Generalized quadratic residue codes

Generalized Quadratic Residue Codes

JACOBUS H. VAN LINT AND F. JESSIE MACWILLIAMS

Abstract—**A simple definition of generalized quadratic residue codes, that is, quadratic residue codes of block length p^m, is given, and an account of many of their properties is presented.**

I. INTRODUCTION

LET p,l be distinct primes such that l is a quadratic residue of p. Let $\mathbb{F}=\mathrm{GF}(l)$, and let G be the Abelian group of the additive structure of $\mathrm{GF}(p)$. The (classical) quadratic residue codes A^+,B^+,A,B are certain ideals in the group algebra $\mathbb{F}G$. G is of course a cyclic group, and the group operation is written as multiplication, i.e., $G=\{1,x,x^2,\cdots,x^{p-1}\}$. A^+ is defined as follows. Let ξ be a primitive pth root of unity over $\mathbb{F}$; a polynomial $c(x)$ of $\mathbb{F}G$ is in A^+ if $c(\xi^r)=0$ for all r which are quadratic residues of p. The code A has one as an additional zero. B^+,B are defined similarly with respect to the nonresidues of p. (See [1], [6], [8].)

We wish to extend this idea to codes of block length $q=p^m$, $m>1$. These will be called generalized quadratic residue (GQR) codes. The restrictions on $\mathbb{F}$ will be described later; in fact, if m is even, there are no restrictions except that $\mathbb{F}$ should not have characteristic p. $\mathbb{F}$ can even be taken to be the real numbers. G is now the Abelian group of the additive structure of $\mathrm{GF}(p^m)$. It is no longer cyclic, but is an elementary Abelian group of type $\{p,p,\overleftarrow{\cdots}^{m}\overrightarrow{\cdots},p\}$, which means that it is the direct product of m cyclic groups of order p. The code positions will be identified with the elements of G. Since we need addition and multiplication both in $\mathrm{GF}(p^m)$ and in the group algebra $\mathbb{F}G$, we use the symbols $\oplus$ and $*$ for these operations in $\mathbb{F}G$; a sum in $\mathbb{F}G$ will be denoted by $\mathbb{\Sigma}$.

We remind the reader that $\mathbb{F}G$ consists of all formal sums $\mathbb{\Sigma}_{g\in G}a_g g$, $a_g\in\mathbb{F}$, with the following rules for addition and multiplication:

$$\Big(\mathbb{\sum}_{g\in G}a_g g\Big)\oplus\Big(\mathbb{\sum}_{g\in G}b_g g\Big)=\mathbb{\sum}_{g\in G}(a_g+b_g)g \tag{1}$$

$$\Big(\mathbb{\sum}_{g\in G}a_g g\Big)*\Big(\mathbb{\sum}_{g\in G}b_g g\Big)=\mathbb{\sum}_{g\in G}\Big(\sum_{g_1+g_2=g}a_{g_1}b_{g_2}\Big)g. \tag{2}$$

A subset S of G can be interpreted as an element of $\mathbb{F}G$ by taking $a_g=1$ if $g\in S$ and $a_g=0$ if $g\notin S$. We use the same symbol for the set and the corresponding element of $\mathbb{F}G$. In particular, $U,V,0$ are the elements of $\mathbb{F}G$ corresponding, respectively, to the set of nonzero squares of $\mathrm{GF}(q)$, the set of nonsquares, and the single element $\{0\}$. A vector $\boldsymbol{c}$ with coordinates c_g is identified with the element $\mathbb{\Sigma}_{g\in G}c_g g$ of $\mathbb{F}G$. We denote the usual inner product of two vectors $\boldsymbol{c},\boldsymbol{c}'$ by $\langle \boldsymbol{c}\cdot\boldsymbol{c}'\rangle$.

A character ψ of G is a homormorphism of G into the set of pth roots of unity over $\mathbb{F}$. The characters of G form a group χ which is isomorphic in many ways to G, let us say $\psi_g\leftrightarrow g$. The exact form of the isomorphism we need will be discussed in Section II. For a detailed account of the properties of characters as applied to coding theory, see [7]. A character is extended in the obvious way to a linear functional on the group algebra

$$\psi_f\Big(\mathbb{\sum}a_g g\Big)=\sum\alpha_g\psi_f(g).$$

Manuscript received February 9, 1978.

J. H. van Lint was with Bell Laboratories, Murray Hill, NJ, on leave from the Department of Mathematics, Technological University Eindhoven, Eindhoven, The Netherlands.

F. J. MacWilliams is with Bell Laboratories, Murray Hill, NJ 07974.

0018-9448/78/1100-0730$00.75

We are now in a position to define the GQR codes A^+, B^+ of block length $q=p^m$.

Definition 1: The code A^+ consists of all $c=\sum c_g g$ for which $\psi_u(c)=0$, for all $u\in U$. B^+ is defined in the same way, replacing U by V. The codes A, B have the additional requirement that $\psi_0(c)=0$. A is a subcode of A^+, and B is a subcode of B^+. It is readily apparent that the dimension of A^+, B^+ is $\frac{1}{2}(q+1)$ and that of A, B is $\frac{1}{2}(q-1)$. (See [7].)

Remark: One easily checks that for $m=1$ this definition agrees with the usual definition of quadratic residue codes. If G is the cyclic group $1, x, x^2, \cdots, x^{p-1}$ and ξ is a primitive pth root of unity, the characters are the mappings $x\to\xi^r$.

This generalization of the classical quadratic residue codes to codes of block length $q=p^m$ occurred in a disguised form in Delsarte [3]. In Section VII we shall show the connection. Later they were defined by Ward [10] and Camion [2] in a much more abstract way than that given above. The proofs of our theorems are usually straightforward generalizations of methods used in the classical case. The interested reader can check that our codes are essentially the same as those described by Ward and Camion. The main purpose of our paper is to present the GQR codes in an elementary way and to show the connection with [3].

$\mathbb{F}G$ is a semisimple group algebra; hence A^+, B^+ are principal ideals, generated by idempotents E_A, E_B. The form of these idempotents is given in Section III. Clearly, A^+, B^+ are equivalent codes, being interchanged by the permutation $g\to gv$ for any nonsquare v.

These codes are extended to codes of block length $q+1$, let us say A_∞, B_∞, by adding a "parity check" symbol in a new coordinate position labeled ∞. The extended codes are invariant under a group of monomial transformations, of which the permutation part is PSL$(2,q)$. If $-1\in V$, then $A_\infty = A_\infty^{\perp}$; if $-1\in U$, then $A_\infty = B_\infty^{\perp}$. This is discussed in Section IV.

The minimum distance d of A^+ satisfies a square-root bound, i.e., $d^2\geq q$ or $d^2-d+1\geq q$. Further, if $m=2t$, then $d=\sqrt{q}=p^t$ over any field $\mathbb{F}$. The supports of the codewords of weight d always form a 2-design, and sometimes a 3-design. This is the subject of Section V.

In Section VI various forms of the generator matrix for A^+ and A_∞ are described, and it is shown that in the case $m=2t$ certain subsets of the coordinate places cannot be taken as information sets.

II. The Character Group

Let ξ be a primitive pth root of unity in some extension field $\hat{\mathbb{F}}$ of $\mathbb{F}$. Let α be a zero of an irreducible polynomial of degree m over GF(p). (In fact, we usually take α to be a primitive element of GF$(p^m)^*$.) Every element of GF(p^m) can be represented as $g=i_0+i_1\alpha+\cdots+i_{m-1}\alpha^{m-1}$, $i_v\in$GF(p). Define the character $\psi_1: G\to\hat{\mathbb{F}}$ by

$$\psi_1(g)=\xi^{i_0}. \tag{3}$$

TABLE I

	ψ_0	ψ_1	ψ_α	ψ_{α^2}	ψ_{α^3}	ψ_{α^4}	ψ_{α^5}	ψ_{α^6}	ψ_{α^7}
0	1	1	1	1	1	1	1	1	1
1	1	ξ	1	ξ	ξ^2	ξ^2	1	ξ^2	ξ
α	1	1	ξ	ξ^2	ξ^2	1	ξ^2	ξ	ξ
α^2	1	ξ	ξ^2	ξ^2	1	ξ^2	ξ	ξ	1
α^3	1	ξ^2	ξ^2	1	ξ^2	ξ	ξ	1	ξ
α^4	1	ξ^2	1	ξ^2	ξ	ξ	1	ξ	ξ^2
α^5	1	1	ξ^2	ξ	ξ	1	ξ	ξ^2	ξ^2
α^6	1	ξ^2	ξ	ξ	1	ξ	ξ^2	ξ^2	1
α^7	1	ξ	ξ	1	ξ	ξ^2	ξ^2	1	ξ^2

For each $h\in G$ define the character ψ_h by

$$\psi_h(g)=\psi_1(gh) \tag{4}$$

which of course implies that $\psi_0(g)=1$.

It is easily checked that the mapping $\psi_h\leftrightarrow h$ is an isomorphism between the group of characters χ and G. We shall often use the following properties of characters.

For any elements $a, b\in\mathbb{F}G$ and any character ψ,

$$\psi(a*b)=\psi(a)\psi(b), \tag{5}$$

and for any $f, g\in G$,

$$\psi_f(g)=\psi_g(f) \tag{6}$$

$$\sum_{\psi\in\chi}\psi(g)=\begin{cases}0, & \text{if } g\neq 0\\ q, & \text{if } g=0\end{cases} \tag{7}$$

$$\sum_{g\in G}\psi_f(g)=\begin{cases}0, & \text{if } f\neq 0\\ q, & \text{if } f=0.\end{cases} \tag{8}$$

An element a of $\mathbb{F}G$ is determined by the values $\psi_h(a)$ for all $h\in G$.

Example 1: Let $p^m=3^2$, and take the following representation for GF(3^2):

$$00=0 \quad 10=1 \quad 01=\alpha \quad 12=\alpha^2 \quad 22=\alpha^3$$
$$20=\alpha^4 \quad 02=\alpha^5 \quad 21=\alpha^6 \quad 11=\alpha^7.$$

The character table for G is given in Table I. The entry in place $(\alpha^i, \psi_{\alpha^j})$ is the value of the character $\psi_{\alpha^j}(\alpha^i)$.

III. The Idempotent

As mentioned in the introduction, A^+ is a principal ideal generated by an idempotent E_A, which has the property that $E_A * E_A = E_A$. In this section we find an expression for E_A.

Lemma 1: There exist constants $c_0, c_1\in\mathbb{F}$ such that $\psi_u(U)=c_0$ and $\psi_u(V)=c_1$, for all $u\in U$ and $\psi_v(U)=c_1$ and $\psi_v(V)=c_0$, for all $v\in V$. Furthermore, we may take

$$c_0=(-1-\sqrt{q})/2 \qquad c_1=(-1+\sqrt{q})/2, \qquad \text{if } -1\in U \tag{9}$$

$$c_0=(-1-\sqrt{-q})/2 \qquad c_1=(-1+\sqrt{-q})/2, \qquad \text{if } -1\in V. \tag{10}$$

Proof: If $u \in U$, then

$$\psi_u(U) = \sum_{g \in U} \psi_u(g) = \sum_{g \in U} \psi_1(ug) = \sum_{h \in U} \psi_1(h) = \psi_1(U).$$

A similar argument proves the other cases.

Let $n \in V$. Then summing over all characters,

$$\sum_{\psi \in \chi} \psi(U)\psi(-n) = \sum_{\psi \in \chi} \sum_{u \in U} \psi(u-n) = 0$$

by (7). Also,

$$\begin{aligned}\sum_{\psi \in \chi} \psi(U)\psi(-n) &= \psi_0(U)\psi_0(-n) + \sum_{u \in U} \psi_u(U)\psi_u(-n) \\ &\quad + \sum_{v \in V} \psi_v(U)\psi_v(-n) \\ &= (q-1)/2 + c_0 \sum_{u \in U} \psi_1(-un) \\ &\quad + c_1 \sum_{v \in V} \psi_1(-vn) \\ &= \begin{cases} (q-1)/2 + 2c_0c_1, & \text{if } -1 \in U \\ (q-1)/2 + c_0^2 + c_1^2, & \text{if } -1 \in V. \end{cases}\end{aligned}$$

Since $\psi_1(0 \oplus U \oplus V) = \sum_{g \in G} \psi_1(g) = 0$ by (8), we find $1 + c_0 + c_1 = 0$, and we now have a quadratic equation with zeros c_0, c_1. The choice $c_0 = \frac{1}{2}(-1 - \sqrt{\pm q})$ is arbitrary; it depends upon the choice of ξ. Q.E.D.

If $m = 2t$, then $-1 \in U$, $c_0 = (-1 - p^t)/2$, and $c_1 = (-1 + p^t)/2$. If $m = 2t+1$, then $-1 \in U$ if $p = 4s+1$, $-1 \in V$ if $p = 4s-1$, and

$$c_0, c_1 = \begin{cases} (-1 \mp p^t\sqrt{p})/2, & \text{if } p = 4s+1 \\ (-1 \mp p^t\sqrt{-p})/2, & \text{if } p = 4s-1. \end{cases}$$

Let R_0, R_1 denote the quadratic residues and nonresidues of p, and let $\theta = \sum_{i \in R_0} \xi^i - \sum_{i \in R_1} \xi^i$. Then (see [8])

$$\theta^2 = \begin{cases} p, & \text{if } p = 4s+1 \\ -p, & \text{if } p = 4s-1. \end{cases}$$

Thus for $m = 2t+1$, $c_0, c_1 = (-1 \mp p^t\theta)/2$.

Example 2: Let $p^m = 3^3$. We may take $c_0, c_1 = (-1 \mp 3\sqrt{-3})/2 = (-1 \mp 3(\xi - \xi^2))/2$, i.e., $c_0 = 1 + 3\xi^2$ and $c_1 = 1 + 3\xi$. In general, if $m = 2t+1$, we may take

$$c_0 = (p^t - 1)/2 + p^t \sum_{i \in R_1} \xi^i \qquad c_1 = (p^t - 1)/2 + p^t \sum_{i \in R_0} \xi^i.$$

Lemma 2: The generating idempotents of the GQR codes are given by

$$qE_A = \begin{cases} (q+1)/2 \cdot 0 \oplus -c_0U \oplus -c_1V, & \text{if } -1 \in U \\ (q+1)/2 \cdot 0 \oplus -c_1U \oplus -c_0V, & \text{if } -1 \in V. \end{cases}$$

qE_B is obtained by interchanging c_0 and c_1.

Proof: We give the proof for the first case; the others are similar. By Lemma 1,

$$\psi_0(E_A) = q^{-1}\{(q+1)/2 - c_0(q-1)/2 - c_1(q-1)/2\} = 1$$

$$\psi_u(E_A) = q^{-1}\{(q+1)/2 - c_0^2 - c_1^2\} = 0, \qquad \text{for } u \in U$$

$$\psi_v(E_A) = q^{-1}\{(q+1)/2 - 2c_0c_1\} = 1, \qquad \text{for } v \in V.$$

TABLE II

		00 0	10 1	01 α	12 α^2	22 α^3	20 α^4	02 α^5	21 α^6	11 α^7
00	0	5	2	−1	2	−1	2	−1	2	−1
$M=$10	1	2	5	2	−1	2	2	−1	−1	−1
01	α	−1	2	5	−1	2	−1	−1	2	2
12	α^2	2	−1	−1	5	2	−1	2	2	−1
22	α^3	−1	2	2	2	5	−1	2	−1	−1
20	α^4	2	2	−1	−1	−1	5	2	−1	2
02	α^5	−1	−1	−1	2	2	2	5	−1	2
21	α^6	2	−1	2	2	−1	−1	−1	5	2
11	α^7	−1	−1	2	−1	−1	2	2	2	5

Thus $\psi_g(E_A)$ is zero or one for all $g \in G$, which shows that E_A is idempotent; moreover, it has the correct zeros to be the idempotent of A^+. Q.E.D.

Remark: Compare the form of the idempotent for classical quadratic residue codes, as given in [8].

Lemma 3: Suppose $m = 2t+1$. If l is a quadratic residue of p, then $c_0, c_1 \in \mathrm{GF}(l)$, and we may take $\mathbb{F} = \mathrm{GF}(l)$. If it is not, we must take $\mathbb{F} = \mathrm{GF}(l^2)$.

Proof: θ is in some extension field of GF(l) which contains the pth roots of unity. (For example, $\theta \in \mathrm{GF}(l^{p-1})$.) In this field

$$\theta^l = \begin{cases} \theta, & \text{if } l \in R_0 \\ -\theta, & \text{if } l \notin R_0. \end{cases}$$

Thus $c_0, c_1 \in \mathrm{GF}(l)$ if $l \in R_0$, and in any case $c_0, c_1 \in \mathrm{GF}(l^2)$. Q.E.D.

Example 3:

i) Let $p^m = 3^3$ and $l = 7$, which is a quadratic residue of three. Then we may take $\xi = 2$. Thus

$$c_0 = 1 + 12 = 6 \bmod 7 \qquad c_1 = 1 + 6 = 0 \bmod 7 \qquad E_A = -V.$$

ii) Take $p^m = 3^3$ and $l = 2$. Then $\mathbb{F} = \mathrm{GF}(2^2)$, and $E_A = \xi^2U + \xi V$, where $\xi^3 = 1$.

Definition 2: A generator matrix M for A^+ may now be constructed as follows. Label the rows and columns of M by the elements $0, 1, \alpha, \alpha^2, \cdots, \alpha^{q-2}$ of GF(q). The first row of M contains the coordinates of qE_A, and the entry in place (α^i, α^j) is the coordinate of qE_A in place $(\alpha^j - \alpha^i)$. M is a $q \times q$ matrix with rank $(q+1)/2$. Other forms for a generator matrix will be discussed in Section VI.

Example 4: Let $p^m = 3^2$, $c_0 = (-1-3)/2 = -2$, and $c_1 = (-1+3)/2 = 1$. Using the table of GF(3^2) given in Example 1 we obtain the results given in Table II.

IV. The Extended Code and Its Automorphism Group

The codes A_∞, B_∞ are obtained from A^+, B^+ by adding a parity check c_∞ in a position which we label as ∞. c_∞ is defined as follows.

Definition 3: If $c = \sum_{g \in G} c_g g$ is a codeword of A^+ or B^+ and $-1 \in V$ (which implies $m = 2t+1$), then

$$c_\infty = \frac{\sqrt{-q}}{q} \sum_{g \in G} c_g = \frac{\theta}{p^{t+1}} \sum_{g \in G} c_g.$$

If $-1 \in U$, then

$$c_\infty = \begin{cases} \frac{\sqrt{q}}{q} \sum_{g \in G} c_g, & \text{for } c \in A^+ \\ -\frac{\sqrt{q}}{q} \sum_{g \in G} c_g, & \text{for } c \in B^+. \end{cases}$$

In fact, c_∞ is chosen to make the extended idempotent (E_A, Y) invariant under the monomial form of PSL$(2,q)$ as will presently appear.

Lemma 4: If $-1 \in V$, then A_∞, B_∞ are self-dual. If $-1 \in U$, then $A_\infty = B_\infty^\perp$.

Proof: Let $I = q^{-1}(0 \oplus U \oplus V)$ in $\mathbb{F}G$. I is characterized by the property that

$$\psi_0(I) = 1 \qquad \psi_h(I) = 0, \qquad \text{for all } h \neq 0. \tag{11}$$

Assume $-1 \in V$. Let $c = (\sum c_g g, c_\infty)$, $c' = (\sum c'_g g, c'_\infty)$ be two codewords of A_∞. For all $v \in V$

$$\psi_v\Big(\sum c'_g(-g)\Big) = \psi_{-v}\Big(\sum c'_g g\Big) = 0.$$

Hence

$$\psi_h\Big(\sum c_g g * \sum c'_g(-g)\Big) = 0, \qquad \text{for all } h \neq 0.$$

Now

$$\psi_0\Big(\sum c_g g * \sum c_g(-g)\Big) = \Big(\sum c_g\Big)\Big(\sum c'_g\Big) = -q c_\infty c'_\infty.$$

Hence

$$\sum c_g g * \sum c'_g(-g) = -q c_\infty c'_\infty I.$$

Therefore,

$$\sum_{g \in G} c_g c'_g = -c_\infty c'_\infty,$$

i.e., $\langle c \cdot c' \rangle = 0$, and A_∞ is self-dual. A similar proof holds for the second statement. Q.E.D.

We shall now show (with some trouble) that A_∞, B_∞ are invariant under the action of a group of monomial transformations, of which the underlying permutation group is PSL$(2,q)$. Since the field automorphisms of GF(q) also leave the code invariant, the automorphism group of A_∞ contains a monomial form of PΣL$(2,q)$.

PSL$(2,q)$ consists of all permutations of the set GF$(q) \cup \infty$ of the form $i \to (ia+b)/(ic+d)$, where $a,b,c,d \in$ GF(q) and $ad - bc = 1$. It is generated by the following set of permutations.

T_1 The additive group of GF(q).
T_2 $i \to ui$, $u \in U$.
T_3 $i \to -1/i$.

T_1 and T_2 fix ∞, and by construction A^+ is invariant under T_1 and T_2. Hence so is A_∞. Hence it suffices to find a monomial transformation for which the underlying permutation is T_3, which preserves A_∞.

Let τ be the transformation formed by multiplying the coordinates in V and ∞ by -1 and then applying T_3.

Remark: There is some latitude as to whether the coordinates in places $0, \infty$ are or are not multiplied by -1. If we replaced the parity check c_∞ by $-c_\infty$, we would have to make a different choice.

A_∞ is generated by a matrix M_∞, obtained from the M of Definition 2 by adding an additional column ∞ which contains the parity check ($\sqrt{-q}$ if $-1 \in V$, $\sqrt{q}$ if $-1 \in U$).

We consider the case $-1 \in V$. The proof for the other case is similar.

i) The first row of M_∞ is mapped by τ into

$$-\sqrt{-q}\; 0 \oplus c_0 U \oplus -c_1 V, (q+1)/2.$$

For any $u \in U$

$$\psi_u\big(-\sqrt{-q}\; 0 \oplus c_0 U \oplus -c_1 V\big) = -\sqrt{-q} + c_0^2 - c_1^2 = 0,$$

and the entry in place ∞ agrees with Definition 3. Thus the permuted row is a codeword in A_∞.

ii) Let s be a square in GF(q), and let $\boldsymbol{r}_s$ be the row of M_∞ with label s. We will show by a rather lengthy argument that

$$(\boldsymbol{r}_s)^\tau = \boldsymbol{r}_{-1/s} + (c_0 0 \oplus -U, c_1).$$

$\boldsymbol{r}_s$ has $-c_0$ in place 0 ($-s \in V$), $(q+1)/2$ in place s, $-c_1$ in place $u+s$ for all squares u, $-c_0$ in place $v+s$ for all nonsquares v, and $\sqrt{-q}$ in place ∞. $(\boldsymbol{r}_s)^\tau$ has $-\sqrt{-q}$ in place 0, $(q+1)/2$ in place $-1/s$, $-c_1$ in place $-1/(u+s)$ if $u+s \in U$, c_1 in place $-1/(u+s)$ if $u+s \in V$, $-c_0$ in place $-1/(v+s)$ if $v+s \in U$, c_0 in place $-1/(v+s)$ if $v+s \in V$, and $-c_0$ in place ∞.

We now compare this with the row labeled $-1/s$, let us say $\boldsymbol{r}'_s$ of M_∞. $\boldsymbol{r}'_s$ has $-c_1$ in place 0, $(q+1)/2$ in place $-1/s$ (which is why we chose this row), $-c_1$ in place $u-1/s$ for all squares u, $-c_0$ in place $v-1/s$ for all nonsquares v, and $\sqrt{-q}$ in place ∞. Let $\boldsymbol{X} = (\boldsymbol{r}_s)^\tau - \boldsymbol{r}'_s$. Clearly, place $-1/s$ (a nonsquare) in $\boldsymbol{X}$ contains zero.

Let $u+s \in U$. Then $u/(s(u+s)) = 1/s - 1/(u+s) \in U$; i.e., $-1/(u+s) = u' - 1/s$, for some $u' \in U$, and place $-1/(u+s)$ (a nonsquare) in $\boldsymbol{X}$ contains zero.

If $u+s \in V$, then $-1/(u+s) = v' - 1/s$, for some $v' \in V$, and place $-1/(u+s)$ (a square) in $\boldsymbol{X}$ contains $c_0 + c_1 = -1$. Similarly, if $v+s \in U$, place $-1/(v+s)$ in $\boldsymbol{X}$ contains zero, and if $v+s \in V$, place $-1/(v+s)$ contains -1. In fact,

$$\begin{aligned} \boldsymbol{X} &= \big((-\sqrt{-q} + c_1)0 \oplus -U, -c_0 - \sqrt{-q}\big) \\ &= (c_0 0 \oplus -U, -c_1). \end{aligned}$$

Now $\psi_u(c_0 0 \oplus -U) = 0$ for all squares u, and the parity check $-c_1$ satisfies Definition 3. Thus $\boldsymbol{X} \in A_\infty$; hence $(\boldsymbol{r}_s)^\tau \in A_\infty$.

iii) If $t \in V$, a similar proof shows that row $\boldsymbol{r}_t$ of M_∞ is transformed by τ into a codeword of A_∞. The same method works for B_∞ and also for the case $-1 \in U$. These results give us the following theorem.

Theorem 1: The codes A_∞, B_∞ are invariant under a group of monomial transformations for which the underlying permutations form the group PSL$(2,q)$.

Corollary 1: The minimum weight of A_∞ is one more than the minimum weight of A^+.

Proof: Since A_∞ is invariant under a transitive group, each codeword of minimum weight can be transformed

into a word with $c_\infty \neq 0$. The word with c_∞ removed must be a minimum weight word of A^+.

Corollary 2: If $\boldsymbol{c} = \mathbb{S}_{g\in G} c_g g$ is a word of minimum weight in A^+, then $\sum c_g \neq 0$.

Let $-1 \in V$. Let S be the Paley matrix of order q. (See Hall [5].) Then

$$M_\infty = \left(q/2 I - \tfrac{1}{2}\sqrt{-q}\, S + \tfrac{1}{2}J;\ \sqrt{-q}\, j^T\right)$$

where J is the all-one matrix and j is the all-one vector. Since $SS^T = qI - J$ and $Sj^T = 0$, we find that

$$M_\infty M_\infty^T = 0.$$

This is another way of showing that A_∞ is self-dual.

V. The Square-Root Bound and the Exact Minimum Distance for $m = 2t$

For the GQR codes we have the following analog of the well-known square-root bound [1], [6], [8].

Theorem 2: Let $q = p^m$, and let d be the minimum distance of A^+ (resp. B^+) over some field $\mathbb{F}$. Then

i) $d \geq \sqrt{q}$,
ii) $d^2 - d + 1 \geq q$ if $-1 \in V$,
iii) $d = \sqrt{q}$ if m is even.

Proof: Let $\boldsymbol{c} = \mathbb{S}_{g\in G} c_g g$ be a codeword of minimum weight d in A^+. Let $n \in V$. Define $\boldsymbol{c}' = \mathbb{S}_{g\in G} c_g ng$. $\boldsymbol{c}'$ is a word of weight d in B^+. By Corollary 2

$$\psi_0(\boldsymbol{c}) \neq 0 \qquad \psi_0(\boldsymbol{c}') \neq 0;$$

thus

$$\psi_0(\boldsymbol{c} * \boldsymbol{c}') \neq 0,$$

and

$$\psi_h(\boldsymbol{c} * \boldsymbol{c}') = 0, \qquad \text{for all } h \neq 0.$$

Thus $\boldsymbol{c} * \boldsymbol{c}'$ is a nonzero multiple of $0 \oplus U \oplus V$.

Now $\boldsymbol{c} * \boldsymbol{c}'$ has at most d^2 nonzero coefficients; hence $d^2 \geq q$. If $-1 \in V$, we may take $n = -1$; then $\boldsymbol{c} * \boldsymbol{c}'$ has at most $d^2 - d + 1$ nonzero coefficients. This proves i) and ii).

Now let $m = 2t$. Define $K = \mathrm{GF}(p^t)$ and

$$U_i = |\alpha^{2i} k | k \in K \setminus \{0\}|, \qquad i = 0, 1, \cdots, (p^t - 1)/2, \ K^* = U_0.$$

All elements of K are squares in $\mathrm{GF}(p^{2t})$; hence

$$U = \sum_i U_i.$$

For any $u \in U$

$$\psi_u(U_i) = \sum_{g\in K^*} \psi_u(\alpha^{2i} g) = \sum_{g\in K^*} \psi_{\alpha^{2i} u}(g).$$

This is the sum of the values of a character over all nonzero elements of a field; hence it is -1 or $|K| - 1 = p^t - 1$. But $\sum_i \psi_u(U_i) = \psi_u(U) = c_0 = (-1 - p^t)/2$, which is possible only if $\psi_u(U_i) = -1$, for all i. It follows that $\psi_u(\mathbb{S}_{g\in K} g) = 1 + \psi_u(K) = 0$ and $\mathbb{S}_{g\in K} g \in A^+$. This proves iii). Q.E.D.

We now say a little more about the case $m = 2t$. Let $q^2 = p^{2t}$ (note that we now denote p^m by q^2); let $\boldsymbol{c} = \mathbb{S}_{g\in K}$ g. The vector $(\boldsymbol{c}, 1)$ is a codeword of weight $(q+1)$ in A_∞, and so are all vectors obtained from $(\boldsymbol{c}, 1)$ by the monomial form of $\mathrm{PSL}(2, q^2)$. The vectors obtained from $(\boldsymbol{c}, 1)$ by all transformations of $\mathrm{PGL}(2, q^2)$ are the circles of the finite miquelian inversive plane [4]; i.e., these vectors form a 3-design with parameters $3 - (q^2 + 1, q + 1, 1)$.

In [3] Delsarte defines A_∞ to be the binary code generated by the $q(q^2+1)/2$ circles obtained from $(\boldsymbol{c}, 1)$ by transformations of $\mathrm{PSL}(2, q^2)$. In the next section we show that A^+ can be generated by the $(q^2+1)/2$ vectors $\mathbb{S}_{g\in G} g$ and $\mathbb{S}_{g\in uK+b} g$, where $u \in U$, $b \in \mathrm{GF}(q^2)$, and $b \neq 0$. Thus Delsarte's A_∞ is the same as ours if we take $l = 2$. We can now prove the following theorem.

Theorem 3: If $t = 1$, i.e., $q = p$, then all minimum weight codewords of A_∞, B_∞ are circles in the miquelian plane.

It clearly suffices to prove that all codewords of weight q in A^+ are of the form $\mathbb{S}_{g\in uK+b} g$. The proof requires several lemmas. For these we do not need the restriction that $q = p$.

Lemma 5: Let $\boldsymbol{a} = \mathbb{S}_{g\in G} a_g g$ be a codeword of weight q in A^+, and suppose A_∞ contains $(\boldsymbol{a}, 1)$. Then $a_g = 0$ or 1, for all $g \in G$.

Proof: $(\boldsymbol{a}, 1)$ is orthogonal to all circles in B_∞, in particular to all vectors of the form $(\mathbb{S}_{g\in uK+b} g - 1)$, where $v \in V$ and $b \in \mathrm{GF}(q^2)$. Fix v, and let b run over $\mathrm{GF}(q^2)$; we obtain a set of q nonintersecting circles. Thus $\boldsymbol{a}$ must meet each of them in one point g, and $a_g = 1$. Q.E.D.

Lemma 6: Suppose $a_0 = 1$, i.e., $\boldsymbol{a}$ contains the point zero. Then $a_g = 1$ implies that g is a square in $\mathrm{GF}(q^2)$.

Proof: $(\boldsymbol{a}, 1)$ must be orthogonal to the extended idempotent of B_∞, which is $1/q^2((q^2+1)/2 \cdot 0 \oplus -c_1 U \oplus -c_0 V, -q)$. Suppose $a_g = 1$ for s values of g in U and t values in V. Then

$$s + t = q - 1$$
$$(q^2+1)/2 - c_1 s - c_0 t - q = 0.$$

Combining these we obtain $s - t = q - 1$, i.e., $s = q - 1$. Q.E.D.

We now suppose that q is a prime p.

Proof of Theorem 3: Let $\boldsymbol{a}$ be a codeword of weight q in A^+ with $a_0 = 1$. From Lemmas 5 and 6, we may suppose that $\boldsymbol{a}$ has ones at points of the set $A = \{0, u_1, u_2, \cdots, u_{p-1}\}$, $u_i \in U$. Let $A_i' = A - u_i = \{-u_i, u_1 - u_i, \cdots, 0, \cdots, u_{p-1} - u_i\}$. The vector $\boldsymbol{a}_i'$ with ones at the points of A_i' is also a codeword of A^+; thus $u_i - u_j \in U$, $i \neq j$.

Let $B = \{0, vu_1, vu_2, \cdots, vu_{p-1}\}$, $v \in V$. If $u_i + vu_j = u_s + vu_t$, $i \neq s$, $t \neq j$, then $u_i - u_s = v(u_t - u_j)$. But one side is a square and the other a nonsquare, a contradiction. Hence $A + B = \mathrm{GF}(p^2)$; that is, any element of $\mathrm{GF}(p^2)$ can be expressed as $x + y$, $x \in A$, $y \in B$. Further, $|A| \cdot |B| = p^2$.

Now it was proved by Sands [9] that if G is a group of type (p,p) having subsets A, B which satisfy the above conditions, then at least one of A, B, let us say A, contains

a nonzero element λ such that $A+\lambda=A$. But this implies that A is of the form $(0,u,2u,\cdots,(p-1)u)$, or $a=uc$. Q.E.D.

Thus we have the following result.

Theorem 4: Let A_∞, B_∞ be the extended GQR codes of block length p^2+1. Each of A_∞, B_∞ contains $\frac{1}{2}p(p^2+1)(l-1)$ codewords of minimum weight $(p+1)$. The $p(p^2+1)$ supports of these codewords form a $3-(p^2+1,p+1,1)$ design.

VI. Bases and Information Sets

In this section we are interested in the following problems.

i) Is it possible to specify *a priori*, and in some canonical way, a set of coordinate positions which form an information set for A_∞? (The answer to this question is that we can only say that certain sets will not do.)

ii) Is it possible to specify in some canonical way a subset of $(q+1)/2$ codewords which generate A_∞? (This, in fact, can be done for the case $m=2t$.)

First we describe a different and easier way to obtain the matrix M_∞. This is done by rearranging the rows and columns in the order $0,1,\alpha^2,\alpha^4,\cdots,\alpha^{q-3},\alpha,\alpha^3,\cdots,\alpha^{q-2},\infty$. Then

$M_\infty =$

$(q+1)/2$	$a,\cdots,a$	$b,\cdots,b$	c_∞
a $\vdots$ a	A	B	c_∞ $\vdots$
b $\vdots$ b	C	D	c_∞ $\vdots$

a and b are either $-c_0$ or $-c_1$.

Lemma 7:

i) A,B,C,D are circulant matrices with elements $(q+1)/2, -c_0, -c_1$ only.

ii) $a_{ii}=d_{ii}=(q+1)/2$; otherwise D is obtained from A by interchanging c_0 and c_1.

iii) C is obtained from B by interchanging c_0 and c_1 and a cyclic permutation one place to the left.

iv) Let $n=(q-1)/2$. In the first row of A, $a_{0j}=a_{0,n-j}$ if $-1\in U$. a_{0j} is obtained from $a_{0,n-j}$ by interchanging c_0 and c_1 if $-1\in V$

Proof:

i) $a_{ij}=$ the coordinate of E_A in place $\alpha^{2j}-\alpha^{2i}$. $a_{i+1,j+1}=$ the coordinate of E_A in place $\alpha^2(\alpha^{2j}-\alpha^{2i})=a_{ij}$. Thus A is circulant. A similar proof holds for the other matrices.

ii) d_{ij} comes from place $\alpha(\alpha^{2j}-\alpha^{2i})$ of E_A. If $i\neq j$, $d_{ij}=-c_1$ if $a_{ij}=-c_0$, and conversely.

iii) b_{ij} comes from place $\alpha^{2j+1}-\alpha^{2i+1}$ of E_A, and $c_{i-1,j-1}$ from place $\alpha^{2j}-\alpha^{2i}$.

iv) a_{0j} comes from place $\alpha^{2j}-1$, and $a_{0,n-j}$ from place $\alpha^{2n-2j}-1$.

TABLE III

	0	1	α^2	α^4	α^6	α	α^3	α^5	α^7	∞
0	5	2	2	2	2	−1	−1	−1	−1	3
1	2	5	−1	2	−1	2	2	−1	−1	3
α^2	2	−1	5	−1	2	−1	2	2	−1	3
α^4	2	2	−1	5	−1	−1	−1	2	2	3
α^6	2	−1	2	−1	5	2	−1	−1	2	3
α	−1	2	−1	−1	2	5	2	−1	2	3
α^3	−1	2	2	−1	−1	2	5	2	−1	3
α^5	−1	−1	2	2	−1	−1	2	5	2	3
α^7	−1	−1	−1	2	2	2	−1	2	5	3

Now $(\alpha^{2j}-1)(\alpha^{q-1-2j}-1)=\alpha^{q-1}-\alpha^{2j}-\alpha^{-2j}+1=(-1)((\alpha^{2j}-1)/\alpha^j)^2$, which proves iv). Q.E.D.

Example 5: The matrix of Example 4 arranged in this way is given in Table III.

The matrix A of Example 5 is invertible over any field of characteristic not equal to three. Thus in this case we may take the first five rows of M_∞ as a set of generators for A_∞ and the first five columns as an information set. This does not always happen.

Theorem 5: If $q\equiv 1 \bmod (4)$ and A_∞ is a GQR code of block length q^2+1, then $0\cup U$ and $0\cup V$ cannot be information sets.

We need a preliminary lemma.

Lemma 8: Let α be a primitive element of $GF(q^2)$. Then the following hold.

i) $\alpha^{i(q-1)}+1=\alpha^{l_1}$, where l_1+i is even, $i\neq(q+1)/2$.

ii) $\alpha^{i(q-1)}-1=\alpha^{l_2}$, where l_2+i is even if $q\equiv -1 \bmod (4)$ and l_2+i is odd if $q\equiv 1 \bmod (4)$.

Proof:

i) Let $\beta=\alpha^{iq}+\alpha^i$. Then $\beta^q=\beta$, i.e., $\beta\in GF(q)$. Hence if $\beta\neq 0$, $\beta=\alpha^{t(q+1)}$. Thus $l_1+i=t(q+1)$, which is even.

ii) Let $\alpha^{l_2+i}=\gamma=\alpha^{iq}-\alpha$. Then $\gamma^q=-\gamma$, so $\gamma=\alpha^{(2t+1)(q+1)/2}$, for some t. Thus $l_2+i=(2t+1)(q+1)/2$, and the result follows. Q.E.D.

Proof of Theorem 5: $\alpha^{(q+1)/2}\in V$, so the transformation $\phi: x\to\alpha^{(q+1)/2}(x+1)/(x-1)$ is in $PGL(2,q^2)$ and not in $PSL(2,q^2)$. The monomial transformation ϕ' corresponding to ϕ interchanges A_∞ and B_∞. Let $\boldsymbol{c}$ be the vector with one in places $\alpha^{i(q-1)}$, $0\leq i\leq q$, and zero elsewhere.

$\phi(1)=\infty$, and by Lemma 8

$$\phi(\alpha^{i(q-1)})=\alpha^{(q+1)}\cdot\alpha^{-i+t_i(q+1)}/\alpha^{-i+(2t_i'+1)(q+1)/2}$$
$$=\alpha^{(t_i-t_i')(q+1)}\in GF(q).$$

Hence ϕ maps $\boldsymbol{c}$ into a vector with one in the places labeled by $GF(q)\cup\infty$.

Since $(x+1)/(x-1)=1+(-2)-1/(x-1)$, ϕ' involves multiplication by -1 for exactly those i for which $\alpha^{i(q-1)}-1\in V$, i.e., for even i. Let $\boldsymbol{c}'$ be the vector with ± 1 in places $\alpha^{i(q-1)}$ according as i is odd or even. Then $(\boldsymbol{c}')^{\phi'}$ has one in the places of $GF(q)\cup\infty$, so $(\boldsymbol{c}')^{\phi'}$ is a codeword of A_∞. (Theorem 2.) Thus $\boldsymbol{c}'$ is a codeword of $B_\infty=A_\infty^\perp$. Thus if we take the columns of M_∞ indexed by $\alpha^{i(q-1)}$ (all

of which are in U) and alternately give them coefficients ± 1, the resulting sum is zero. Hence $0 \cup U$ cannot be an information set for A_∞. A similar argument shows that $0 \cup V$ cannot be an information set. Q.E.D.

In [10] Ward observes that if $q \equiv 3 \bmod (4)$, $q < 50$ and $\mathbb{F} = GF(2)$, $0 \cup U$ always contains an information set.

Another way of obtaining (maybe!) a set of basis vectors and an information set is as follows.

Find an element ϕ of $PSL(2,q)$ which has a cycle representation as two cycles of length $(q+1)/2$. (One way of doing this is to try permutations of the form $x \to (x+1)/\alpha^s x$, where $s = 2t$ if $-1 \in U$ and $s = 2t+1$ if $-1 \in V$.) Take any codeword, e.g., the extended idempotent, and act on it with ϕ'. This gives two $(q+1)/2 \times (q+1)/2$ matrices $(A|B)$ which are not quite circulants, since some coordinates are multiplied by -1.

Hopefully this matrix has rank $(q+1)/2$, and one or both of A, B are invertible, giving a canonical form for the generator matrix of A_∞. An example of this technique is given in Section VII.

We now describe how to find a set of basis vectors for A^+, B^+ for the case of block length q^2+1. The proof is essentially the same as in [10, th. 7.3]. $GF(q^2)$ is considered to be an affine two-dimensional space $AG(2,q)$ over $K = GF(q)$. From the proof of Theorem 2 the vector $\mathbb{S}_{g \in uK+b} g$ is in A^+ for all $u \in U$, and $\mathbb{S}_{g \in vK+b} g$ is in B^+ for all $v \in V$. These codewords are the lines of $AG(2,q)$. Also $qI = 0 \oplus U \oplus V$ is in both A^+, B^+.

Let H_A be a $(q^2+1)/2 \times q^2$ matrix, consisting of the coordinates of qI and of all codewords $\mathbb{S}_{g \in uK+b} g$ with $b \neq 0$. Let H_B consist of qI and all codewords $\mathbb{S}_{g \in vK+b} g$ with $b \neq 0$. Clearly, H_A, H_B generate subcodes A', B' of A^+, B^+. Since qI is the sum of any parallel class of lines, $A'(B')$ contains all the lines in $A^+(B^+)$. Let P be any point of $AG(2,q)$. The sum of $-qI$ and all lines through P has a nonzero entry only in the position corresponding to P. Hence A', B' together generate a code of dimension q^2. This implies that A', B' both have dimension $(q^2+1)/2$. Thus we have proved the following theorem.

Theorem 6: If A^+ is a GQR code of length q^2 over some field $\mathbb{F}$ and $K = GF(q)$, then the words qI and $\mathbb{S}_{g \in uK+b} g$, $b \neq 0$, form a basis for A^+.

Of course, a basis for A_∞ is obtained by adding a column containing the appropriate parity check.

VII. Designs

$PSL(2,q)$ is 2-transitive; hence the supports of the codewords of minimum weight in A_∞ form a 2-design. In addition, if $-1 \in V$, $PSL(2,q)$ is a 3-homogeneous group (i.e., any 3-set can be transformed into any 3-set), and the supports of the codewords of minimum weight form a 3-design.

If $q = p^{2t}$, the minimum weight is $p^t + 1$. We have already described (Section V) the designs which occur in this case. Here we given an example.

TABLE IV

5	2	2	2	2	−1	−1	−1	−1	3
2	5	−1	2	−1	2	2	−1	−1	3
2	−1	5	−1	2	−1	2	2	−1	3
2	2	−1	5	−1	−1	−1	2	2	3
2	−1	2	−1	5	2	−1	−1	2	3

TABLE V

1	2	3	4	5	6	7	8	9	10
	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			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		1						1
1		1		1					1
	1	1	1	1					

Example 6: Consider the top half of the matrix of Example 5, as shown in Table IV. The determinant of the 5×5 matrix on the left is 9^3; hence this matrix is invertible over any finite field of characteristic not equal to three. By multiplying by this inverse (over the reals), we find a generator matrix for A_∞ of the form

$$G = (I_5|C) = \left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 0 & 0 & -1 & -1 & -1 & -1 & -1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{array}\right].$$

By Section V this code should contain $\frac{1}{2}q(q^2+1) = \frac{1}{2} \cdot 3.10 = 15$ supports for vectors of weight four, and these supports form a $2-(10,4,2)$ design. In fact, these vectors are as shown in Table V.

If we add the 15 supports of words of weight four in the dual code B_∞, we obtain the 30 blocks of the miquelian plane $3-(10,4,1)$. We now give an example in which $-1 \in V$.

Example 7: Let $q = 27$. If $\mathbb{F} = GF(p)$, then p must be a quadratic residue of three, and the smallest such p is seven. From Lemma 1 we find that $c_0 = -1$ and $c_1 = 0$; hence $qE_A = V$.

In order to study this code, we proceeded as suggested in Section VI. Let α be a primitive element of $GF(3^3)$ with $\alpha^3 = \alpha^2 + 2$. The permutation $\phi: x \to (x+1)/\alpha^7 x$ consists of two cycles:

$$(\alpha^{20}, \alpha^{14}, \alpha^3, \alpha^8, \alpha^{12}, \alpha^{17}, \alpha^{25}, \alpha^{11}, \alpha^9, \alpha^{16}, \alpha^{23}, \alpha^{21}, \alpha^7, \alpha^{15})$$
$$(\infty, \alpha^{19}, \alpha^{22}, \alpha^5, \alpha^2, \alpha^{24}, 1, \alpha^6, \alpha^8, \alpha^4, \alpha, \alpha^{10}, \alpha^{13}, 0).$$

TABLE VI

20	14	3	8	12	17	25	11	9	16	23	21	7	15
		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	

TABLE VII

∞	19	22	5	2	24	0	6	8	4	1	10	13	0
1	1		1							1		1	
	−1	−1		−1							−1		−1
−1		1	−1		−1							−1	

TABLE VIII

0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	1	3	0	0	0	0	2	−1	0	3	2	−3	−2
0	−2	−3	2	3	0	−1	2	0	0	0	0	3	1

TABLE IX

20	14	3	8	12	17	25	11	9	16	23	21	7	15
ω^2	ω^2	ω	ω^2	ω^2	ω	ω	ω	ω	ω^2	ω	ω	ω	ω
α	19	22	5	2	24	0	6	8	4	1	10	13	
1	ω	ω^2	ω	ω^2	ω^2	ω^2	ω^2	ω^2	ω^2	ω	ω^2	ω	0

TABLE X

0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	1	ω^2	0	0	0	0	ω	1	0	ω^2	ω	ω^2	ω
0	ω	ω^2	ω	ω^2	0	1	ω	0	0	0	0	ω^2	1

We take V as the first row of the matrix; subsequent rows are obtained by applying ϕ to the previous row. The result is a matrix of the form $(A|B)$, where A,B would be circulants except for some multiplications by -1. The first three rows of A,B are shown in Tables VI and VII.

Some columns were multiplied by -1 so that both matrices become negacyclic (that is, cyclic except for the fact that the coordinate moved from the last to the first position is multiplied by -1). Both matrices are invertible, giving a generator matrix of the form $(I|C)$ or $(C'|I)$. C,C' are also negacyclic; their first rows are shown in Table VIII.

A computer search then showed that this code has minimum weight nine. (It sufficed to calculate the sums of four rows of C, since the number of codewords of weight i,j is the same as the number of weight j,i.) There are 1092 supports of codewords of weight nine, and these form a $3-(28,9,28)$ design. Since the size of PSL(2,27) is 9×1092, each codeword of minimum weight is fixed by a subgroup of order nine of PSL(2,27). For example, the word with coordinates 1, −1, −1, 2, 2, −2, 3, 3, −3 in positions α^{20}, α^{19}, α^8, α^6, α^{10}, 0, α^{22}, α, α^{13} is fixed by

$$x\to\frac{\alpha^{13}x+1}{\alpha^{17}x+\alpha^{20}} \qquad x\to\frac{\alpha^{8}x+\alpha^{17}}{\alpha^{8}x+\alpha^{20}}$$

which are both of order three and commute.

Example 8: We take the same code over the field GF(4). Let $GF(4)=\{0,1,\omega,\omega^2\}$. From Lemma 1 and Example 2, $E_A=\omega^2U\oplus\omega V$. The same permutation ϕ was used to obtain a 14×28 matrix $(A|B)$. A,B are now circulant matrices, with first rows as shown in Table IX. Both matrices are invertible, giving generator matrices for A_α of the form $(I|C)$ or $(C'|I)$, where the first row of C,C' is as shown in Table X. Again the minimum weight is nine, and the 1092 supports of codewords of weight nine form the same $3-(28,9,28)$ design as before.

ACKNOWLEDGMENT

The authors would like to express their gratitude to A. M. Odlyzko for several valuable suggestions and for the computations of Section VII. The proof of Theorem 3 was suggested by P. Camion.

REFERENCES

[1] E. F. Assmus, Jr., and H. F. Mattson, Jr., "New 5-designs," *J. Comb. Theory*, vol. 6, pp. 122–151, 1969.
[2] P. Camion, "Global quadratic Abelian codes," in *Information Theory* (CISM Courses and Lectures, no. 219), G. Longo, Ed. Vienna: Springer, 1975; also "Codes quadratiques abéliens et plans inversifs miquéliens," *C. R. Acad. Sci.* (Paris) t. 284, ser. A, pp. 1401–1404, June 6, 1977.
[3] P. Delsarte, "Majority logic decodable codes derived from finite inversive planes," *Inform. Contr.*, vol. 18, pp. 319–325, 1971.
[4] P. Dembowski, *Finite Geometries*. Berlin: Springer, 1968.
[5] M. Hall, Jr., *Combinatorial Theory*. Waltham, MA: Blaisdell, 1967.
[6] J. H. van Lint, *Coding Theory* (Lecture Notes in Math., no. 201). Berlin: Springer, 1971.
[7] F. J. MacWilliams, "Binary codes which are ideals in the group algebra of an Abelian group," *Bell Syst. Tech. J.*, vol. 49, pp. 987–1011, 1970.
[8] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam: North Holland, 1977.
[9] A. D. Sands, "On the factorization of finite Abelian groups," *Acta. Math. Acad. Sci. Hung.*, vol. 13, pp. 153–159, 1962.
[10] H. N. Ward, "Quadratic residue codes and symplectic groups," *J. Algebra*, vol. 29, pp. 150–171, 1974.