes, quasi-cyclic binary codes and symmetry codes. We show how to regard such a code as an ideal in an algebra generated by a group of automorphisms of the code. We then use the algebra to establish a square-root bound on the minimum weight of the code.

We begin by proving that any linear code may be regarded as an ideal in a suitable polynomial ring.

In chapter 2 we present the extended quadratic residue codes of length $(q+1)$, where $q$ is an odd prime power. We construct these codes in an elementary way from representations of the special linear group, $SL_2(q)$.

We then establish a square root bound on the minimum weight in the quasi-cyclic binary codes constructed by V. K. Bhargava, S. E. Tavares, and S.G.S. Shiva. The bound is tight and is achieved only by the [8,4,4] Hamming code. This result answers a question raised by F. J. MacWilliams and N.J.A. Sloane in 'The Theory of Error-Correcting Codes'. The proof rests on viewing these binary codes as ideals in a group algebra over GF(4).

In chapter 4 we extend the construction for symmetry codes given by V. Pless to fields other than GF(3). Given an odd prime power $q$, and a finite field $F$ of odd characteristic containing $\sqrt{-q}$, we construct a $[2q+2, q+1]$ symmetry code over $F$. We establish a square root bound on the minimum weight in this enlarged family of symmetry codes. When $q \equiv -1 \pmod 4$ this bound is tight and is achieved by an [8,4,4] code over GF(7).

Finally let $q \equiv -1 \pmod 8$ be an odd prime power and let $C(q)$ and $C(q)^*$ be the two extended binary quadratic residue codes of length $(q+1)$. We show how to regard $C(q)$ and $C(q)^*$ as one-sided ideals in a binary group algebra and that the appropriate product is a 2-dimensional ideal. This allows us to prove that if $d$ is the minimum weight in $C(q)$ then $(d-1)^2 - (d-1) + 1 - st \geq q$ where $s$, $t$ are non-negative integers with $s \equiv 0 \pmod 4$, and $t$ odd. The integers $s$ and $t$ depend on the way the non-zero entries of a codeword of minimum weight are distributed among the coordinate positions. We prove that $(d-1)^2 - (d-1) + 1 = q$ only if $q = 7$ and $d = 4$. When $s = 0$ we establish a correspondence between codewords of minimum weight $d$ in $C(q)$ and $d \times d$ Hadamard submatrices of the $(q+1) \times (q+1)$ Paley-Hadamard matrix.

CONTENTS

# INTRODUCTION

In coding theory we consider a set $F$ of $q$ distinct symbols which is called the alphabet. In practice $q$ is generally 2 and $F = \{0,1\}$. In most of the theory $q$ is a prime power and $F = GF(q)$. We then form the set of all possible n-tuples of elements of $F$. If $F$ is a field then we denote this set by $V_n(F)$ (or by $V_n(q)$ if $F = GF(q)$) and interpret it as an n-dimensional vector space over $F$. We shall denote the zero vector by $\underline{0}$ and the all-one vector by $\underline{1}$.

Given $x, y \in V_n(F)$ we define the distance $d(x,y)$ between $x$ and $y$ to be the number of coordinate positions in which $x$ and $y$ differ. This is a natural distance function to use since we shall be interested in the number of errors in a word that is spelled incorrectly. Given $x \in V_n(F)$ we define the weight $wt(x)$ of $x$ to be the number of non-zero entries, i.e., $wt(x) = d(x,\underline{0})$. For $r \geq 0$ and for $x \in V_n(F)$ we define the sphere of radius $r$ with center at $x$ by

$$B_r(x) = \{y \in V_n(F) : d(x,y) \leq r\}.$$

Consider a subset $C$ of $V_n(F)$ with the property that the distance between any two distinct vectors in $C$ is at least $(2e+1)$. If we take any vector $x$ in $C$ and change $t$ coordinates, where $t \leq e$ (i.e., we make t errors) then the resulting vector still resembles $x$ more than any of the other vectors in $C$. That is it has a smaller distance to $x$ than to any other vector in $C$. If we know $C$ we can correct the $t$ errors.

The purpose of coding theory is to study such e-error-correcting codes. An e-error-correcting code $C$ in $V_n(F)$ is said to be perfect

if

$$\bigcup_{x \in C} B_e(x) = V_n(F).$$

In this case the spheres of radius $e$ about the codewords are disjoint and they exhaust $V_n(F)$.

A linear $[n,k]$ code over $F$ is a k-dimensional subspace of $V_n(F)$. The error-correcting capacity of a code is determined by the minimum distance between all pairs of distinct codewords. For an arbitrary code consisting of $K$ codewords there are $\binom{K}{2}$ comparisons to make to find this minimum distance. For a linear code $C$ we have the following advantage. If $x, y \in C$ then $x - y \in C$ and $d(x,y) = d(x-y,\underline{0}) = wt(x-y)$. Thus the minimum distance is equal to the minimum weight among all non-zero codewords. An $[n,k,d]$ code is a linear code for which $d$ is the minimum weight among all non-zero codewords. In the present investigation we shall only be concerned with linear codes.

A monomial matrix is the product of a diagonal matrix with a permutation matrix. The error-correcting properties of a code depend on the minimum weight and this is unaltered by a monomial transformation of the underlying vector space. We say that two $[n,k]$ codes $C$ and $D$ are isomorphic if there exists an $n \times n$ monomial matrix $M$ such that $CM = D$. An automorphism of an $[n,k]$ code $C$ is an $n \times n$ monomial matrix $M$ such that $CM = C$. The automorphisms of $C$ form a group which we shall denote by $Aut(C)$.

In chapter 2 we construct quadratic residue codes of length $q$ where $q$ is an odd prime power. Two members of this family of linear codes are particularly interesting. The first is the binary Golay

[23,12,7] code and the second is the ternary Golay [11,6,5] code. The codes were discovered by M.J.E. Golay [5], an electrical engineer. The binary code is a perfect 3-error-correcting code and the ternary code is a perfect 2-error-correcting code. The automorphism group of each code involves a sporadic simple group. The automorphism group of the binary code is isomorphic to the Mathieu group $M_{23}$, and if $G$ is the automorphism group of the ternary code then $G/\{\pm I\}$ is isomorphic to the Mathieu group $M_{11}$.

Many codes with good error-correcting properties are also invariant under large automorphism groups. In this thesis we consider three infinite families of linear codes. Each code is invariant under a large automorphism group and we use the symmetries of the code to establish lower bounds on the minimum weight.

## CHAPTER 1. LINEAR CODES AS IDEALS IN POLYNOMIAL RINGS

We begin by proving that any linear code may be regarded as an ideal in a suitable polynomial ring.

THEOREM 1. Let $F$ be a field, let $\mathcal{B} = \{e_1,\ldots,e_n\}$ be the standard basis for $V_n(F)$, and let $C$ be a k-dimensional subspace of $V_n(F)$.

Let $f(x), g(x) \in F[x]$ be polynomials with $\deg f(x) = n - k$ and $\deg g(x) = k$, and let $h(x) = f(x)\, g(x)$.

Then there exist polynomials $\xi_s(x) \in F[x]$, $s = 1, \ldots, n$, each of degree $\leq n - 1$ such that the maps

$$e_s \to \xi_s(x) \quad s = 1, \ldots, n$$

extend linearly to a vector space isomorphism $\xi$ between $V_n(F)$ and the F-algebra $R = F[x]/(h(x))$. Under this isomorphism $\xi$ the code $C$ corresponds to the principal ideal generated by $f(x)$.

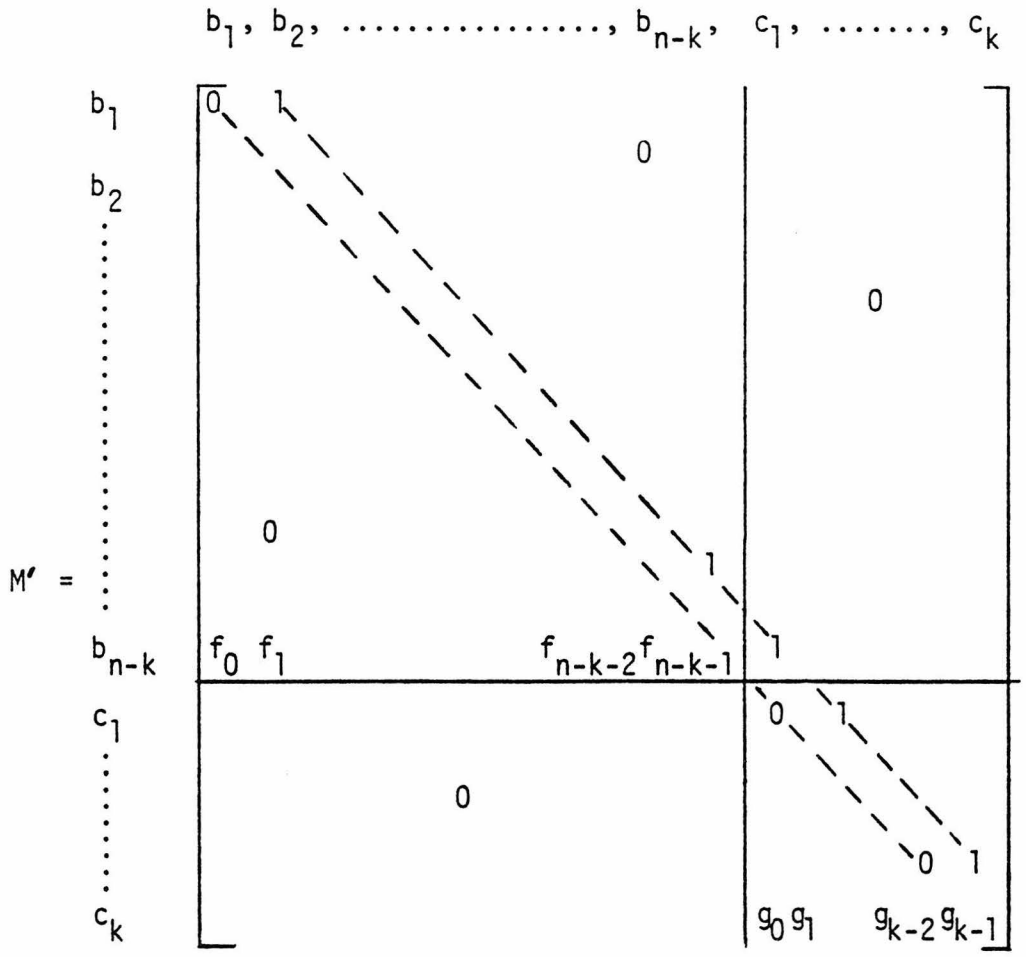
PROOF. We may suppose that $C \neq V_n(F)$ so that for some $i$, $e_i \notin C$. For convenience we assume $i = 1$. Let $c_1, \ldots, c_k$ be a basis for the code $C$ and extend this to a basis $\mathcal{B}' = \{b_1,\ldots,b_{n-k},c_1,\ldots,c_k\}$ of $V_n(F)$, where $b_1 = e_1$. We may suppose that $f(x)$ and $g(x)$ are both monic and we set

$$f(x) = x^{n-k} - f_{n-k-1}x^{n-k-1} - \cdots - f_0,$$

and

$$g(x) = x^k - g_{k-1}x^{k-1} - \cdots - g_0.$$

The matrix $M'$ given below determines a linear transformation $T$ with respect to the basis $\mathcal{B}'$




The principal submatrix in the upper left-hand corner is the companion matrix of $f(x)$ and the principal submatrix in the lower right-hand corner is the companion matrix of $g(x)$. The characteristic polynomial of $M'$ is $h(x) = f(x)\, g(x)$.

We have

$$b_1 T^j = b_{j+1} \qquad j = 0, 1, \ldots, n-k-1,$$

$$b_1 f(T) = c_1, \tag{1}$$

and

$$b_1 f(T) T^j = c_{j+1}, \quad j = 0, 1, \ldots, k-1,$$

and so the vectors $b_1T^j$, $j = 0, 1, \ldots, n-1$, are a cyclic basis for $V_n(F)$. Therefore $M'$ is non-derogatory and the minimum polynomial of $M'$ is $h(x)$. The polynomial $h(x)$ is the monic polynomial of smallest degree such that $b_1h(T) = 0$.

We now define polynomials $\xi_s(x)$, $s = 1, \ldots, n$, each of degree $\leq (n-1)$, by setting

$$e_s = b_1\xi_s(T) \quad s = 1, \ldots, n. \tag{2}$$

Note that $\xi_1(x) = 1$. The polynomials $\xi_s(x)$, $s = 1, \ldots, n$ are linearly independent and the linear map $\xi : V_n(F) \to R$ determined by

$$e_s \to \xi_s(x) \quad s = 1, \ldots, n,$$

is bijective. An appeal to (1) reveals that the linear map $\xi$ identifies the code $C$ with the principal ideal $(f(x))$ in $R$.

EXAMPLE 1. Take $F = GF(2)$ and take $C$ to be the [5,2] binary code spanned by the vectors $c_1 = (11001)$ and $c_2 = (01110)$. Choose $f(x) = x^3 + x + 1$ and $g(x) = x^2 + x + 1$. Then

$$h(x) = f(x)\, g(x) = x^5 + x^4 + 1.$$

If $b_1 = (10000)$, $b_2 = (01000)$, and $b_3 = (00100)$ then $\mathcal{B}' = \{b_1, b_2, b_3, c_1, c_2\}$ is a basis for $V_5(2)$. The matrix

$$M' = \begin{array}{c|ccc|cc} & b_1 & b_2 & b_3 & c_1 & c_2 \\ b_1 & 0 & 1 & 0 & 0 & 0 \\ b_2 & 0 & 0 & 1 & 0 & 0 \\ b_3 & 1 & 1 & 0 & 1 & 0 \\ \hline c_1 & 0 & 0 & 0 & 0 & 1 \\ c_2 & 0 & 0 & 0 & 1 & 1 \end{array}$$

determines a linear transformation $T$ with respect to the basis $\mathfrak{B}'$. We have

$$\begin{aligned} b_1 &= e_1 & \xi &: e_1 \to 1 \\ b_1T &= e_2 & \xi &: e_2 \to x \\ b_1T^2 &= e_3 & \xi &: e_3 \to x^2 \\ b_1T^3 &= e_5 & \xi &: e_5 \to x^3 \\ b_1T^4 &= e_4 & \xi &: e_4 \to x^4 . \end{aligned}$$

Thus

$$\xi(c_1) = \xi(e_1 + e_2 + e_5) = 1 + x + x^3$$

$$\xi(c_2) = \xi(e_2 + e_3 + e_4) = x + x^2 + x^4$$

and $$\xi(c_1 + c_2) = 1 + x^2 + x^3 + x^4 .$$

The map $\xi$ identifies the code $C$ with the principal ideal $(1 + x + x^3)$ in $F[x]/(x^5+x^4+1)$.

REMARKS. (1) An $[n,k]$ code $C$ over a finite field $F$ is called *cyclic* if $(c_0,c_1,\ldots,c_{n-1}) \in C$ implies $(c_{n-1},c_0,\ldots,c_{n-2}) \in C$. The map

$$\xi_1 : (a_0,a_1,\ldots,a_{n-1}) \to a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$$

is a vector space isomorphism between $V_n(F)$ and the polynomial ring $R = F[x]/((x^n-1))$. Notice that multiplication by $x$ in $R$ corresponds to the cycle shift

$$(a_0,a_1,\ldots,a_{n-1}) \to (a_{n-1},a_0,\ldots,a_{n-2})$$

in $V_n(F)$. It follows that the code $C$ corresponds to an ideal in $R$. This ideal is principal and is generated by a polynomial $g(x)$ that divides $(x^n - 1)$.

The linear map $\xi_1$ is weight preserving; the weight $\omega t(v)$ of a vector $v \in V_n(F)$ is equal to the number of non-zero coefficients of $\xi_1(v)$. However the linear map $\xi$ of theorem 1 need not respect weights in this way.

(2) We may choose the polynomial $f(x)$ of theorem 1 to have $(n-k)$ distinct zeros $\alpha_1, \ldots, \alpha_{n-k}$ in some extension field $K$ of $F$. Let $H$ be the $n \times (n-k)$ matrix with entries

$$(H)_{ij} = \xi_i(\alpha_j) \qquad i = 1, \ldots, n; \quad j = 1, \ldots, n-k.$$

where the polynomials $\xi_i(x)$ are defined in (2). If $a \in V_n(F)$ then $a \in C$ if and only if $f(x) | \xi(a)$. Now

$$aH = [(\xi(a))(\alpha_j)]$$

and so

$$C = \{a \in V_n(F) : aH = \underline{0}\}$$

The matrix $H$ is called *a parity check matrix* for $C$.

EXAMPLE 2. We return to the code $C$ of example 1. The zeros of $f(x) = x^3 + x + 1$ are $\alpha, \alpha^2, \alpha^4 \in GF(8)$. The matrix

$$H = \begin{bmatrix} 1 & 1 & 1 \\ \alpha & \alpha^2 & \alpha^4 \\ \alpha^2 & \alpha^4 & \alpha \\ \alpha^4 & \alpha & \alpha^2 \\ \alpha^3 & \alpha^6 & \alpha^5 \end{bmatrix}$$

is a parity check matrix for $C$.

Chapter 1 is joint work with Mrs. F. J. MacWilliams. The results presented here appear as a Bell Laboratories Technical Memorandum.

## CHAPTER 2. QUADRATIC RESIDUE CODES

We shall present the extended quadratic residue codes of length $q + 1$, where $q$ is an odd prime power. When $q$ is prime these codes become the classical quadratic residue codes. Examples include the ternary [12,6,6] Golay code and the binary [24,12,8] Golay code. The original construction is due to H. N. Ward [19]. We shall construct the codes in an elementary way from representations of the special linear group, $SL_2(q)$. A different elementary construction is given by J. H. van Lint and F. J. MacWilliams in [8].

Let $G$ be the group generated by the monomial matrices given as (1), (2) and (3) below. The rows and columns of each matrix are indexed by the elements of the projective line $GF(q) \cup \{\infty\}$. If $j \in GF(q)$ then we shall write $j = 0$, $j = \square$, or $j \neq \square$, according as $j$ is zero, $j$ is a non-zero square, or $j$ is a non-square respectively. We adopt the standard conventions about operations involving $\infty$.

(1) $T_i$, $i \in GF(q)$; the matrix corresponding to the permutation $(z \to z + i)$

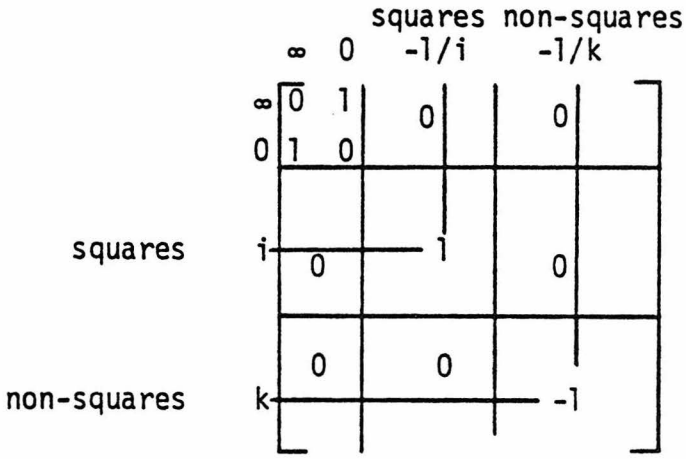
(2) $P_i$, $i = \square$; the matrix corresponding to the permutation $(z \to iz)$

and (3) a matrix $\tau$ corresponding to the permutation $(z \to -1/z)$ given by

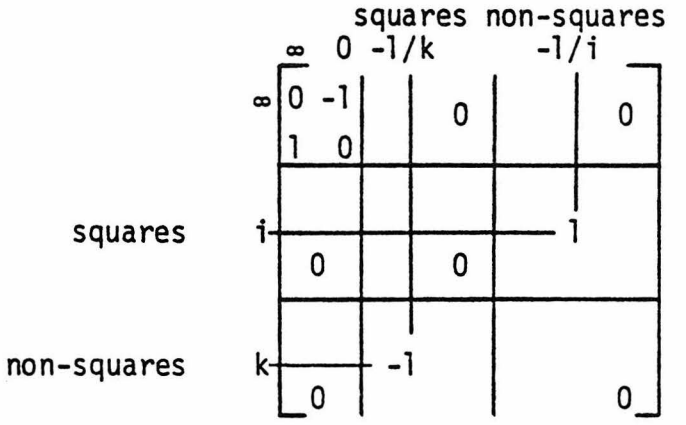
$$(\tau)_{ij} = \begin{cases} \varepsilon, & \text{if } j = 0 \text{ and } i = \infty \\ 1, & \text{if } j = \infty \text{ and } i = 0 \\ 1, & \text{if } j = -1/i \text{ and } i = \square \\ -1, & \text{if } j = -1/i \text{ and } i \neq \square \\ 0, & \text{otherwise} \end{cases}$$

where $\varepsilon = (-1)^{\frac{q-1}{2}}$.

If $q \equiv 1 \pmod 4$ then $\tau$ has the form




and if $q \equiv -1 \pmod 4$ then $\tau$ has the form



EXAMPLES. When $q = 5$,

$$\tau = \begin{array}{c|cc|cccc} & \infty & 0 & 1 & 2 & 3 & 4 \\ \hline \infty & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 & -1 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & -1 & 0 \\ 4 & 0 & 0 & 1 & 0 & 0 & 0 \end{array}$$

and when $q = 7$,

$$\tau = \begin{array}{c|cc|ccccc} & \infty & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline \infty & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 2 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 4 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 5 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 6 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \end{array}$$

If $q \equiv 1 \pmod 4$ then G affords a representation of $L_2(q)$. If $q \equiv -1 \pmod 4$ then G affords a representation of $SL_2(q)$. The subgroup

$$H = \left\{ \begin{bmatrix} a & d \\ 0 & a^{-1} \end{bmatrix} : a, d \in GF(q), a \neq 0 \right\}$$

of $SL_2(q)$ is the stabilizer of a one-dimensional subspace. The representations are induced from the linear representation of H with a kernel of index 2.

We define

$$\delta = \begin{cases} \sqrt{-q}, & \text{if } q \equiv -1 \pmod 4 \\ \sqrt{q}, & \text{if } q \equiv 1 \pmod 4 \end{cases}$$

The extended quadratic residue code $C(q)$ over $\mathbb{C}$ is the subspace of $V_{q+1}(\mathbb{C})$ spanned by the rows of the matrix $M(q)$ given below. The rows and columns of $M(q)$ are indexed by the elements of the projective line $GF(q) \cup \{\infty\}$.

$$M(q) = \begin{array}{c|c|c} & \infty & GF(q) \\ \hline \infty & \delta & 1 \ \ldots\ldots\ 1 \\ \hline GF(q) & \varepsilon \\ & \vdots & W + \delta I \\ & \varepsilon \end{array}$$

where

$$(W)_{ij} = \begin{cases} 0, & \text{if } j = i \\ 1, & \text{if } j - i = \square \\ -1, & \text{if } j - i \neq \square. \end{cases}$$

EXAMPLES. The code $C(5)$ over $\mathbb{C}$ is the row space of the matrix.

| | $\infty$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|---|
| $\infty$ | $\sqrt{5}$ | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | $\sqrt{5}$ | 1 | -1 | -1 | 1 |
| 1 | 1 | 1 | $\sqrt{5}$ | 1 | -1 | -1 |
| 2 | 1 | -1 | 1 | $\sqrt{5}$ | 1 | -1 |
| 3 | 1 | -1 | -1 | 1 | $\sqrt{5}$ | 1 |
| 4 | 1 | 1 | -1 | -1 | 1 | $\sqrt{5}$ |

and the code $C(7)$ over $\mathbb{C}$ is the row space of the matrix

$$M(7) = \begin{array}{c|cccccccc} & \infty & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline \infty & \sqrt{-7} & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & -1 & \sqrt{-7} & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & \sqrt{-7} & 1 & 1 & -1 & 1 & -1 \\ 2 & -1 & -1 & -1 & \sqrt{-7} & 1 & 1 & -1 & 1 \\ 3 & -1 & 1 & -1 & -1 & \sqrt{-7} & 1 & 1 & -1 \\ 4 & -1 & -1 & 1 & -1 & -1 & \sqrt{-7} & 1 & 1 \\ 5 & -1 & 1 & -1 & 1 & -1 & -1 & \sqrt{-7} & 1 \\ 6 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & \sqrt{-7} \end{array}$$

Let $n$ be a fixed non-square. We use the elements of the projective line $GF(q) \cup \{\infty\}$ to index the rows and columns of a matrix $\lambda$ and we set

$$(\lambda)_{ij} = \begin{cases} -1, & \text{if } i = j = \infty \\ 1, & \text{if } i \neq \infty \text{ and } j = ni \\ 0, & \text{otherwise} \end{cases}$$

We define $C(q)^* = C(q)\lambda$. When $q \equiv -1 \pmod 4$ we choose $n = (-1)$.

EXAMPLE. Choosing $n = 2$ we see that the code $C(5)^*$ is the row space of the matrix

$$\begin{array}{c|ccccc} & \infty & 0 & 1 & 2 & 3 & 4 \\ \hline \infty & -\sqrt{5} & 1 & 1 & 1 & 1 & 1 \\ 0 & -1 & \sqrt{5} & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & \sqrt{5} & -1 & 1 \\ 2 & -1 & -1 & 1 & 1 & -1 & \sqrt{5} \\ 3 & -1 & -1 & \sqrt{5} & -1 & 1 & 1 \\ 4 & -1 & 1 & 1 & -1 & \sqrt{5} & -1 \end{array}$$

THEOREM 1.1. The codes $C(q)$ and $C(q)^*$ are invariant under the group $G$ and are interchanged by $\lambda$.

If $q \equiv -1 \pmod 4$ then $C(q)$ and $C(q)^*$ are both self-dual and if $q \equiv 1 \pmod 4$ then $C(q)^* = C(q)^\perp$.

Figure 1 provides a summary of properties of $C(q)$ and $C(q)^*$.

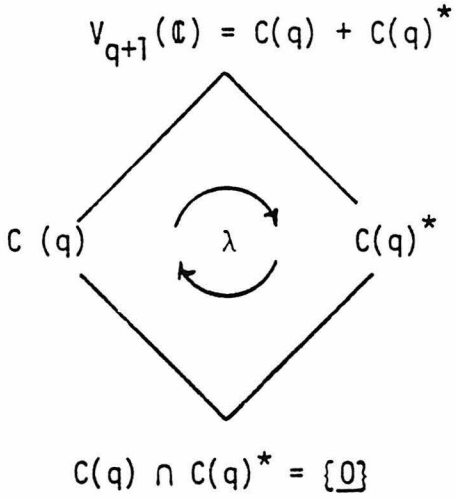



Figure 1.

PROOF. If $m_i$ is the row of $M(q)$ indexed by $i$ then

(1) $m_i T_j = m_{i+j}$, for $j \in GF(q)$,

(2) $m_i P_j = m_{ij}$, for $j = \square$,

and (3) $$m_i \tau = \begin{cases} \varepsilon m_0, & \text{if } i = \infty \\ m_\infty, & \text{if } i = 0 \\ m_{-1/i}, & \text{if } i = \square \\ -m_{-1/i}, & \text{if } i \neq \square \end{cases}$$

Thus $C(q)$ is invariant under $G$. Another calculation gives

(4) $\lambda^{-1} T_i \lambda = T_{i/n}$,

(5) $\lambda^{-1} P_i \lambda = P_i$,

and (6) $\lambda^{-1} \tau\lambda = -\tau(P_{n2})$.

We conclude that $\lambda^{-1} G\lambda \subseteq \langle G,-I\rangle$. Since the code $C(q)^*$ is invariant under $\lambda^{-1} G\lambda$, it is invariant under $G$. Since $\lambda^2 = P_{n2}$ and since $P_{n2}$ is an automorphism of $C(q)$ the matrix $\lambda$ interchanges $C(q)$ and $C(q)^*$.

If $q \equiv 1 \pmod 4$ then $m_\infty\lambda \perp m_i$ for all $i \in GF(q) \cup \{\infty\}$. If $M$ is a monomial matrix with each non-zero entry $\pm 1$ then multiplication by $M$ preserves the dot product. Thus $(m_\infty\lambda) M \perp C(q) M$ for all $M \in G$ and it follows that $C(q) \perp C(q)^*$. A similar argument proves that $C(q)$ and $C(q)^*$ are both self-orthogonal when $q \equiv -1 \pmod 4$. Since $\lambda$ is non-singular, $\dim C(q) = \dim C(q)^* \leq \frac{q+1}{2}$. Since $G$ acts transitively on the coordinate positions and since $m_\infty - m_\infty\lambda$ is a vector of weight 1, we have $C(q) + C(q)^* = V_{q+1}(\mathbb{C})$. The forces $C(q) \cap C(q)^* = \{\underline{0}\}$ and $\dim C(q) = \dim C(q)^* = \frac{q+1}{2}$.

REMARKS. Direct calculation reveals that $C(q)$ and $C(q)^*$ are both invariant under the matrix $\rho$ corresponding to the permutation $(z \to z^p)$, where $q = p^n$ and $p$ is prime. Let $\mathcal{G} = \langle G,\rho\rangle$.

If $\varepsilon q$ is a square in $GF(s)$ and if $s \neq 2^\alpha, p^\alpha$ then we may regard each vector $m_i$ as a vector in $V_{q+1}(s)$. The extended quadratic residue code $C(q)$ over $GF(s)$ is defined to be the $GF(s)$ span of the vectors $m_i$, where $i \in GF(q) \cup \{\infty\}$. The code $C(q)^*$ over $GF(s)$ is then the $GF(s)$ span of the vectors $m_i\lambda$, where $i \in GF(q) \cup \{\infty\}$. Since $\varepsilon q$ is a square in $GF(s^2)$ we may always define extended quadratic residue codes $C(q)$ and $C(q)^*$ over $GF(s^2)$. Every matrix in $\mathcal{G}$ has all non-zero entries $\pm 1$ and may be viewed over any finite

field. The same arguments that we used to prove Theorem 1.1 apply and all the conclusions of that theorem remain valid.

EXAMPLE. Since $11 \equiv -1 \pmod 4$ and since $-11 = (1)^2 \pmod 3$ the ternary code $C(11)$ is well defined. This code is the [12,6,6] ternary Golay code and it is the row space of the matrix given below

| | ∞ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ∞ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | -1 | 1 | 1 | -1 | 1 | 1 | 1 | -1 | -1 | -1 | 1 | -1 |
| 1 | -1 | -1 | 1 | 1 | -1 | 1 | 1 | 1 | -1 | -1 | -1 | 1 |
| 2 | -1 | 1 | -1 | 1 | 1 | -1 | 1 | 1 | 1 | -1 | -1 | -1 |
| 3 | -1 | -1 | 1 | -1 | 1 | 1 | -1 | 1 | 1 | 1 | -1 | -1 |
| 4 | -1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 | 1 | 1 | 1 | -1 |
| 5 | -1 | -1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 | 1 | 1 | 1 |
| 6 | -1 | 1 | -1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 | 1 | 1 |
| 7 | -1 | 1 | 1 | -1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 | 1 |
| 8 | -1 | 1 | 1 | 1 | -1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 |
| 9 | -1 | -1 | 1 | 1 | 1 | -1 | -1 | -1 | 1 | -1 | 1 | 1 |
| 10 | -1 | 1 | -1 | 1 | 1 | 1 | -1 | -1 | -1 | 1 | -1 | 1 |

Viewing the vectors $m_i$ as vectors in $V_{q+1}(2^\alpha)$ gives $m_i = \underline{1}$ for all $i \in GF(q) \cup \{\infty\}$. However the vectors $\frac{m_i \pm m_j}{2}$, $i, j \in GF(q) \cup \{\infty\}$, span $C(q)$ over $\mathbb{C}$, and the $\mathbb{Z}$-span of these vectors is invariant under $G$. The only entries that are not rational integers are $\frac{1\pm\delta}{2}$ and either negatives and $\frac{1\pm\delta}{2}$ are the roots of

$$f(z) = z^2 - z + (\frac{1-\delta^2}{4}) .$$

If $q \equiv \pm 1 \pmod 8$ then $f(z) \equiv z(z-1) \pmod 2$. Working over $GF(2)$ we take $\frac{(-1)+\delta}{2} = 1$, $\frac{1+\delta}{2} = 0$, and we set $m'_\infty = m_\infty$, and $m'_i = \frac{m_i + m_\infty}{2}$ for $i \in GF(q)$. The extended binary quadratic residue code $C(q)$ is

defined to be the row space of the matrix

$$\begin{matrix} & \infty \\ GF(q) & \end{matrix}\begin{bmatrix} m'_\infty \\ m'_i \end{bmatrix}$$

The vector $m'_\infty = \underline{1}$ and if $i \in GF(q)$ then

$$(m'_i)_j = \begin{cases} \frac{q-1}{2}, & \text{if } j = \infty \\ 1, & \text{if } j - i = \square \\ 0, & \text{otherwise} \end{cases}$$

Working over $GF(2)$ the matrix $\lambda$ is a permutation matrix. The binary code $C(q)^*$ is defined to be the $GF(2)$ span of the vectors $m'_i\lambda$, where $i \in GF(q) \cup \{\infty\}$. Working over $GF(2)$ the group $\mathcal{G}$ is a group of permutation matrices. The codes $C(q)$ and $C(q)^*$ remain invariant under $\mathcal{G}$ and the orthogonality properties of $C(q)$ and $C(q)^*$ also remain unchanged. We have $C(q) \cap C(q)^* = \{\underline{0},\underline{1}\}$ and

$$C(q) + C(q)^* = \{w : w \cdot \underline{1} = 0\}.$$

EXAMPLES. The binary code $C(7)$ is the row space of the matrix

| | $\infty$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|---|
| $\infty$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 2 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |
| 3 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 |
| 4 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |
| 5 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| 6 | 1 | 1 | 1 | 0 | 1 | 0 | 0 | 0 |

This is the [8,4,4] Hamming code.

If $x$ is a root of the polynomial

$$z^2 + z - 1 = 0$$

then $GF(9) = GF(3)(x)$.

We have

$$x^1 = x \qquad x^2 = 1 - x$$
$$x^3 = -(1+x) \qquad x^4 = -1$$
$$x^5 = -x \qquad x^6 = -1 + x$$
$$x^7 = 1 + x \qquad x^8 = 1$$

The binary code $C(9)$ is the row space of the matrix.

| | $\infty$ | 0 | 1 | (-1) | x | (1+x) | (x-1) | (-x) | (1-x) | -(1+x) |
|---|---|---|---|---|---|---|---|---|---|---|
| $\infty$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 |
| 1 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| -1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| x | 0 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 1+x | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 |
| x-1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| -x | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| 1-x | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 |
| -(1+x) | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 |

This code is a [10,5,4] code.

If $q \not\equiv \pm 1 \pmod 8$ then

$$f(z) \equiv z^2 + z + 1 \pmod 2$$

and so $f(z)$ splits in $GF(4)$ and in any field $GF(2^{2\alpha})$. Let $\omega \in GF(4)$ be a primitive cube root of unity and set $\frac{1+\delta}{2} = \omega$, and $\frac{(-1)+\delta}{2} = \omega^2$. Let $m'_\infty = m_\infty$ and $m'_i = \frac{m_\infty + m_i}{2}$ for $i \in GF(q)$. The

extended quadratic residue code $C(q)$ over $GF(4)$ is defined to be the row space of the matrix

$$\begin{matrix} \\ \infty \\ GF(q) \end{matrix}\begin{bmatrix} m'_\infty \\ m'_i \end{bmatrix}$$

The vector $m'_\infty = \underline{1}$ and if $i \in GF(q)$ then

$$(m'_i)_j = \begin{cases} \omega^\varepsilon, & \text{if } j = \infty \\ \omega, & \text{if } j = i \\ 1, & \text{if } j - i = \square \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

Working within $GF(4)$ the matrix $\lambda$ is a permutation matrix. The code $C(q)^*$ over $GF(4)$ is defined to be the $GF(4)$ span of the vectors $m'_i\lambda$, where $i \in GF(q) \cup \{\infty\}$. Working within $GF(4)$ the group $\mathcal{G}$ is a group of permutation matrices. Again the codes $C(q)$ and $C(q)^*$ remain invariant under $\mathcal{G}$ and the orthogonality properties of $C(q)$ and $C(q)^*$ are not changed. We also have $C(q) \cap C(q)^* = \langle 1 \rangle$, and $C(q) + C(q)^* = \{w : w \cdot \underline{1} = 0\}$.

EXAMPLE. The code $C(3)$ over $GF(4)$ is the row space of the matrix

$$\begin{matrix} & \infty & 0 & 1 & 2 \\ \infty & 1 & 1 & 1 & 1 \\ 0 & \omega^2 & \omega & 1 & 0 \\ 1 & \omega^2 & 0 & \omega & 1 \\ 2 & \omega^2 & 1 & 0 & \omega \end{matrix}$$

## 2. A SQUARE ROOT BOUND ON THE MINIMUM WEIGHT.

Let $F$ be a field and suppose that the extended quadratic residue codes $C(q)$ and $C(q)^*$ are defined over $F$. Let $Q$ and $Q^*$ be the subspaces of $V_q(F)$ obtained from $C(q)$ and $C(q)^*$ respectively

by taking each codeword and deleting the entry indexed by $\infty$. The matrix $\lambda$ and the matrices $T_i$, $i \in GF(q)$ fix the coordinate position indexed by $\infty$. The two codes $Q$ and $Q^*$ are invariant under the group $T = \langle T_i : i \in GF(q) \rangle$ and have the properties described in Figure 2.

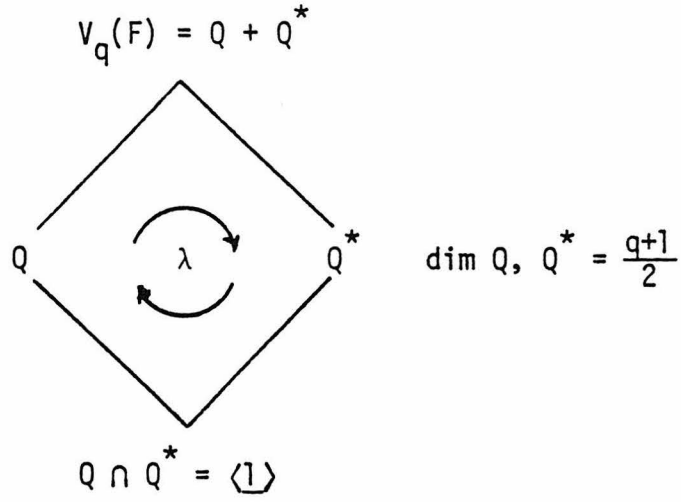



Figure 2.

The map

$$\gamma : (\ldots, c_i, \ldots) \to \sum_{i \in GF(q)} c_i T_i$$

is a vector space isomorphism between $V_q(F)$ and the group algebra $A$ over $F$ with basis the matrices in $T$. Since

$$(\sum c_i T_i)\, T_j = \sum c_i T_{i+j}$$

the map $\gamma$ is an A-module homomorphism and we may regard $Q$ and $Q^*$ as ideals in the commutative algebra $A$. Since the matrices $T_i$ are linearly independent in $A$ the map

$$(\sum c_i T_i) \to (\sum c_i)$$

from $A$ to $F$ is well defined. This substitution map is a ring homomorphism.

THEOREM 2.1. If $d$ is the minimum weight in $C(q)$ then

(1) $(d-1)^2 \geq q$

and (2) if $q \equiv -1 \pmod 4$ then

$$(d-1)^2 - (d-1) + 1 \geq q.$$

PROOF. Since $G$ acts transitively on the coordinate positions there exists

$$v = (a_\infty, \ldots, a_i, \ldots) \in C(q)$$

with $a_\infty = 1$ and $wt(v) = d$. Since $v$ is orthogonal to $(\delta, 1, \ldots 1)$ or to $(-\delta, 1, \ldots, 1)$ we have $\sum_{i \in GF(q)} a_i = \pm\delta$. Now

$$v_1 = (\sum a_i T_i) \in Q \quad \text{and} \quad v_1\lambda = (\sum a_i T_{ni}) \in Q^*.$$

The product $v_1(v_1\lambda) \in QQ^*$ and since $QQ^* \subseteq Q \cap Q^*$ we have

$$v_1(v_1\lambda) = (\sum a_i T_i)(\sum a_i T_{ni}) = k(\sum T_i) \qquad (2)$$

where $k \in F$. The substitution map gives

$$qk = (\sum a_i)^2 = \varepsilon q \neq 0.$$

The number of different non-zero terms on the left-hand side of (2) is at most $(d-1)^2$. This proves (1).

When $q \equiv -1 \pmod 4$, we have $n = -1$, and (2) becomes

$$v_1(v_1\lambda) = (\sum a_i T_i)(\sum a_i T_{-i}) = (-1)(\sum T_i) \qquad (3)$$

The number of different non-zero terms on the left-hand side of (3) is at most $(d-1)^2 - (d-1) + 1$. This proves (2).

REMARKS. A different proof of theorem 2.1 is given by J. H. van Lint and F. J. MacWilliams in [8]. Equality holds in (1) for the binary code $C(9)$ and equality holds in (2) for the binary Hamming code $C(7)$.

In [19] H. N. Ward proves that whatever the field $F$, the minimum weight in the code $C(q^2)$ over $F$ is always $q + 1$.

H.C.A. van Tilborg [18] generalized theorem 1.2 as follows

THEOREM 2.2. Suppose $q \equiv -1 \pmod 8$ is prime. Let $d$ be the minimum weight in the binary code $C(q)$. Then

(a) If $(d-1)^2 - (d-1) + 1 > q$ then $(d-1)^2 - (d-1) + 1 \geq q + 12$

and (b) If $(d-1)^2 - (d-1) + 1 = q$ then $d = 8t + 4$ and $q = 64t^2 + 40t + 7$ for some $t$. Furthermore there exists a projective plane of order $(d-2)$.

Part (a) of theorem 2.2 also holds when $q$ is a prime power. The proof rests on analysis of (3) and is essentially the same as that given in [18]. In chapter 5 we shall prove that $(d-1)^2 - (d-1) + 1 = q$ only if $q = 7$ and $d = 4$. Theorem 2.3 is an intermediate result. It is a special case of a theorem of E. F. Assmus, Jr., H. F. Mattson, Jr., and H. E. Sachar [1].

THEOREM 2.3. Let $q \equiv -1 \pmod 8$ be an odd prime power. Suppose the minimum weight $d$ in the binary code $C(q)$ satisfies

$$(d-1)^2 - (d-1) + 1 = q .$$

Then the vectors of minimum weight $(d-1)$ in $Q$ are the lines of a projective plane of order $(d-2)$.

PROOF. We identify a vector $v \in V_q(2)$ with the set of field elements that index the non-zero entries of $v$. Equation (3) reveals that the vector $v_1 \in Q$ is a difference set in the elementary abelian group $GF(q)$. The corresponding symmetric block design is the projective plane $PG(2,d-2)$. The lines of this projective plane are the vectors

$v_1T_j$, $j \in GF(q)$.

Let $w \in Q$ be a vector of minimum weight $(d-1)$. Since the code $C(q)$ is self-orthogonal the vector $w$ meets every line in an odd number of points. There is a line $v_1T_k$ that meets $w$ in at least 3 points. If there is a point $P$ of $v_1T_k$ not on $w$ then every other line through $P$ also meets $w$. But this forces $wt(w) \geq (d-2) + 3$ contradicting the choice of $w$. We conclude that $w = v_1T_k$ as required.

## CHAPTER 3. QUASI-CYCLIC BINARY CODES.

We establish a square root bound on the minimum weight in the quasi-cyclic binary codes constructed by V. K. Bhargava, S. E. Tavares, and S.G.S. Shiva [2]. The proof rests on viewing the codes as ideals in a group algebra over GF(4). Theorem 2.6 answers a question raised by F. J. MacWilliams and N.J.A. Sloane in "The Theory of Error-Correcting Codes" [10]. Theorems 2.3, 2.4 and 2.5 provide information about the way the non-zero entries of a codeword of minimum weight are distributed among the coordinate positions.

Let $q \equiv 3 \pmod 8$ be an odd prime power. The quasi-cyclic binary code $C(q)$ is that subspace of $V_{2q+2}(2)$ spanned by the rows of the matrix $M(q)$ given below. The rows of $M(q)$ are indexed by the elements of the projective line $GF(q) \cup \{\infty\}$. The columns are indexed by two copies of the projective line distinguished by the letters $\ell$ and $r$.

$$M(q) = GF(q) \quad \begin{array}{c|c|c|c|c} & \multicolumn{2}{c|}{GF(q)} & & GF(q) \\ & \ell_\infty \; \ell_0 \quad\quad \ell_i & & r_\infty \; r_0 \quad\quad r_i & \\ \infty & 0 \; 0 \; . \; . \; . \; . \; 0 & & 1 \; 1 \; . \; . \; . \; . \; 1 & \\ \hline 0 & 1 & & 0 & \\ i & \vdots \quad I_q & & \vdots \quad S & \\ & 1 & & 0 & \end{array} \qquad (1)$$

where

$$(S)_{ij} = \begin{cases} 1, & \text{if } j - i = \square \text{ or if } j = i \\ 0, & \text{otherwise} \end{cases}$$

EXAMPLE. The code $C(3)$ is the row space of the matrix

$$M(3) = \begin{array}{c|cccc|cccc} & \ell_\infty & \ell_0 & \ell_1 & \ell_{(-1)} & r_\infty & r_0 & r_1 & r_{(-1)} \\ \infty & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ (-1) & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \end{array}$$

The code $C(3)$ is the $[8,4,4]$ Hamming code. In general if $q$ is prime then $S$ is a circulant matrix.

We always have $\dim C(q) = q + 1$ and since

$$SS^T = (\tfrac{q+1}{4})\, I + (\tfrac{q+1}{4})\, J$$

$$\equiv I + J \pmod 2,$$

it follows that $C(q)$ is self-dual. Note that every row of the matrix $M(q)$ has weight divisible by 4. Since $C(q)$ is self-orthogonal it follows by induction that any sum of the rows of $M(q)$ has weight divisible by 4. Thus all weights in $C(q)$ are divisible by 4.

It is straightforward to prove that the automorphism group $\mathrm{Aut}(C(q))$ contains

(i) a permutation

$$\tau = (\ell_\infty r_\infty)(\ell_0 r_0) \cdots\cdots (\ell_i r_{-i}) \cdots\cdots$$

which interchanges the $\ell$ and $r$ coordinates in (1),

and (ii) the permutations in $P\Gamma L(2,q)$ applied simultaneously to the $\ell$ and $r$ coordinates in (1).

Recall that the group $P\Gamma L(2,q)$ consists of all permutations of $GF(q) \cup \{\infty\}$ that have the form $\left(z \to \frac{az^{\sigma}+b}{cz^{\sigma}+d}\right)$, with $a, b, c, d \in GF(q)$, $ad - bc$ a non-zero square and $\sigma$ an automorphism of $GF(q)$. Let $T_i = (z \to z + i)$ for $i \in GF(q)$.

## 2. A SQUARE ROOT BOUND ON THE MINIMUM WEIGHT.

Let

$$v = (a_\infty, \ldots, a_i, \ldots; b_\infty, \ldots, b_i, \ldots) \tag{2}$$

be a vector in $C(q)$. Let

$$d_1(v) = |\{i \in GF(q) : a_i \neq 0\}|,$$

and

$$d_2(v) = |\{i \in GF(q) : b_i \neq 0\}|.$$

Since $C(q)$ is self-orthogonal and since $(\underline{1};\underline{0})$ and $(\underline{0};\underline{1})$ are vectors in $C(q)$ we have

$$a_\infty = \sum_{i \in GF(q)} a_i \quad \text{and} \quad b_\infty = \sum_{i \in GF(q)} b_i \tag{3}$$

LEMMA 2.1. If $(a;b) \in C(q)$ then $(a+b;a)$ and $(b;a+b) \in C(q)$.

PROOF. Note that if $(a;b) \in C(q)$ and $(a+b;a) \in C(q)$ then so is $(b;a+b)$. The code $C(q)$ is the row space of $M(q)$ and it suffices to prove the lemma for the rows of this matrix. Let $M_i$ be the row of $M(q)$ indexed by $i$. If the lemma holds for $M_0$ then it holds for $M_i$, $i \neq \infty$, because $M_i$ is obtained from $M_0$ by applying the permutation $T_i$ simultaneously to the $\ell$ and $r$ coordinates in (1). Now $M_\infty = (\underline{0};\underline{1})$ and $(\underline{0}+\underline{1};\underline{0}) \in C(q)$. It remains to show that $c = (1,f;1,1,0,\ldots,0) \in C(q)$ where $f \in V_q(2)$ and $(f)_j = 1$

if and only if $j$ is a non-zero square. If $j \in GF(q)$ then let $n_j$ be the number of times $(j - i)$ is a square (or $j - i = 0$) as $i$ runs through the non-zero squares in $GF(q)$. We set $q = 8m + 3$. We have $n_0 = 0$ and if $j \neq 0$ then Perron's theorem (pg. 519 of [10] and [13]) reveals that $n_j = 2m + 1$. It follows that

$$c = M_\infty + \sum_{\substack{i \in GF(q) \\ i \text{ a non-zero square}}} M_i$$

and the proof is complete.

We now view the binary code $C(q)$ as a code of length $(q+1)$ over $GF(4)$. F. J. MacWilliams and M. Karlin were the first to employ this technique and further information may be found on page 508 of [10]. Let $\omega \in GF(4)$ be a primitive cube root of unity and let $\gamma : V_{2q+2}(2) \to V_{q+1}(4)$ be given by

$$\gamma : (a_\infty, \ldots, a_i, \ldots; b_\infty, \ldots, b_i, \ldots) \to (c_\infty, \ldots, c_i, \ldots)$$

where

$$c_i = \begin{cases} 0, & \text{if } a_i = b_i = 0 \\ \omega, & \text{if } a_i = 1 \text{ and } b_i = 0 \\ \omega^2, & \text{if } a_i = 0 \text{ and } b_i = 1 \\ 1, & \text{if } a_i = b_i = 1 \end{cases}$$

Since $\omega^2 + \omega + 1 = 0$ we have $\gamma(x+y) = \gamma(x) + \gamma(y)$. The map $\gamma$ identifies $C(q)$ with the extended quadratic residue code (QR code) of length $(q+1)$ over $GF(4)$ (see chapter 2, page 18). The extended QR code is spanned by $\underline{1}$ and the vectors $xT_i$, $i \in GF(q)$,

where

$$(x)_j = \begin{cases} \omega^2, & \text{if } j = \infty \\ \omega, & \text{if } j = 0 \\ 1, & \text{if } j = \square \\ 0, & \text{otherwise} \end{cases}$$

If $v = (a;b) \in V_{2q+2}$ then $\gamma(v) = \omega a + \omega^2 b$. Note that

$$\gamma(a+b;a) = \omega^2(\omega a + \omega^2 b)$$

and

$$\gamma(b;a+b) \quad \omega(\omega a + \omega^2 b).$$

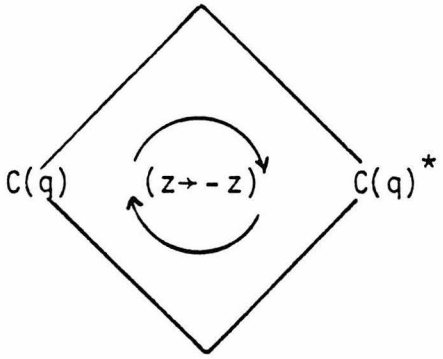
EXAMPLE. The map $\gamma$ identifies $C(3)$ with the row space of the matrix

$$\begin{array}{c} \infty \quad 0 \quad 1 \quad (-1) \\ \begin{bmatrix} 1 & 1 & 1 & 1 \\ \omega & 1 & \omega^2 & 0 \\ \omega & 0 & 1 & \omega^2 \\ \omega & \omega^2 & 0 & 1 \end{bmatrix} \end{array}$$

Thus we may regard $C(3)$ as an extended cyclic [4,2] code over GF(4).

Define $C(q)^* = C(q)\phi$, where $\phi$ is the permutation $(z \to -z)$ applied simultaneously to the $\ell$ and $r$ coordinates in (1). Note that $q \equiv -1 \pmod 4$ and so $(-1)$ is a non-square in GF(q). The map $\gamma$ identifies the binary code $C(q)^*$ with the complementary extended QR code of length $(q+1)$ over GF(4). In chapter 2 we proved that the codes have the properties described in Figure 1.

$$C(q) + C(q)^* = \{t \in V_{q+1}(4) : t \cdot \underline{1} = 0\}$$



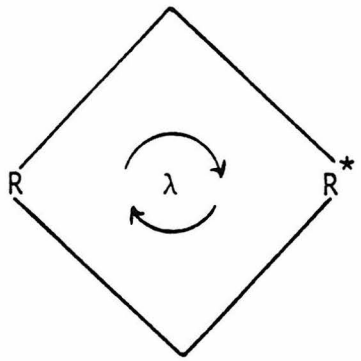

$$\dim C(q),\ C(q)^* = \frac{q+1}{2}$$

$$C(q) \cap C(q)^* = \langle \underline{1} \rangle$$

Figure 1.

Let $R$ and $R^*$ be those subspaces of $V_q(4)$ obtained from $C(q)$ and $C(q)^*$ respectively by taking each codeword and deleting that entry indexed by $\infty$. Let $\lambda$ be the permutation of $GF(q)$ given by $(z \to -z)$. Then the subspaces $R$ and $R^*$ have the properties described in Figure 2.

$$V_q(4) = R + R^*$$




$$\dim R,\ R^* = \frac{q+1}{2}$$

$$R \cap R^* = \langle \underline{1} \rangle$$

Figure 2.

The two codes $R$ and $R^*$ are invariant under the group $T = \langle T_i : i \in GF(q) \rangle$. The map

$$\xi : (c_0,\ldots,c_i,\ldots) \to \sum_{i \in GF(q)} c_i T_i$$

is a vector space isomorphism between $V_q(4)$ and the group albegra $A$ over $GF(4)$ with basis the permutations in $T$. Since

$$(\sum c_i T_i)\, T_j = \sum c_i T_{i+j},$$

the map $\xi$ is an $A$-module homomorphism. Each subspace in Figure 2 corresponds to an ideal in $A$. Since the permutations $T_i$ are linearly independent in $A$ the map

$$(\sum c_i T_i) \to (\sum c_i)$$

from $A$ to $GF(4)$ is well defined. This substitution map is a ring homomorphism.

Let $d$ be the minimum weight in the binary code $C(q)$. Define

$$\Omega^* = \{v = (a;b) \in C(q) : a_\infty = b_\infty = 1 \text{ and } wt(v) = d\}$$

and $$\Omega = \{v = (a;b) \in C(q) : a_\infty = 1, b_\infty = 0 \text{ and } wt(v) = d\}.$$

We have not been able to prove that $\Omega^*$ is always non-empty but we do have

LEMMA 2.2. (1) The set $\Omega$ is non-empty.

(2) If $x \in \Omega$ and $d_1(x) > d_2(x)$ then either

(i) $q = 3$ and $x = (\underline{1}:\underline{0})$

or (ii) there exists $v \in \Omega$ with $d_2(v) = d_1(x) + 1$
$d_1(v) = d_2(x) - 1$.

(3) If $v \in \Omega$ and $d_2(v) > d_1(v)$ then there exists $x \in \Omega$ with $d_1(x) = d_2(v) - 1$ and $d_2(x) = d_1(v) + 1$.

PROOF. (1) Let $v = (a;b)$ be a codeword of minimum weight. Suppose that for all $i \in GF(q) \cup \{\infty\}$ we either have $a_i = b_i = 1$, or $a_i = 1$ and $b_i = 0$, or $a_i = 0$ and $b_i = 0$. Then $(b;a+b) \in C(q)$ and $wt(b;a+b) \leq wt(a;b)$, with equality only if $b = \underline{0}$. If $b = \underline{0}$ then analysis of $M(q)$ shows $a = \underline{1}$. In particular $v \neq (a;a)$ for any $a \in V_{q+1}(2)$. By applying a suitable automorphism we may choose $v = (a;b)$ so that $a_\infty = 1$ and $b_\infty = 0$.

(2) Let $x = (c;d) \in \Omega$ with $d_1(x) > d_2(x)$. If $x \neq (\underline{1};\underline{0})$ then the argument of part (1) reveals that there exists $j \in GF(q)$ with $d_j = 1$ and $c_j = 0$. Let $\sigma$ be an automorphism that interchanges the indices $j$ and $\infty$, and let $v = (x)\sigma\tau$. Then $d_2(v) = d_1(x) + 1$ and $d_1(v) = d_2(x) - 1$ as required. If $(\underline{1};\underline{0}) \in \Omega$ then the minimum weight $d$ is $(q+1)$. But by a theorem of C. L. Mallows and N.J.A. Sloane [11] we must have

$$d \leq 4\left[\frac{2q+2}{24}\right] + 4,$$

and so $q = 3$.

(3) is proved in the same way as (2) and we omit the details.

We now define

$$t = \max_{v \in \Omega}\{|d_2(v) - d_1(v)|\}$$

THEOREM 2.3. If $\Omega^*$ is non-empty and if

$$s = \max_{v \in \Omega^*}\{|d_1(v) - d_2(v)|\}$$

then the minimum weight $d$ satisfies

$$(d-1)^2 - (d-1) + 1 - st \geq 2q + 1 \qquad (4)$$

PROOF. Let

$$x = (1,\ldots,a_i,\ldots;0,\ldots,b_i,\ldots) \in \Omega$$

with $d_1(x) = \left(\frac{(d-1)-t}{2}\right)$ and $d_2(x) = \left(\frac{(d-1)+t}{2}\right)$. Since $\tau \in \mathrm{Aut}(C(q))$ there exists

$$v = (1,\ldots,c_i,\ldots;1,\ldots,d_i,\ldots) \in \Omega^*$$

with $d_1(v) = \left(\frac{(d-2)+s}{2}\right)$ and $d_2(v) = \left(\frac{(d-2)-s}{2}\right)$. Now

$$v_1 = \omega \sum c_i T_i + \omega^2 \sum d_i T_i \in R$$

and

$$x_1 = \omega \sum a_i T_{-i} + \omega^2 \sum b_i T_{-i} \in R^*.$$

Since $A$ is a commutative algebra $RR^* \subseteq R \cap R^*$ and we have

$$\begin{aligned} v_1 x_1 &= \omega^2(\Sigma c_i T_i)(\Sigma a_i T_{-i}) + \omega(\Sigma d_i T)(\Sigma b_i T_{-i}) \\ &\quad + (\Sigma d_i T_i)(\Sigma a_i T_{-i}) + (\Sigma c_i T_i)(\Sigma b_i T_{-i}) \\ &= k_1\omega(\Sigma T_i) + k_2\omega^2(\Sigma T_i), \end{aligned} \tag{5}$$

where $k_1, k_2 \in GF(2)$. Since $1 = \omega + \omega^2$, the substitution map gives

$$k_1 = (\Sigma d_i)(\Sigma b_i) + (\Sigma d_i)(\Sigma a_i) + (\Sigma c_i)(\Sigma b_i)$$

and

$$k_2 = (\Sigma c_i)(\Sigma a_i) + (\Sigma d_i)(\Sigma a_i) + (\Sigma c_i)(\Sigma b_i)$$

Now (3) reveals that $k_1 = 1$ and $k_2 = 0$. Since $k_2 = 0$ we have

$$(\Sigma c_i T_i)(\Sigma a_i T_{-i}) = (\Sigma d_i T_i)(\Sigma a_i T_{-i}) + (\Sigma c_i T_i)(\Sigma b_i T_{-i})$$

and so (5) gives

$$(\Sigma T_i) = (\Sigma d_i T_i)(\Sigma b_i T_{-i}) + (\Sigma c_i T_i)(\Sigma a_i T_{-i}). \tag{6}$$

Counting non-zero coefficients in (6) gives

$$\left(\frac{(d-2)-s}{2}\right)\left(\frac{(d-1)+t}{2}\right) + \left(\frac{(d-2)+s}{2}\right)\left(\frac{(d-1)-t}{2}\right) \geq q.$$

This reduces to (4) and the theorem is proved.

REMARKS. If $v \in \Omega$ then (3) implies that $d_1(v)$ is odd and $d_2(v)$ is even. Thus $t$ is odd and so is not 0. If $v \in \Omega^*$ then $d_1(v)$ and $d_2(v)$ are both odd and $d_1(v) + d_2(v) = d - 2$. Since $d \equiv 0 \pmod 4$ we have $d_1(v) \equiv d_2(v) \pmod 4$ and so $s$ is a multiple of 4.

When $q = 3$, we have $d = 4$ and $(d-1)^2 - (d-1) + 1 = 2q + 1$. The set $\Omega^*$ consists of the three vectors given below.

$$\begin{array}{rccccccccc} & \ell_\infty & \ell_0 & \ell_1 & \ell_{(-1)} & & r_\infty & r_0 & r_1 & r_{(-1)} \\ x_1 = ( & 1 & 1 & 0 & 0 & ; & 1 & 0 & 0 & 1 \ ) \\ x_2 = ( & 1 & 0 & 1 & 0 & ; & 1 & 1 & 0 & 0 \ ) \\ x_3 = ( & 1 & 0 & 0 & 1 & ; & 1 & 0 & 1 & 0 \ ) \end{array}$$

Notice that $s = 0$.

The code $C(11)$ is the [24,12,8] Golay code. If

$$\begin{array}{rcccccccccccccccccccccccc} & \infty & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \infty & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ x = ( & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & ; & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \ \ 0 ) \\ v = ( & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & ; & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \ \ 0 ) \end{array}$$

and

then it is straightforward to check that $x \in \Omega$ and $v \in \Omega^*$. Note that

$$(\Sigma T_i) = T_0(T_0 + T_{-1} + T_{-3} + T_{-4} + T_{-5} + T_{-9}) + (T_1 + T_3 + T_4 + T_5 + T_9)T_0$$

as predicted by (6). Notice that $s = 4$, $t = 5$ and

$$(d-1)^2 - (d-1) + 1 - st = 2q + 1.$$

By lemma 2.2, or by inspection when $q = 3$, there exist vectors $v \in \Omega$ with $d_2(v) > d_1(v)$. We now define

$$r = \min_{\substack{d_2(v) > d_1(v) \\ v \in \Omega}} \{d_2(v) - d_1(v)\}$$

THEOREM 2.4. The minimum weight $d$ satisfies

$$\frac{(d-1)^2}{2} + \frac{(r-2)^2}{2} - (d-1) + 1 \geq q \tag{7}$$

PROOF. By part (3) of lemma 2.2 there exists

$$x = (1,\ldots,a_i,\ldots;0,\ldots,b_i,\ldots) \in \Omega$$

with $d_1(x) = \left(\frac{(d-1)+(r-2)}{2}\right)$ and $d_2(x) = \left(\frac{(d-1)-(r-2)}{2}\right)$. Now

$$x_1 = \omega(\sum a_i T_i) + \omega^2(\sum b_i T_i) \in R$$
$$x_1\lambda = \omega(\sum a_i T_{-i}) + \omega^2(\sum b_i T_{-i}) \in R^*.$$

Since $x_1(x_1\lambda) \in R \cap R^*$ we have

$$\begin{aligned} x_1(x_1\lambda) &= \omega^2(\sum a_i T_i)(\sum a_i T_{-i}) + \omega(\sum b_i T_i)(\sum b_i T_{-i}) \\ &+ (\sum a_i T_i)(\sum b_i T_{-i}) + (\sum b_i T_i)(\sum a_i T_{-i}) \\ &= k_1\omega(\sum T_i) + k_2\omega^2(\sum T_i) \end{aligned}$$

where $k_1, k_2 \in GF(2)$. Applying the substitution map reveals $k_1 = 0$ and $k_2 = 1$. We conclude that

$$(\sum T_i) = (\sum a_i T_i)(\sum a_i T_{-i}) + (\sum b_i T_i)(\sum b_i T_{-i}). \tag{8}$$

Counting non-zero coefficients in (8) gives

$$\left(\frac{(d-1)+(r-2)}{2}\right)^2 + \left(\frac{(d-1)-(r-2)}{2}\right)^2 - (d-1) + 1 \geq q$$

This reduces to (7) and the theorem is proven.

REMARK. When $q = 3$, we have $d = 4$ and $r = 1$, and equality holds in (7).

THEOREM 2.5. The minimum weight $d$ satisfies

$$\frac{(d-1)^2}{2} - \frac{t^2}{2} + t \geq q \tag{9}$$

PROOF. By (3) of lemma 2.2 there exists

$$v = (1,\ldots,a_i,\ldots;0,\ldots,b_i,\ldots) \in \Omega$$

with $d_1(v) = \left(\frac{(d-1)-t}{t}\right)$ and $d_2(v) = \left(\frac{(d-1)+t}{2}\right)$, and

$$x = (1,\ldots,c_i,\ldots;0,\ldots,d_i,\ldots) \in \Omega$$

with $d_1(x) = \frac{(d-1)+(t-2)}{2}$ and $d_2(x) = \frac{(d-1)-(t-2)}{2}$. Now

$$v_1 = \omega(\sum a_i T_i) + \omega^2(\sum b_i T_i) \in R$$

and

$$x_1 = \omega(\sum c_i T_{-i}) + \omega^2(\sum d_i T_{-i}) \in R^*.$$

The arguments used to prove theorems 2.3, 2.4, and 2.5 show that $v_1 x_1 = \omega^2(\sum T_i)$ and that

$$(\sum T_i) = (\sum a_i T_i)(\sum c_i T_{-i}) + (\sum b_i T_i)(\sum d_i T_{-i}) \qquad (10)$$

Counting non-zero coefficients in (10) gives

$$\left(\frac{(d-1)-t}{2}\right)\left(\frac{(d-1)+(t-2)}{2}\right) + \left(\frac{(d-1)+t}{2}\right)\left(\frac{(d-1)-(t-2)}{2}\right) \geq q$$

This reduces to (9) and the theorem is proven.

THEOREM 2.6. The minimum weight $d$ satisfies

$$(d-1)^2 - (d-1) + 1 \geq 2q + 1 \qquad (11)$$

If equality holds in (11) then $q = 3$ and $d = 4$.

PROOF. If $t \leq \sqrt{d-1} + 1$ then theorem 2.4 gives

$$\frac{(d-1)^2}{2} - \frac{(d-1)}{2} \geq q$$

and (11) holds. If $t = \sqrt{d-1} + s$ then theorem 2.5 gives

$$\frac{(d-1)^2}{2} - \frac{(d-1)}{2} - \sqrt{d-1}\,(s-1) - s\left(\frac{s}{2}-1\right) \geq q$$

and (11) holds even when $s = 1$. This proves (11).

If equality holds in (11) then theorem 2.4 gives

$$(t-2)^2 \geq (d-3) \tag{12}$$

and theorem 2.5 gives

$$t(t-2) \leq (d-1). \tag{13}$$

Equations (12) and (13) force $d = 4$. If $d = 4$ then (11) implies $q = 3$ and the proof is complete.

REMARKS. Let Q be an $[\ell+1, \frac{\ell+1}{2}]$ extended QR code over any finite field where the prime power $\ell \equiv -1 \pmod 8$. If d is the minimum weight in Q then

$$(d-1)^2 - (d-1) + 1 \geq L. \tag{14}$$

In [10] F. J. MacWilliams and N.J.A. Sloane asked if there was a square root bound on the minimum weight in the double circulant binary codes analogous to (14). Theorem 2.6 answers this question. Theorems 2.3, 2.4, and 2.5 also give information about the way the non-zero entries of a codeword of minimum weight are distributed among the coordinate positions.

Figure 3, below, is taken from page 509 of [10] and is a list of parameters of the first few quasi-cyclic binary code C(q). Here n is the block length, k is the dimension and d is the minimum distance.

| | n | k | d |
|---|---|---|---|
| C(3) | 8 | 4 | 4 |
| C(11) | 24 | 12 | 8 |
| C(19) | 40 | 20 | 8 |
| C(27) | 56 | 28 | 12 |
| C(43) | 88 | 44 | 16 |
| C(53) | 108 | 54 | 20 |

Figure 3.

Sometimes theorem 2.6 allows us to calculate the minimum weight $d$ directly. If $q = 27$ then $4|d$ and $(d-1)^2 - (d-1) + 1 \geq 55$. We conclude that $d \geq 12$. But by a theorem of C. L. Mallows and N.J.A. Sloane [11].

$$d \leq 4\left[\frac{56}{24}\right] + 4$$

i.e., $d \leq 12$. Hence $C(27)$ is a [56,28,12] code.

The results presented in Chapter 3 will appear in the IEEE Transactions on Information Theory.

## CHAPTER 4. SYMMETRY CODES

We begin by extending the construction for symmetry codes given by V. Pless [14] to fields other than GF(3). We then prove a decomposition theorem for these codes in terms of the extended quadratic residue codes introduced in chapter 2. Theorem 2.5 gives a square root bound on the minimum weight in this enlarged family of symmetry codes.

Let $q$ be an odd prime power. Again if $j \in GF(q)$ then we write $j = 0$, $j = \square$, or $j \neq \square$ according as $j$ is zero, $j$ is a non-zero square, or $j$ is a non-square respectively. Let $F$ be a finite field of odd characteristic for which $(-q) = \square$, and set $\theta = \sqrt{-q}$. The symmetry code $S(q)$ over $F$ is the subspace of $V_{2q+2}(F)$ spanned by the rows of the matrix $M(q)$ given below. The rows of $M(q)$ are indexed by the elements of the projective line $GF(q) \cup \{\infty\}$. The columns are indexed by two copies of the projective line distinguished by the letters $\ell$ and $r$.

$$M(q) = \begin{array}{c} \\ \infty \\ 0 \\ GF(q)\ i \end{array} \begin{array}{c} \begin{array}{cccccc} GF(q) & & & & GF(q) & \\ \ell_\infty & \ell_0 & \cdots & \ell_i & r_\infty & r_0 \quad \cdots \quad r_i \end{array} \\ \left[\begin{array}{c|ccc|c|ccc} \theta & 0 & \cdots & 0 & 0 & 1 & \cdots & 1 \\ \hline 0 & & & & \varepsilon & & & \\ \vdots & & & & \vdots & & & \\ 0 & & \theta I & & \varepsilon & & W & \end{array}\right] \end{array} \qquad (1)$$

where $\varepsilon = (-1)^{(\frac{q-1}{2})}$, and where

$$(W)_{ij} = \begin{cases} 0, & \text{if } i = j \\ 1, & \text{if } j - i = \square \\ -1, & \text{if } j - i \neq \square \end{cases}$$

Notice that $W = \varepsilon W^T$. If $q \equiv -1 \pmod 3$ then $(-q) = (1)^2$ and the ternary symmetry code $S(q)$ is defined. V. Pless constructs ternary symmetry codes in [14] and investigates their properties in [15,16, and 17].

EXAMPLE. The ternary symmetry code $S(5)$ is the row space of the matrix

$$M(5) = \begin{array}{c|c|cccccc|cccccc} & \ell_\infty & \ell_0 & \ell_1 & \ell_2 & \ell_3 & \ell_4 & r_\infty & r_0 & r_1 & r_2 & r_3 & r_4 \\ \hline \infty & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & -1 & -1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & -1 & -1 \\ 2 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & -1 & 1 & 0 & 1 & -1 \\ 3 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & -1 & -1 & 1 & 0 & 1 \\ 4 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & -1 & -1 & 1 & 0 \end{array} \qquad (2)$$

This is the [12,6,6] ternary Golay code.

We always have $\dim S(q) = (q+1)$. Perron's theorem [13] gives

$$WW^T = qI - J$$

and so $$M(q)\, M(q)^T = \theta^2 + qI = 0.$$

It follows that $S(q)$ is self-dual. If $\phi = \begin{bmatrix} 0 & I_{q+1} \\ -\varepsilon I_{q+1} & 0 \end{bmatrix}$

then

$$M(q)(M(q)\phi)^T = \theta \left[\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & -\varepsilon W^T + W & \\ 0 & & & \end{array}\right] = 0 .$$

and so $\phi$ is an automorphism of $S(q)$.

Suppose $q \equiv -1 \pmod 4$. On page 12 of chapter 2 we defined the extended quadratic residue code $C(q)$ over $F$ to be the row space of the matrix $H$ given below

$$H = \begin{array}{c} \\ \infty \\ i \end{array} \overset{\begin{array}{cc} \infty & \quad i \end{array}}{\left[\begin{array}{c|ccc} \theta & 1 & \cdots & 1 \\ \hline -1 & & & \\ \vdots & & W + \theta I & \\ -1 & & & \end{array}\right]} \qquad \text{GF}(q) \qquad (3)$$

where

$$(W)_{ij} = \begin{cases} 0, & \text{if } j = i \\ 1, & \text{if } j - i = \square \\ -1, & \text{if } j - i \neq \square \end{cases}$$

The complementary code $C(q)^*$ is the row space of $H'$ where

$$H' = \begin{array}{c} \\ \infty \\ i \end{array} \overset{\begin{array}{cc} \infty & \quad i \end{array}}{\left[\begin{array}{c|ccc} -\theta & 1 & \cdots & 1 \\ \hline -1 & & & \\ \vdots & & W - \theta I & \\ -1 & & & \end{array}\right]} \qquad \text{GF}(q) \qquad (4)$$

THEOREM 1.1. Suppose $q \equiv -1 \pmod 4$.

Given $a, b \in V_q(F)$, then $(a,b) \in S(q)$ if and only if

$$a + b \in C(q) \quad \text{and} \quad a - b \in C(q)^*.$$

PROOF. We have $M(q)(1+\phi) = [H,H]$ and $M(q)(1-\phi) = [-H',H']$. Now

$$S(q) = S(q)(1+\phi) + S(q)(1-\phi)$$

and from (3) and (4) we have

$$S(q)(1+\phi) = \{(f,f) : f \in C(q)\}$$

and

$$S(q)(1-\phi) = \{(-g,g): g \in C(q)^*\}.$$

If $(a,b) \in S(q)$ then $(a,b) = (f+g, f-g)$ for some $f \in C(q)$ and $g \in C(q)^*$. Thus

$$a + b = 2f \in C(q) \quad \text{and} \quad (a-b) = 2g \in C(q)^*.$$

The argument is easily reversed and we omit the details.

Let $\mathcal{G}$ be the group generated by $\phi$ and by the monomial matrices given as (1) through (5) below. Every matrix is of the form $\begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}$ where $A$ and $B$ are square monomial matrices of size $(q+1)$. The rows and columns of both $A$ and $B$ are indexed by the elements of the projective line $GF(q) \cup \{\infty\}$.

(1) $T_i$, $i \in GF(q)$; the matrix corresponding to the permutation $(z \to z+i)$ applied simultaneously to the $\ell$ and $r$ coordinates in (1).

(2) $P_i$, $i = \square$; the matrix corresponding to the permutation $(z \to iz)$ applied simultaneously to the $\ell$ and $r$ coordinates in (1).

(3) $\rho$; the matrix corresponding to the permutation $(z \to z^p)$ (where $q = p^n$ and $p$ is prime) applied simultaneously to the $\ell$ and $r$

in (1).

$$(4)\quad \tau = \begin{bmatrix} A & 0 \\ 0 & A \end{bmatrix} \quad \text{where}$$

$$(A)_{ij} = \begin{cases} \varepsilon, & \text{if } j = 0 \text{ and } i = \infty \\ 1, & \text{if } j = \infty \text{ and } i = 0 \\ 1, & \text{if } j = -1/i \text{ and } i = \square \\ -1, & \text{if } j = -1/i \text{ and } i \neq \square \\ 0, & \text{otherwise} \end{cases}$$

$$(5)\quad Q_k = \begin{bmatrix} -D_k & 0 \\ 0 & D_k \end{bmatrix}, \quad k \neq \square, \quad \text{where}$$

$$(D_k)_{ij} = \begin{cases} -1, & \text{if } i = j = \infty \\ 1, & \text{if } i \neq \infty \text{ and } j = ki \\ 0, & \text{otherwise} \end{cases}$$

Let $n$ be fixed non-square, let $\lambda = \begin{bmatrix} D_n & 0 \\ 0 & D_n \end{bmatrix}$ and set $S(q)^* = S(q)\lambda$. When $q \equiv -1 \pmod 4$ we choose $n = (-1)$.

THEOREM 1.2.

(1) $\lambda^{-1} \mathcal{G} \lambda \subseteq \langle -I_{2q+2}, \mathcal{G} \rangle$.

(2) The codes $S(q)$ and $S(q)^*$ are both invariant under $\mathcal{G}$.

(3) The codes $S(q)$ and $S(q)^*$ have the properties described in Figure 1 below.

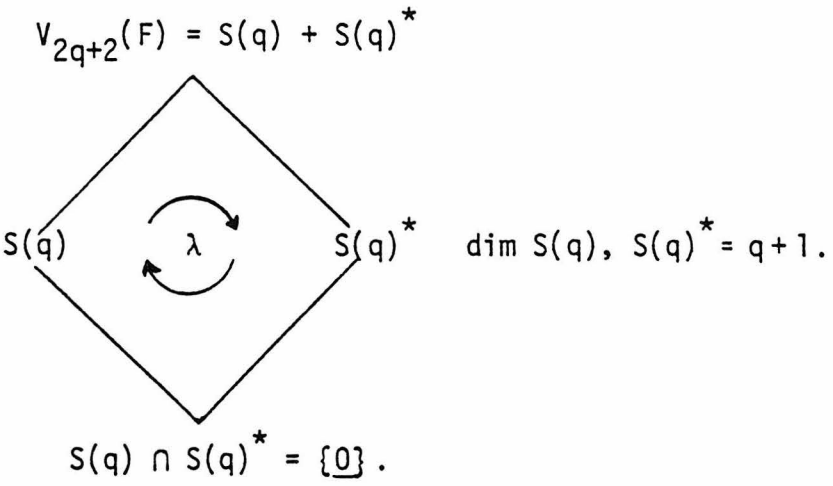



Figure 1.

The proof is very similar to the proof of theorem 1.1 of chapter 2 and we omit the details.

## 2. A SQUARE ROOT BOUND ON THE MINIMUM WEIGHT

Let

$$v = (a_\infty,\ldots,a_i,\ldots;b_\infty,\ldots,b_i,\ldots)$$

be a vector in $S(q)$. Let

$$d_1(v) = |\{i \in GF(q) : a_i \neq 0\}|$$

and

$$d_2(v) = |\{i \in GF(q) : b_i \neq 0\}|.$$

Since $S(q)$ is self-orthogonal and since $(\theta,0,\ldots,0;0,1,\ldots,1)$ and $(0,-\varepsilon,\ldots,-\varepsilon;\theta,0,\ldots,0)$ are vectors in $S(q)$ we have

$$\theta a_\infty = -\sum_{i \in GF(q)} b_i \quad \text{and} \quad \theta b_\infty = \varepsilon \sum_{i \in GF(q)} a_i \tag{5}$$

Let $d$ be the minimum weight in $S(q)$. Define

$$\Omega^* = \{v = (a,b) \in S(q) : a_\infty \neq 0,\ b_\infty \neq 0 \text{ and } \omega t(v) = d\}$$

and

$$\Omega = \{v = (a,b) \in S(q) : a_\infty \neq 0,\ b_\infty = 0 \text{ and } \omega t(v) = d\}.$$

LEMMA 2.1. If the set $\Omega^*$ is empty then

(1) The set $\Omega$ is non-empty.

(2) If $x \in \Omega$ and $d_1(x) > d_2(x)$ then there exists $v \in \Omega$ with $d_2(v) = d_1(x) + 1$ and $d_1(v) = d_2(x) - 1$

and (3) If $v \in \Omega$ and $d_2(v) > d_1(v)$ then there exists $x \in \Omega$ with $d_1(x) = d_2(v) - 1$ and $d_2(x) = d_1(v) + 1$.

PROOF. (1) Let $v = (a;b)$ be a codeword of minimum weight. Analysis of (1) shows $a = \underline{0}$ is impossible and $b = \underline{0}$ is impossible. If $a_i \neq 0$ and $b_i \neq 0$ for some $i \in GF(q) \cup \{\infty\}$ then there exists an automorphism $M$ such that $vM \in \Omega^*$. This contradicts $\Omega^* = \phi$ and by applying a suitable automorphism we may choose $v = (a;b)$ so that $a_\infty \neq 0$ and $b_\infty = 0$.

(2) Let $x = (c;d) \in \Omega$ with $d_1(x) > d_2(x)$. The argument of part (1) reveals that there exists $j \in GF(q)$ with $d_j \neq 0$ and $c_j = 0$. Let $M$ be an automorphism that interchanges the indices $j$ and $\infty$, and let $v = xM\phi$. Then $d_2(v) = d_1(x) + 1$ and $d_1(v) = d_2(x) - 1$ as required.

(3) is proved in the same way as (2) and we omit the details.

When $\Omega^*$ is non-empty define

$$s = \max_{v \in \Omega^*} \{|d_1(v) - d_2(v)|\}$$

and when $\Omega^*$ is empty define

$$t = \max_{v \in \Omega} \{d_2(v) - d_1(v)\}.$$

Let $R$ and $R^*$ be the subspaces of $V_{2q}(F)$ obtained from $S(q)$ and $S(q)^*$ respectively by taking each codeword and deleting the two entries indexed by $\infty$. Let $\lambda_1$ be the matrix obtained from $\lambda$ by deleting the two rows and columns indexed by $\infty$. From Figure 1 we see that the subspaces $R$ and $R^*$ have the properties described in Figure 2.

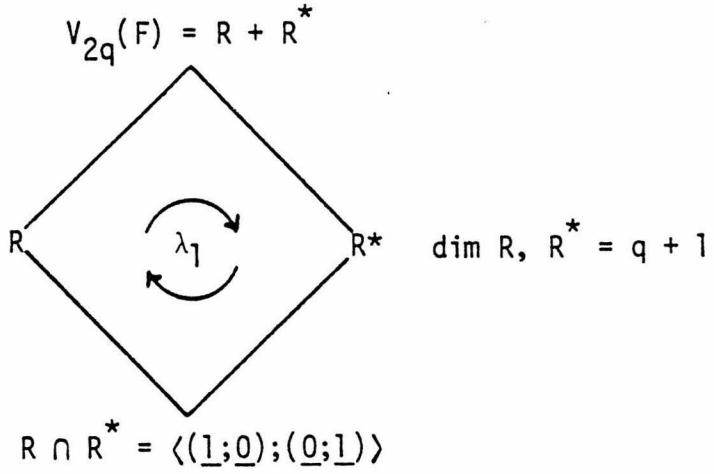



Figure 2.

Let $A$ be the matrix algebra over $F$ spanned by $\phi$ and by $T_i$, i e GF(q). Since $\phi T_i = T_i \phi$ the matrices $T_i$, $\phi T_i$ i e GF(q) are a basis for $A$. The linear map $\xi : V_{2q}(F) \to A$ given by

$$\xi : (\ldots,a_i,\ldots;\ldots,b_i,\ldots) \to \sum_{i \in GF(q)} a_i T_i + \phi \sum_{i \in GF(q)} b_i T_i$$

is bijective. The matrices $T_i$ and $\phi$ act as automorphisms of $R$ and $R^*$. These matrices also act on $A$ by right multiplication. Since

$$\{(\Sigma a_i T_i) + \phi(\Sigma b_i T_i)\}\,\phi = (-\varepsilon)\,\Sigma b_i T_i + \phi\,\Sigma a_i T_i$$

and

$$\{(\Sigma a_i T_i) + \phi(\Sigma b_i T_i)\}\,T_j = \Sigma a_i T_{i+j} + \phi\,\Sigma b_i T_{i+j}$$

the map $\xi$ is an A-module homomorphism. This allows us to regard

$R$ and $R^*$ as ideals in $A$. Since the matrices $T_i$ are linearly independent in $A$ the map

$$(\sum a_i T_i) \to (\sum a_i)$$

is a well defined map from the subalgebra of $A$ spanned by the matrices $T_i$ to $F$. This substitution map is a ring homomorphism.

THEOREM 2.2. If $\Omega^*$ is non-empty then the minimum weight $d$ satisfies

$$(d-2)^2 - s^2 \geq 2q \tag{6}$$

PROOF. Let

$$v = (a_\infty,\ldots,a_i,\ldots;b_\infty,\ldots,b_i,\ldots) \in \Omega^*$$

with $d_1(v) = \left(\frac{(d-2)-s}{2}\right)$ and $d_2(v) = \left(\frac{(d-2)+s}{2}\right)$. Then

$$v_1 = \sum a_i T_i + \phi \sum b_i T_i \in R$$

and

$$v_1\lambda_1 = \sum a_i T_{ni} + \phi \sum b_i T_{ni} \in R^*.$$

Since $A$ is a commutative algebra $RR^* \subseteq R \cap R^*$ and we have

$$\begin{aligned} v_1(v_1\lambda_1) &= (\sum a_i T_i)(\sum a_i T_{ni}) - \varepsilon(\sum b_i T_i)(\sum b_i T_{ni}) \\ &\quad + \phi\{(\sum a_i T_i)(\sum b_i T_{ni}) + (\sum b_i T_i)(\sum a_i T_{ni})\} \\ &= k_1(\sum T_i) + k_2\phi(\sum T_i) \end{aligned} \tag{7}$$

where $k_1, k_2 \in F$. The substitution map gives

$$k_2 = 2(\sum a_i)(\sum b_i)$$

and from (5) we have $k_2 \neq 0$. Counting non-zero coefficients in (7) gives

$$2\left(\frac{(d-2)-s}{2}\right)\left(\frac{(d-2)+s}{2}\right) \geq q$$

This reduces to (6) and the theorem is proved.

THEOREM 2.3. If $\Omega^*$ is empty then the minimum weight $d$ satisfies

$$(d-1)^2_{/2} - t^2_{/2} + t \geq q \tag{8}$$

PROOF. Let

$$v = (a_\infty,\ldots,a_i,\ldots;b_\infty,\ldots,b_i,\ldots) \in \Omega$$

with $d_1(v) = \left(\frac{(d-1)-t}{2}\right)$ and $d_2(v) = \left(\frac{(d-1)+t}{2}\right)$. By part (3) of lemma 2.1 there exists

$$x = (c_\infty,\ldots,c_i,\ldots;d_\infty\ldots,d_i,\ldots) \in \Omega$$

with $d_1(x) = \left(\frac{(d-1)+(t-2)}{2}\right)$ and $d_2(x) = \left(\frac{(d-1)-(t-2)}{2}\right)$. Then

$$v_1 = (\sum a_i T_i) + \phi(\sum b_i T_i) \in R$$

and

$$w_1 = (\sum c_i T_{ni}) + \phi(\sum d_i T_{ni}) \in R^*.$$

It follows that $v_1 w_1 = k(\sum T_i)$, where $k \neq 0$. The usual counting argument gives

$$\left(\frac{(d-1)-t}{2}\right)\left(\frac{(d-1)+(t-2)}{2}\right) + \left(\frac{(d-1)+t}{2}\right)\left(\frac{(d-1)-(t-2)}{2}\right) \geq q.$$

This reduces to (8) and the theorem is proved.

THEOREM 2.4. If $\Omega^*$ is empty and if $q \equiv -1 \pmod 4$ then the minimum weight $d$ satisfies

$$(d-1)^2_{/2} + (t-2)^2_{/2} - (d-1) + 1 \geq q \tag{9}$$

PROOF. By part (3) of lemma 2.1 there exists

$$x = (c_\infty,\ldots,c_i,\ldots;d_\infty,\ldots,d_i,\ldots) \in \Omega$$

with $d_1(x) = \left(\frac{(d-1)+(t-2)}{2}\right)$ and $d_2(x) = \left(\frac{(d-1)-(t-2)}{2}\right)$.

Then

$$x_1 = (\sum c_i T_i) + \phi(\sum d_i T_i) \in R$$

and

$$x_1\lambda_1 = (\sum c_i T_{-i}) + \phi(\sum d_i T_{-i}) \in R^*.$$

It follows that $x_1(x_1\lambda_1) = k(\sum T_i)$ where $k \neq 0$. The usual counting argument gives

$$d_1(x)^2 + d_2(x)^2 - (d_1(x) + d_2(x)) + 1 \geq q$$

and this reduces to (9).

THEOREM 2.5. The minimum weight $d$ satisfies

$$(d-1)^2 \geq 2q - 1 \tag{10}$$

If $q \equiv -1 \pmod 4$ then $d$ satisfies

$$(d-1)^2 - (d-1) + 1 \geq 2q + 1 \tag{11}$$

and equality holds only if $d = 4$ and $q = 3$.

PROOF. If $\Omega^*$ is non-empty then by theorem 2.2 we have $(d-2)^2 \geq 2q$ and both (10) and (11) hold.

If $\Omega^*$ is empty then by theorem 2.3 we have $(d-1)^2 \geq 2q-1$. If $\Omega^*$ is empty and if $q \equiv -1 \pmod 4$ then (8) and (9) hold. The argument used to prove theorem 2.6 of chapter 3 shows that $(d-1)^2 - (d-1) + 1 \geq 2q + 1$ and the equality holds only if $d = 4$ and $q = 3$.

REMARKS. The symmetry code $S(3)$ over $GF(7)$ is the row space of the matrix

$$M(3) = \begin{array}{c|cccc|cccc} & \ell_\infty & \ell_0 & \ell_1 & \ell_{(-1)} & r_\infty & r_0 & r_1 & r_{(-1)} \\ \hline \infty & 2 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 2 & 0 & 0 & -1 & 0 & 1 & -1 \\ 1 & 0 & 0 & 2 & 0 & -1 & -1 & 0 & 1 \\ (-1) & 0 & 0 & 0 & 2 & -1 & 1 & -1 & 0 \end{array}$$

From (11) we see that $S(3)$ is an $[8,4,4]$ code over $GF(7)$. Since $(d-2)^2 < 2q-1$, it follows from theorem 2.2 that $\Omega^*$ is empty.

Figure 3 below is taken from page 511 of [10] and is a list of parameters of the first five ternary symmetry codes. Here $n$ is the block length, $k$ is the dimension and $d$ is the minimum distance.

| | n | k | d |
|---|---|---|---|
| S(5) | 12 | 6 | 6 |
| S(11) | 24 | 12 | 9 |
| S(17) | 36 | 18 | 12 |
| S(23) | 48 | 24 | 15 |
| S(29) | 60 | 30 | 18 |

Figure 3.

Theorem 2.5 only allows us to find the exact minimum weight directly in the first two cases. If $q = 11$ then $3|d$ and $(d-1)^2 - (d-1) + 1 > 22$. We conclude that $d \geq 9$. But by a theorem of C. L. Mallows and N.J.A. Sloane [11],

$$d \leq 3\left[\frac{n}{12}\right] + 3$$

i.e. $d \leq 12$. Hence the ternary code $S(11)$ is a $[24,12,9]$ code.

## CHAPTER 5. MULTIPLYING VECTORS IN QUADRATIC RESIDUE CODES.

Let $q \equiv -1 \pmod 8$ be an odd prime power and let $C(q)$ and $C(q)^*$ be the two extended binary quadratic residue codes of length $(q+1)$. In this chapter we show how to regard $C(q)$ and $C(q)^*$ as one-sided ideals in a binary group algebra and we show that the appropriate product is a 2-dimensional ideal. This allows us to prove that if $d$ is the minimum weight in $C(q)$ then

$$(d-1)^2 - (d-1) + 1 - st \geq q$$

where $s$, $t$ are non-negative integers with $s \equiv 0 \pmod 4$, and $t$ odd. The integers $s$ and $t$ depend on the way the non-zero entries of a codeword of minimum weight are distributed among the coordinate positions. When $s = 0$ we establish a correspondence between codewords of minimum weight $d$ in $C(q)$ and $d \times d$ Hadamard submatrices of the $(q+1) \times (q+1)$ Paley-Hadamard matrix.

In chapter 2 we defined the extended binary quadratic residue code $C(q)$ to be the subspace of $V_{q+1}(2)$ spanned by the rows of the matrix $M(q)$ given below. The rows and columns of $M(q)$ are indexed by the elements of the projective line $GF(q) \cup \{\infty\}$.

$M(q) =$

| | | $\infty$ | GF(q) $i$ |
|---|---|---|---|
| $\infty$ | | 1 | 1 . . . . . 1 |
| GF(q) | $i$ | 1 ⋮ 1 | $S$ |

(1)

where

$$(S)_{ij} = \begin{cases} 1, & \text{if } j - i = \square \\ 0, & \text{otherwise} \end{cases} \tag{2}$$

EXAMPLE. The code $C(7)$ is the row space of the matrix

$$M(7) = \begin{array}{c|cccccccc} & \infty & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline \infty & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 3 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 4 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 5 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 6 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \end{array} \tag{3}$$

This is the [8,4,4] Hamming code. Notice that the incidence matrix of the projective plane $PG(2,2)$ is a principal submatrix of $M(7)$.

If $q$ is prime then $C(q)$ is a classical quadratic residue code. The matrix $S$ is a circulant and $C(q)$ is an extended cyclic code.

We replace 0 by (-1) throughout $M(q)$ to obtain a (1,-1) matrix $P(q)$. If we regard $P(q)$ as an integral matrix then $P(q)$ is the Hadamard matrix constructed by R.E.A.C. Paley in [12]. Since $q \equiv -1 \pmod 8$ we may write $q + 1 = 4t + 4$ where $t$ is odd. We have

$$SS^T = ((2t+1) - t)\, I + tJ \tag{4}$$

$$\equiv J \pmod 2.$$

It follows that $C(q)$ is self-orthogonal. Note that every row of the matrix $M(q)$ has weight divisible by 4. Since $C(q)$ is self-orthogonal it follows by induction that any sum of rows of $M(q)$ has weight divisible by 4. Thus all weights in $C(q)$ are divisible by 4.

Recall that the group $P\Gamma L(2,q)$ is represented by all permutations of $GF(q) \cup \{\infty\}$ that have the form $\left(z \to \frac{az^{\sigma}+b}{cz^{\sigma}+d}\right)$, with $a, b, c, d, \in GF(q)$, $ad - bc$ a non-zero square, and $\sigma$ an automorphism of $GF(q)$. This group is generated by the permutations given as (1), (2), (3) and (4) below.

(1) $T_i = (z \to z + i)$, for $i \in GF(q)$,

(2) $P_i = (z \to iz)$, for $i = \square$,

(3) $\rho = (z \to z^p)$ (where $p$ is prime and $q = p^n$), the permutation corresponding to the Frobenius automorphism of $GF(q)$,

and (4) $\tau = (z \to -1/z)$.

We adopt the standard conventions about operations involving $\infty$.

LEMMA 1.1. If $m_i$ is the row of $M(q)$ indexed by $i$ then

(1) $m_i T_j = m_{i+j}$, for $j \in GF(q)$,

(2) $m_i P_j = m_{ij}$, for $j = \square$,

(3) $m_i \rho = m_i p$,

$$(4) \qquad m_i\tau = \begin{cases} m_\infty, & \text{if } i = \infty \\ m_0 + m_\infty, & \text{if } i = 0 \\ m_{-1/i} + m_0, & \text{if } i = \square \\ m_{-1/i} + m_0 + m_\infty, & \text{if } i \neq \square. \end{cases}$$

The calculations are not difficult and we omit the details. They also follow from the definitions on page 16 and from calculation (3) in the proof of theorem 1.1 of chapter 2. It follows that the code $C(q)$ is invariant under $P\Gamma L(2,q)$. Let $\lambda$ be the permutation $(z \to -z)$ and let $C(q)^* = C(q)\lambda$. The code $C(q)^*$ is spanned by the vectors $m_i^* = m_{(-i)}\lambda$ for $i \in GF(q) \cup \{\infty\}$. We have

$$m_\infty^* = m_\infty = \underline{1} \qquad (5)$$

and if $i \neq \infty$

$$(m_i^*)_j = \begin{cases} 1, & \text{if } j = \infty \\ 1, & \text{if } j - i \neq \square \\ 0, & \text{otherwise} \end{cases} \qquad (6)$$

Since $\lambda$ normalizes $P\Gamma L(2,q)$ the code $C(q)^*$ is also invariant under $P\Gamma L(2,q)$. In chapter 2 we proved that the codes $C(q)$ and $C(q)^*$ have the properties described in Figure 1.

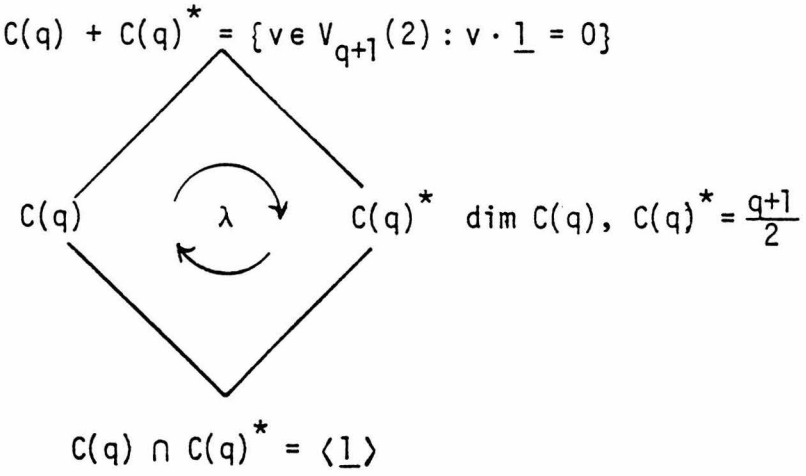



Figure 1.

Let $Q$ and $Q^*$ be the subspaces of $V_q(2)$ obtained from $C(q)$ and $C(q)^*$ respectively by taking each codeword and deleting the entry indexed by $\infty$. We have $Q^* = Q\lambda$ and $Q^* \cap Q = \langle \underline{1} \rangle$.

We specialize theorem 2.1 of chapter 2 to give

THEOREM 1.2. If $d$ is the minimum weight in $C(q)$ then

$$(d-1)^2 - (d-1) + 1 \geq q.$$

We also recall theorem 2.3 of chapter 2.

THEOREM 1.3. Suppose the minimum weight $d$ in $C(q)$ satisfied

$$(d-1)^2 - (d-1) + 1 = q.$$

Then the vectors of minimum weight in $Q$ are the lines of a projective plane of order $(d-2)$.

We are now ready to prove our generalization of theorem 1.2.

## 2. A STRONGER FORM OF THE SQUARE ROOT BOUND

We may write $v \in V_{q+1}(2)$ in the form

$$v = (a_\infty, \ldots, a_i, \ldots; b_0, \ldots, b_i, \ldots)$$

$$\infty \qquad i \qquad\qquad (-i)$$

non-zero squares  non-squares.

Define

$$d_1(v) = |\{i : a_i \neq 0 \text{ and } i \neq \infty\}|$$

and

$$d_2(v) = |\{i : b_i \neq 0 \text{ and } i \neq 0\}|$$

Since $C(q)$ is self-orthogonal and since $(\underline{1};\underline{0})$ and $(\underline{0};\underline{1})$ are vectors in $C(q)$ we have

$$a_\infty = \sum_{i=\square} a_i \quad \text{and} \quad b_0 = \sum_{i=\square} b_i \tag{7}$$

Let $R$ and $R^*$ be the subspaces of $V_{q-1}(2)$ obtained from $C(q)$ and $C(q)^*$ respectively by taking each codeword and deleting the entries indexed by $\infty$ and $0$. From Figure 1 we see that the subspaces $R$ and $R^*$ have the properties described in Figure 2.

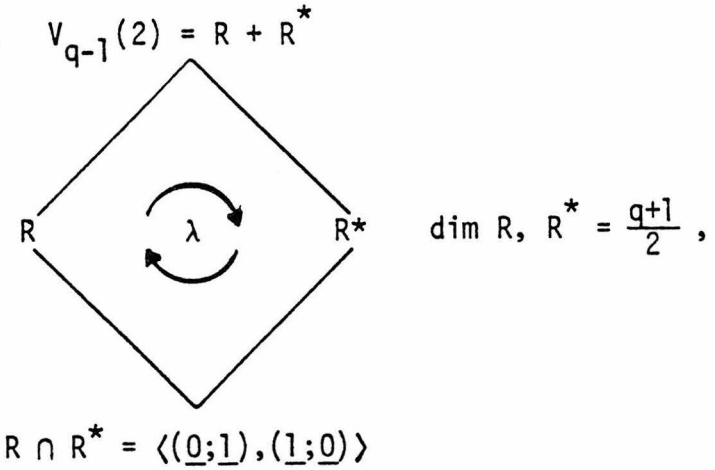



Figure 2.

In section 1 we defined vectors $m_k$ and $m_k^*$ for $k \in GF(q) \cup \{\infty\}$. Let $x_k$ and $x_k^*$ be the vectors obtained from $m_k$ and $m_k^*$ by deleting the entries indexed by $\infty$ and 0. Then we have $R = \langle x_k : k \in GF(q) \cup \{\infty\} \rangle$ and $R^* = \langle x_k^* : k \in GF(q) \cup \{\infty\} \rangle$.

Since $\tau^2 = 1$, and since $\tau P_i \tau = P_{i-1}$ the group $D = \{P_i, P_i\tau : i = \square\}$ is dihedral of order $(q-1)$. Let $B$ be the binary group algebra with basis the elements of $D$. Let $\xi : R \to B$ be the linear map given by

$$\xi : (\ldots,a_i,\ldots;\ldots b_i,\ldots) \to \sum a_i P_i + \sum b_i \tau P_i$$

and let $\xi^* : R^* \to B$ be the linear map given by

$$\xi^* : (\ldots,c_i,\ldots;\ldots,d_i,\ldots) \to \sum c_i P_i + \sum d_i P_i \tau.$$

Since the elements of $D$ are linearly independent, $\xi$ and $\xi^*$ are injective. We have $\tau P_i = P_{i-1}\tau$ and $\tau(\sum P_i) = (\sum P_i)\,\tau$, and so $\xi$ and $\xi^*$ agree on $R \cap R^*$. Every element of $D$ acts as an automorphism of both $R$ and $R^*$. The group $D$ also acts on the algebra $B$ by left and right multiplication. The next lemma connects the different group actions.

LEMMA 2.1. (1) If $v^* \in R^*$ and $d \in D$ then $\xi^*(v^*d) = d\xi^*(v)$.

(2) If $v \in R$ and $d \in D$ then $\xi(vd) = \xi(v)\,d$.

(3) The subspace $\xi(R)$ is a right ideal of $B$ and the subspace $\xi^*(R^*)$ is a left ideal of $B$.

PROOF. (1) If $v^* = (\ldots,c_i,\ldots;\ldots,d_i,\ldots) \in R^*$ then

$$\begin{aligned} P_j\xi^*(v^*) &= P_j(\sum c_i P_i + \sum d_i P_i \tau) \\ &= \sum c_i P_{ij} + \sum d_i P_{ij}\tau \\ &= \xi^*(v^* P_j) \end{aligned}$$

and $$\tau\xi^*(v^*) = \tau(\sum c_i P_i + \sum d_i P_i \tau)$$

$$= \sum d_i P_{i-1} + \sum c_i P_{i-1}\tau$$

$$= \xi^*(v^*\tau).$$

Part (2) is similar to (1) and we omit the details. Part (3) follows from parts (1) and (2).

Henceforth we shall identify $R$ with $\xi(R)$ and $R^*$ with $\xi^*(R^*)$. This allows us to multiply vectors in $R^*$ by vectors in $R$.

If $x_1 = (\ldots,f_i,\ldots;\ldots,g_i,\ldots)$ then

$$f_i = \begin{cases} 1, & \text{if } i - 1 = \square \text{ (or if } -i-(-1) \neq \square) \\ 0, & \text{otherwise} \end{cases}$$

and

$$g_i = \begin{cases} 1, & \text{if } -i - 1 = \square \text{ (or if } i-(-1) \neq \square) \\ 0, & \text{otherwise} \end{cases}$$

From (6) we have $x^*_{(-1)} = (\ldots,g_i,\ldots;\ldots,f_i,\ldots)$. Identifying $R$ with $\xi(R)$ and $R^*$ with $\xi^*(R^*)$ gives

$$x_1 = \sum f_i P_i + \sum g_i \tau P_i$$

and

$$x^*_{(-1)} = \sum g_i P_i + \sum f_i P_i \tau$$

The results in this section rest on the following calculation.

LEMMA 2.2. If $x_1$, $x^*_{(-1)}$ are as above then

$$(x^*_{(-1)})(x_1) = \tau(\sum P_i)$$

PROOF. Since $B$ is a binary algebra we have

$$(x_{(-1)}^{*})(x_1) = (\sum g_i P_i + \sum f_i P_i \tau)(\sum f_i P_i + \sum g_i \tau P_i)$$

$$= \tau\{(\sum g_i P_{i-1})(\sum g_i P_i) + (\sum f_i P_{i-1})(\sum f_i P_i)\}$$

$$= \tau(\sum c_k P_k) .$$

Now we prove that every coefficient $c_k \equiv 1 \pmod 2$.

$$c_k = |\{(i,j) : g_i \neq 0,\ g_j \neq 0 \text{ and } j = ik\}|$$

$$+ |\{(i,j) : f_i \neq 0,\ f_j \neq 0 \text{ and } j = ik\}| .$$

Thus $c_k = (x_1)(x_1 P_k)^T$, the inner product of the vectors $x_1$ and $x_1 P_k$ in $V_{q-1}(2)$. Since $x_k = x_1 P_k$ we have $c_k = (x_1)(x_k)^T$. If $S$ is the matrix defined in (2) then $(S)_{10} = 0$ and (4) gives

$$c_k = \begin{cases} t, & \text{if } k \neq 1 \\ 2t + 1, & \text{if } k = 1 \end{cases}$$

where $q + 1 = 4t + 4$. Since $t$ is odd $c_k \equiv 1 \pmod 2$ as required.

LEMMA 2.3. $R^{*}R = \langle(\sum P_i),\ \tau(\sum P_i)\rangle$ .

PROOF. If $J = \langle(\sum P_i),\ \tau(\sum P_i)\rangle$ then $J$ is an ideal in $B$. From lemma 2.2 we have

$$(x_{(-1)}^{*})\, x_1 = \tau(\sum P_i) .$$

We multiply on the right by $P_k$ and apply lemma 2.1 to give

$$(x_{(-1)}^{*})\, x_k = \tau(\sum P_i) \tag{8}$$

for all $k = \square$. Multiplying (8) on the right by $\tau$ yields

$$(x_{(-1)}^{*})(x_{-1/k} + x_0) = (\sum P_i) .$$

Since $x_0 = (\sum P_i) \in J$ we have

$$(x_{(-1)}^{*})(x_{-1/k}) \in J \tag{9}$$

for all $k = \square$. Equations (8) and (9) force

$$(x_{(-1)}^{*})\, R \subseteq J. \tag{10}$$

Multiplying (10) on the left by $\tau$, and by $P_k$ for all $k = \square$, we obtain $R^{*}R \subseteq J$ and the proof is complete.

Since the permutations $P_i$ are linearly independent in $B$ the map

$$(\sum c_i P_i) \to (\sum c_i)$$

is well-defined. This substitution map is a ring homomorphism from the subalgebra of $B$ spanned by the permutations $P_i$ to $GF(2)$.

We define

$$\Omega^{*} = \{v = (a;b) \in C(q) : a_\infty = b_0 = 1 \text{ and } wt(v) = d\}$$

and $$\Omega = \{v = (a;b) \in C(q) : a_\infty = 1,\ b_0 = 0 \text{ and } wt(v) = d\}.$$

Then we define

$$s = \max_{v \in \Omega^{*}} \{|d_1(v) - d_2(v)|\}$$

and $$t = \max_{v \in \Omega} \{|d_1(v) - d_2(v)|\}.$$

THEOREM 2.4. The minimum weight $d$ satisfies

$$(d-1)^2 - (d-1) + 1 - st \geq q \tag{11}$$

PROOF. There exists

$$v = (1,\ldots,a_i,\ldots;0,\ldots,b_i,\ldots) \in \Omega$$

with $d_1(v) = \left(\frac{(d-1)\pm t}{2}\right)$ and $d_2(v) = \left(\frac{(d-1)\mp t}{2}\right)$. Since $\tau \in Aut(C(q))$

there exists

$$w = (1,\ldots,c_i,\ldots;1,\ldots,d_i,\ldots) \in \Omega^*$$

with $d_1(w) = \left(\frac{(d-2)-s}{2}\right)$ and $d_2(w) = \left(\frac{(d-2)+s}{2}\right)$. Now

$$v_1 = \sum a_i P_i + \sum b_i \tau P_i \in R$$

and

$$w_1 = \sum d_i P_i + \sum c_i P_i \tau \in R^*.$$

Thus $w_1 v_1 \in R^* R$ and from lemma 2.3 we have

$$\begin{aligned} w_1 v_1 &= (\sum d_i P_i)(\sum a_i P_i) + (\sum c_i P_i)(\sum b_i P_i) \\ &\quad + \tau\{(\sum c_i P_{i-1})(\sum a_i P_i) + (\sum d_i P_{i-1})(\sum b_i P_i)\} \\ &= k_1(\sum P_i) + k_2\tau(\sum P_i) \end{aligned} \tag{12}$$

where $k_1, k_2 \in GF(2)$. The substitution map gives

$$k_1 = (\sum d_i)(\sum a_i) + (\sum c_i)(\sum b_i)$$

and

$$k_2 = (\sum c_i)(\sum a_i) + (\sum d_i)(\sum b_i)$$

and from (7) we have $k_1 = 1$ and $k_2 = 1$. Counting non-zero coefficients in (12) using $k_1 = 1$ or $k_2 = 1$ depending on the sign of $\pm t$ gives

$$\left(\frac{(d-2)-s}{2}\right)\left(\frac{(d-1)+t}{2}\right) + \left(\frac{(d-2)+s}{2}\right)\left(\frac{(d-1)-t}{2}\right) \geq \frac{(q-1)}{2}.$$

This reduces to (11) and the theorem is proved.

REMARKS. If $v \in \Omega$ then (7) implies that $d_1(v)$ is odd and $d_2(v)$ is even. Thus $t$ is odd and so it not 0. If $v \in \Omega^*$ then $d_1(v)$ and $d_2(v)$ are both odd and $d_1(v) + d_2(v) = d - 2$. Since $d \equiv 0 \pmod 4$ we have $d_1(v) \equiv d_2(v) \pmod 4$ and so $s$ is a multiple of 4.

When $q = 7$ we have $d = 4$ and $(d-1)^2 - (d-1) + 1 = q$. The set $\Omega^*$ consists of the three vectors given below

$$\infty\ 1\ 2\ 4\ ;\ 0\ (-1)(-2)(-4)$$
$$(1\ 1\ 0\ 0\ ;\ 1\ 0\ 0\ 1)$$
$$(1\ 0\ 1\ 0\ ;\ 1\ 1\ 0\ 0)$$
$$(1\ 0\ 0\ 1\ ;\ 1\ 0\ 1\ 0)$$

Notice that $s = 0$.

The code $C(23)$ is the [24,12,8] Golay code. If

$$\infty 1\ 2\ 3\ 4\ 6\ 8\ 9\ 12\ 13\ 16\ 18;\ 0(-1)(-2)(-4)(-6)(-8)(-9)(-12)(-13)(-16)(-18)$$
$$v = (1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ ;\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0)$$
and
$$w = (1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ ;\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 1)$$

then it is straightforward to check that $v \in \Omega$ and $w \in \Omega^*$ using (41) on page 498 of [10]. We have

$$v_1 = P_4 + \tau(P_1 + P_2 + P_3 + P_9 + P_{12} + P_{13}) \in R$$

and

$$w_1 = (P_4 + P_6 + P_8 + P_{16} + P_{18}) + P_4\tau \in R^*.$$

It is easily checked that $w_1 v_1 = (\sum P_i) + \tau(\sum P_i)$ and in particular we have

$$(\sum P_i) = P_4(P_4 + P_6 + P_8 + P_{16} + P_{18}) + P_4(P_1 + P_2 + P_3 + P_9 + P_{12} + P_{13}).$$

Notice that $s = 4$, $t = 5$ and $(d-1)^2 - (d-1) + 1 - st = q$.

We now define

$$r = \min_{v \in \Omega}\{|d_1(v) - d_2(v)|\}.$$

THEOREM 2.5. The minimum weight $d$ satisfies

$$(d-1)^2 - (d-1) + 1 - ((d-3) - r^2) \geq q \qquad (13)$$

PROOF. Let

$$v = (1,\ldots,a_i,\ldots;0,\ldots,b_i,\ldots) \in \Omega$$

with $d_1(v) = \left(\frac{(d-1)\pm r}{2}\right)$ and $d_2(v) = \left(\frac{(d-1)\mp r}{2}\right)$. Then

$$v_1 = \sum a_i P_i + \sum b_i \tau P_i \in R$$

and

$$v_1\lambda = \sum b_i P_i + \sum a_i P_i \tau \in R^*.$$

Since $B$ is a binary algebra and since $(v_1\lambda)\, v_1 \in R^*R$ we have

$$\begin{aligned}(v_1\lambda)\, v_1 &= \tau\{(\sum b_i P_{i-1})(\sum b_i P_i) + (\sum a_i P_{i-1})(\sum a_i P_i)\} \\ &= k\tau(\sum P_i) \qquad (14)\end{aligned}$$

where $k \in GF(2)$. The substitution map gives $k = 1$. Counting different non-zero terms in (14) gives

$$d_1(v)^2 + d_2(v)^2 - (d_1(v) + d_2(v)) + 1 \geq \left(\frac{q-1}{2}\right),$$

and so

$$\left(\frac{(d-1)-r}{2}\right)^2 + \left(\frac{(d-1)+r}{2}\right)^2 - (d-1) + 2 \geq \frac{q+1}{2}.$$

This reduces to (13) and the proof is complete.

THEOREM 2.6. If the minimum weight $d$ satisfies

$$(d-1)^2 - (d-1) + 1 = q$$

then $d = 4$ and $q = 7$.

PROOF. By theorem 2.4 we have $(d-1)^2 - (d-1) + 1 - st \geq q$, where $s, t \geq 0$ and $t$ is odd. This forces $s = 0$. By theorem 1.3 the vectors of minimum weight in the code $Q$ are the lines of a projective plane $PG(2,d-2)$. If $L_1, \ldots, L_{d-1}$ are the lines through $0$ then $L_i \cap L_j = \{0\}$ if $i \neq j$.

Since $s = 0$, every line $L_i$ contains $(\frac{d-2}{2})$ non-zero squares and $(\frac{d-2}{2})$ non-squares. Note that $(d-1)(\frac{d-2}{2}) = (\frac{q-1}{2})$ and that each non-zero square is on a unique line $L_i$. It follows that $P = \langle P_i : i = \square \rangle$ acts transitively on $L_1, \ldots, L_{d-1}$, and that the stabilizer of a line is the subgroup generated by $P_\gamma$, where $\gamma$ is a primitive $(\frac{d-2}{2})$ root of unity in $GF(q)$. Hence there exist non-zero squares $y_i, z_i \in GF(q)$, $i = 1, \ldots, d-1$, with $y_1 = 1$ such that

$$L_i = \{0, y_i\gamma^j, (-z_i)\gamma^j : j = 1, \ldots, \tfrac{d-2}{2}\}$$

for $i = 1, \ldots, (d-1)$. Since the vector $L_1T_{(-1)}$ contains 0 we have $L_1T_{(-1)} = L_m$ for some line $L_m$. If $d \geq 8$ then $(\frac{d-2}{2}) \geq 3$ and there exist $(\gamma^i - 1), (\gamma^j - 1) \in L_1T_{(-1)}$ such that $(\gamma^j - 1) = \gamma^k(\gamma^i - 1)$, for some $k \neq 0$. If $\alpha = \gamma^j - 1 = \gamma^{k+i} - \gamma^k$ then $L_1T_{(-1)}$ and $L_1T_{(-\gamma^k)}$ are distinct lines in $PG(2,d-2)$ and $0, \alpha \in L_1T_{(-1)} \cap L_1T_{(-\gamma^k)}$. This is impossible and we conclude that $d = 4$. If $d = 4$ then (4) implies $q = 7$ and the proof is complete.

As a corollary we have the following theorem on cyclic projective planes.

THEOREM 2.7. Let $\mathfrak{B}$ be a cyclic projective plane of order $(d-2)$ with $d - 2 \equiv 2 \pmod 8$ and with $q = (d-2)^2 + (d-2) + 1$ a prime.

If 2 is a primitive $(\frac{q-1}{2})$ root of unity in $GF(q)$ then $\mathfrak{B} = PG(2,2)$.

PROOF. We note that $q = (d-1)^2 - (d-1) + 1$ and that $q \equiv -1 \pmod 8$. We may suppose that the points of $\mathfrak{B}$ are labelled with the elements of $GF(q)$ and that $\mathfrak{B}$ is invariant under the cyclic permutation $(z \to z+1)$. If $L = \{e_1, \ldots, e_{d-1}\}$ is a line in $\mathfrak{B}$ then $L$ is a difference set in

GF(q). The rows of the incidence matrix of $\mathcal{B}$ span a cyclic code W. The linear map

$$(a_0,\ldots,a_{q-1}) \to a_0 + a_1x + \cdots + a_{q-1}x^{q-1}$$

allows us to regard W as an ideal in the polynomial ring $K = GF(2)[x]/\langle(x^q-1)\rangle$. Clearly we have $W = \langle(\sum_{i=1}^{d-1} x^{e_i})\rangle$ and

$$(\sum_{i=1}^{d-1} x^{e_i})(\sum_{i=1}^{d-1} x^{-e_i}) = 1 + x + \cdots + x^{q-1}$$

in K. Let $\alpha$ be a primitive qth root of unity in an extension field of GF(2) and let

$$g_0(x) = \prod_{i=\square} (x - \alpha^i) \quad \text{and} \quad g_1(x) = \prod_{i\neq\square} (x - \alpha^i).$$

Since 2 is primitive $\frac{q-1}{2}$ root of unity in GF(q) the polynomials $g_0(x)$ and $g_1(x)$ are irreducible in GF(2)[x]. Since GF(2)[x] is a unique factorization domain and since

$$g_0(x)\, g_1(x) = 1 + x + \cdots + x^{q-1}$$

we have $W = \langle g_0(x)\rangle$ or $W = \langle g_1(x)\rangle$. But it is well known that $Q = \langle g_0(x)\rangle$ and $Q^* = \langle g_1(x)\rangle$. Indeed this is the way the classical quadratic residue codes are usually defined. The result now follows easily from theorem 2.6.

This connection between cyclic projective planes and quadratic residue codes was pointed out by van Tilborg in [18].

## 3. THE CASE s = 0

In view of theorems 2.4 and 2.5 the possible values of the parameters s, t, and r are of interest. We have seen that s is divisible by 4 and that t, r are both odd. When s = 0, theorem 2.4

gives the same bound on the minimum weight as theorem 1.2. In this section we consider a consequence of the condition $s = 0$.

For every vector $v \in \Omega^*$ we define a $d \times d$ matrix $D(v)$ with all entries $\pm 1$. We use the elements of $v$ to index the rows and columns of $D(v)$.

$$D(v) = \begin{array}{c|c|c} & \infty & i \\ \hline \infty & 1 & 1 \ldots\ldots\ldots 1 \\ \hline i & \begin{array}{c}1\\ \vdots \\ 1\end{array} & H \end{array}$$

where

$$(H)_{ij} = \begin{cases} 1, & \text{if } j - i = \square \\ -1, & \text{otherwise} \end{cases}$$

Notice that $D(v)$ is a principal submatrix of the Paley-Hadamard matrix $P(q)$ that is defined in section 1.

THEOREM 3.1. If $s = 0$ then for every $v \in \Omega^*$ we have

$$D(v)\ D(v)^T = D(v)^T\ D(v) = dI$$

PROOF. Let $d_i$ be the row of $D(v)$ indexed by $i$. Since $s = 0$, every vector $x \in \Omega^*$ contains $(\frac{d-2}{2})$ non-zero squares and $(\frac{d-2}{2})$ non-squares. If $i \in v$ and $i \neq \infty$ then $vT_{-i} \in \Omega^*$. The row $d_i$ must have $d/2$ entries 1 and $d/2$ entries $(-1)$, and so $d_i d_\infty^T = 0$.

Let $x \in \Omega^*$, let $\beta \in x$ be a non-zero square and set

$$k_1 = |\{\alpha \in x : \alpha = \square \text{ and } \alpha - \beta = \square\}|,$$

$$k_2 = |\{\alpha \in x : \alpha = \square \text{ and } \alpha - \beta \neq \square\}|,$$

$$k_3 = |\{\alpha \in x : \alpha \neq \square \text{ and } \alpha - \beta = \square\}|,$$

and $$k_4 = |\{\alpha \in x : \alpha \neq \square \text{ and } \alpha - \beta \neq \square\}|.$$

Since $x \in \Omega^*$ we have

$$k_1 + k_2 = \left(\frac{d-2}{2}\right) - 1 \quad \text{and} \quad k_3 + k_4 = \left(\frac{d-2}{2}\right). \tag{16}$$

Since $xT_{-\beta} \in \Omega^*$ we have

$$k_1 + k_3 = \left(\frac{d-2}{2}\right) \quad \text{and} \quad k_2 + k_4 = \left(\frac{d-2}{2}\right) - 1 \tag{17}$$

Since $x\tau \in \Omega^*$ and since $-1/\beta \in x\tau$ we have $x\tau T_{1/\beta} \in \Omega^*$.

Hence

$$\left(\frac{d-2}{2}\right) - 1 = |\{\alpha \in x : \alpha \neq 0, \infty \text{ and } -1/\alpha + 1/\beta = \square\}|$$

$$= |\{\alpha \in x : \alpha \neq 0, \infty \text{ and } \frac{\alpha-\beta}{\alpha} = \square\}| \tag{18}$$

and $$\left(\frac{d-2}{2}\right) = |\{\alpha \in x : \alpha \neq 0, \infty \text{ and } -1/\alpha + 1/\beta \neq \square\}|$$

$$= |\{\alpha \in x : \alpha \neq 0, \infty \text{ and } \frac{\alpha-\beta}{\alpha} \neq \square\}|. \tag{19}$$

From (18) we have

$$k_1 + k_4 = \left(\frac{d-2}{2}\right) - 1 \tag{20}$$

and from (19) we have

$$k_2 + k_3 = \left(\frac{d-2}{2}\right). \tag{21}$$

Together (16), (17), (20) and (21) imply

$$k_1 = k_2 = k_4 = \left(\frac{d-4}{4}\right) \quad \text{and} \quad k_3 = \left(\frac{d-4}{4}\right) + 1. \tag{22}$$

Let $d_i$, $d_j (i,j \neq \infty)$, be two distinct rows of $D(v)$. Without loss we may suppose $i - j = \square$. We have

$$(vT_{-i})\, T_{(i-j)} = vT_{-j}.$$

If $\alpha \in vT_{-i}$ then $\alpha = k - i$ for some $k \in v$ and if $\alpha' \in vT_{-j}$ then $\alpha' = k' - j$ for some $k' \in v$. If we set $x = vT_{-i}$ and $\beta = j - i$ then (22) implies

$$\begin{aligned} d_i d_j^T &= 1 \cdot 1 + H_{ij}H_{jj} + H_{ii}H_{ji} + k_1 + k_4 \\ &\quad - k_2 - k_3 \\ &= 0. \end{aligned}$$

This proves $D(v)\ D(v)^T = dI$ and since $H^T = -H$ we also have $D(v)^T\ D(v) = dI$.

EXAMPLE. There are 620 codewords of minimum weight 8 in code $C(31)$. Since the group $PSL_2(31)$ acts 3-homogeneously on $GF(31) \cup \{\infty\}$ the codewords of weight 8 are the blocks of a 3-design. The seven codewords of weight 8 that contain $\infty$, 0 and 1 are listed below. The semi-colon separates non-zero squares from non-squares

$$\begin{aligned} v_1 &= \{\infty,\ 1,\ 9,\ 25;\ 0,\ 6,\ 26,\ 27\} \\ v_2 &= \{\infty,\ 1,\ 5,\ 14;\ 0,\ 6,\ 11,\ 30\} \\ v_3 &= \{\infty,\ 1,\ 16,\ 19;\ 0,\ 3,\ 6,\ 23\} \\ v_4 &= \{\infty,\ 1,\ 2,\ 7;\ 0,\ 6,\ 12,\ 15\} \\ v_5 &= \{\infty,\ 1,\ 9,\ 18;\ 0,\ 11,\ 15,\ 23\} \\ v_6 &= \{\infty,\ 1,\ 7,\ 20;\ 0,\ 3,\ 11,\ 27\} \\ v_7 &= \{\infty,\ 1,\ 5,\ 25;\ 0,\ 15,\ 3,\ 13\} \end{aligned}$$

Now

$$\Omega^* = \{v_i P_k;\ k \in GF(31,\ k = \square, \text{ and } i = 1,\ldots,7\}$$

and we conclude that $s = 0$.

The matrix

$$D(v_1) = \begin{array}{c|cccccccc} & \infty & 1 & 9 & 25 & 0 & 6 & 26 & 27 \\ \hline \infty & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & 1 & 1 & -1 \\ 9 & 1 & -1 & -1 & 1 & -1 & 1 & -1 & 1 \\ 25 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 6 & 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 26 & 1 & -1 & 1 & -1 & 1 & -1 & -1 & 1 \\ 27 & 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \end{array}$$

is an $8 \times 8$ Hadamard matrix. If

$$w_1 = \{\infty, 2, 5, 7; 3, 15, 17, 27\},$$

$$w_2 = \{\infty, 4, 5, 7, 9, 19; 17, 29\},$$

$$w_3 = \{\infty, 1, 2, 7, 8, 16; 3, 13\},$$

$$w_4 = \{\infty, 2, 4, 8, 9, 14; 3, 17\}$$

then a similar argument shows that

$$\Omega = \{w_i P_k : k \in GF(31), k = \square, \text{ and } i = 1,2,3,4\}.$$

We conclude that $t = 3$ and $r = 1$.

Chapter 5 is joint work with David B. Wales. The results presented here will be submitted to the SIAM Journal on Algebraic and Discrete Methods.

## REFERENCES

[1] E. F. Assmus, Jr., H. F. Mattson, Jr., and H. E. Sachar, A new form of the square root bound, Siam J. Applied Math., 30(1976), 352-354.

[2] V. K. Bhargava, S. E. Tavares, and S.G.S. Shiva, Difference sets of the Hadamard type and quasi-cyclic codes, Info. and Control, 26(1974), 341-350.

[3] P. J. Cameron and J. H. van Lint, Graph Theory, Coding Theory and Block Designs, London Math. Soc. Lecture Notes Series No. 19 (Cambridge Univ. Press, London, 1975).

[4] P. Camion, Global quadratic abelian codes, Information Theory (C.I.S.M. Courses and Lectures, No. 219) G. Longo, Ed. Vienna Springer 1975.

[5] M.J.E. Golay, Notes on digital coding, Proc. IEEE, 37(1949), 657.

[6] M. Hall, Jr., Note on the Mathieu group $M_{12}$, Arch. Math. 13(1962), 334-340.

[7] J. H. van Lint, Recent results on perfect codes and related topics, in Combinatorics part 1 (M. Hall, Jr., and J. H. van Lint editors) Mathematical Centre Tracts 55(1974), 158-178.

[8] J. H. van Lint and F. J. MacWilliams, Generalized quadratic residue codes, IEEE Trans. Info. Theory, IT-24(1978), 730-737.

[9] F. J. MacWilliams and M. Karlin, Quadratic residue codes over GF(4) and their binary images, unpublished report.

[10] F. J. MacWilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, Amsterdam: North Holland 1978.

[11] C. L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, Info. and Control, 22(1973), 188-200.

[12] R.E.A.C. Paley, On orthogonal matrices, J. Math. and Phys., 12(1933), 311-320.

[13] O. Perron, Bemerkungen über die Verteilung der quadratischen Reste, Math. Zeit., 56(1952), 122-130.

[14] V. Pless, On a new family of symmetry codes and related new 5-designs, Bull. Am. Math. Soc., 75(1969), 1339-1342.

[15] V. Pless, The weight of the symmetry code for p = 29 and the 5-designs contained therein, Annals N. Y. Acad. Sci. 175(1970), 310-313.

[16] V. Pless, Symmetry codes over GF(3) and new 5-designs, J. Comb. Theory 12(1972), 119-142.

[17] V. Pless, Symmetry codes and their invariant subcodes, J. Comb. Theory, 18(1975), 116-125.

[18] H.C.A. van Tilborg, On weights in codes, Report 71-WSK-03, Department of Mathematics, Technological University of Eindhoven, Netherlands, December 1971.

[19] H. N. Ward, Quadratic residue codes and symplectic groups, J. Algebra, 29(1974), 150-171.