BEST AVAILABLE COPY
NOTICE: When government or other drawings, specifications or other data are used for any purpose other than in connection with a definitely related government procurement operation, the U. S. Government thereby incurs no responsibility, nor any obligation whatsoever; and the fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use or sell any patented invention that may in any way be related thereto.
The work reported in this document was performed at Lincoln Laboratory, a center for research operated by Massachusetts Institute of Technology, this work was supported by the U. S. Advanced Research Projects Agency under Air Force Contract AF19(604)-7400 (ARPA Order 56-61).
QUATERNARY CYCLIC CODES

by

G. Solomon

ABSTRACT

We consider cyclic codes for the quaternary alphabet, the field $K = \text{GF}(2^2)$. If $A$ is a $(k,n)$ (n odd) quaternary group codes - i.e., a $k$-dimensional subspace of ordered $n$-tuples of $K$ elements - then $A$ is isomorphic via the Solomon-Mattson polynomials, to a subgroup of the direct product of $K$ with $r$ copies of $L$. ($L$ is the smallest field over $K$ containing the $n^{\text{th}}$ roots of unity and $r$ is the number of irreducible factors of $x^n + \frac{1}{x} + 1$ over $K$.)

Let $d(A,K)$ be the minimum weight of non-zero vectors of $A$.

For $p$, a prime, and $A$, a $(k,p)$ cyclic $K$ code, $d(A,K) \geq d(A,F)$ where $d(A,F)$ is the Bose-Chaudhuri bound for the corresponding binary cyclic codes of the same order (if there is one). Number theoretic methods are introduced to improve the Zierler-Gorenstein lower bound for certain primes $p$. For $p$ such that 2 has multiplicative order $p-1$, there exists $(p+1/2, p)$ cyclic codes with $d(p) \geq 3$ if 3 is not a quadratic residue of $p$, $d(p) \geq 4$ if 3 is a quadratic residue of $p$, and $d \geq 5$ if both 3 and 5 are quadratic residues of $p$. 

GS:jj
I. Introduction

In this report we consider cyclic codes for the special alphabet of $2^2$ symbols. Interest in coding for this particular alphabet arose from private discussions with Dr. Robert Price. The work of M. Golay\(^4\) in the penny-weighing problem gives general results for alphabet of $p^m$ symbols. In addition, Zierler and Gorenstein\(^5\) have formulated decoding procedures for cyclic codes using $p^m$ symbols. We apply the methods of (2) and (3) to treat the special case. We improve the previous error correcting estimates and indicate how number-theoretic properties of primes enter in the general problem. The results are easily analogized to $p^2$ symbol alphabets and from there generalizable to $p^m$ symbols.

II. Preliminaries

The alphabet we wish to encode shall be elements of the field $K = GF(2^2)$ of degree 2 over $F$; the field of two elements. $K$ contains the elements 0, 1, $\alpha$, $\alpha^2$ subject to addition modulo 2 and the rule $\alpha^2 + \alpha + 1 = 0$. We are interested in linear mappings of $V_n(K)$ into $V_n(K)$ for $n$ odd. These are the $(k,n)$ group codes. We shall consider here a subclass of these codes which are generated by linear recursion. We derive the general error-correcting properties for these codes and give algorithms for particular $(p)$ to improve the general estimates.

Let $a = (a_0, a_1, \ldots, a_{n-1})$ be a vector of $V_n(K)$. Following (2), (3) we associate a polynomial of degree less than or equal to $(n-1)$ to the vector $a$, such that $g_a(\beta^i) = a_i$ where $\beta$ is a fixed primitive generator of the $n$th roots of unity. Corresponding to $a = (0, \ldots, 0)$ we put $g_a(x) = 0$. Putting $g_a(x) = \sum c_i x^i$ and using $g_a(\beta^i) \in K$ for $i = 0, 1, \ldots, n-1$, we obtain the condition that

\[ g_a(x)^4 = g_a(x) \text{ for } x = \beta^i \quad i = 0, 1, \ldots, n-1 \]

which yields
\((\Sigma c_i x^i)^4 = (\Sigma c_i x^i)\).

Reducing the powers of \(x\) modulo \(n\) gives us conditions on the \(c_i\)

\[c_0^4 = c_0; \quad c_{4i}^4 = c_i^4 \quad 1 \leq i \leq n-1.\]

The constants are now partitioned into mutually disjoint classes.

Thus the polynomial \(g_a(x)\) has in reality very few independent constants. Those are \(c_0, c_1, c_{i_1}, \ldots, c_{i_{r-1}}\) where \(c_1\) is the coefficient of \(x; c_{i_1}\) is the coefficient of \(x^{i_1}\) where \(i_1\) is the smallest integer such that \(i_1 \not\equiv 4^s \pmod{n}\) for any \(s; i_2\) is the smallest integer larger than \(i_1\) such that \(i_2 \not\equiv 4^s \pmod{n}\) and so on.

The polynomial \(g_a(x)\) can therefore be written as

\[g(x) = c_0 + c_1 x + c_1^4 x^4 + c_1^2 x^{16} + \ldots + c_{i_1} x^{i_1} + c_{i_1}^4 x^{4i_1} + \ldots + c_{i_2} x^{i_2} + c_{i_2}^4 x^{4i_2} + \ldots + c_{i_{r-1}} x^{i_{r-1}} + c_{i_{r-1}}^4 x^{4i_{r-1}} + \ldots\]

The coefficients \(c_i\) can also be given by the Reed formula

\[c_0 = \sum_{i=0}^{n-1} a_i\]

\[c_1 = \sum_{i=0}^{n-1} a_i \beta^{-i}\]
Thus \( c_0 \) is in \( K = \text{GF}(2^2) \) and the \( c_k \) are contained in the smallest field \( L \) over \( K \) containing the \( n \)th roots of unity. This also follows from the conditions \( c_{4^i} = c_i^4 \).

Thus to every code word \( a \in V_n(K) \) is associated a unique* set of \( (r(n) + 1) \) constants \( (c_0, c_1, c_1, \ldots, c_{i-1}) \). This correspondence is linearly additive (3). In particular, to every subgroup \( V_k(K) \) of \( V_n(K) \) is associated a subgroup \( G \) of the direct product of \( K \) with \( r \) copies of \( L \). Actually \( V_n(K) \) is the direct product of fields \( K \times L_1 \times L_2 \ldots \times L_r \) where \( L_j \) is a subfield (proper or improper) of \( L \) and the degree \( (L/L_j) = \text{order of } i_j \text{ modulo } n \). If \( n \) is a prime, the \( L_j = L \) all \( j \) and \( G \) for \( V_n(K) = K \times L^F \). For example, \( n = 9 \to G_9(K) \cong G = K \times L \times L \times K \times K \), \( \deg (L/K) = 3 \). For \( n = 5 \to G = K \times L^2 \), \( \deg (L/K) = 2 \).***

We are concerned with the number \( r(n) + 1 \) of independent constants at our disposal. The alphabet \( K = \text{GF}(2^2) \) is algebraically more fortunate than the alphabet \( F^{**} \), \( r(n) \) for \( F \) is sometimes 1. We have, however, for our case

**Lemma 1**: For \( n \) odd, \( r(n) \geq 2 \).

**Proof**: \( r(n) = 1 \) implies that \( 4^h \equiv 1 \) modulo \( n \) has \( h = n-1 \) as its smallest positive integer solution. Since 2 is prime to odd \( n \) we must have that \( 2^{\phi(n)} \equiv 1 \) (modulo \( n \)) where \( \phi(n) \) is the (Euler) number of integers prime to \( n \). For \( n \) odd, \( \phi(n) \) is even \( (2m) \). We have therefore \( 4^{2m} \equiv 1 \) (modulo \( n \)) and \( m < n-1 \). Thus \( r(n) \geq 2 \). q.e.d.

There are thus non-trivial cyclic codes for every odd \( n \). In particular, the map \( (c_0, c, 0, 0, \ldots) \to g(c_0, c, 0, 0; x = \beta^i) \)\( i = 0, \ldots, n-1 \) gives us a cyclic code over \( K \) of dimension \( (1 + s) \)

*Note that this depends on the choice of \( \beta \).

**See (3).**

***A correction of an earlier oversight in(3) thanks to S. Shatz."
where \( s = \text{degree of } L/K \) where \( L \) is the smallest field over \( K \) containing the \( n \)th roots of unity. The codes we shall consider are obtained by setting any of the \( c_i, i \neq 0 \), equal to zero. The groups of code words corresponding to this set (via \( g(\beta^i) \)) are generated by linear recursive sequences associated with finite difference equations.

Let \( V_k(K) \) be a subgroup of \( V_n(K) \) which corresponds to the set \( (c_0, c_1, c_1, c_2, \ldots c_{n-1}) \) where at least one of the \( c_i = 0 \). Then for \( \beta \) a primitive \( n \)th root of unity, we form the polynomial \( f(x) \) over \( K \) in the following manner.

\[
f(x) = \Pi f_j(x) = \sum_{i=0}^{k} d_i x^i
\]

where \( f_j(x) \) is the irreducible polynomial over \( K \) with \( \beta^j \) as a root. If \( k \) is the degree of \( f(x) \) then we associate to \( f(x) \) the difference equation of order \( k \)

\[
d_k y_{n+k} + d_{k-1} y_{n+k-1} + \cdots + d_1 y_m = 0
\]

The \( d_i \) are in \( K \) and for any \( k \) initial values in \( K \) we obtain a sequence of elements in \( K \) of period \( n \). There is then the natural mapping of \( V_k(K) \) into \( V_n(K) \) arising by taking the sequence of length \( n \) generated by any initial sequence of length \( k \). This is a standard cyclic code over the alphabet \( K \).

III. Error Correction Properties

We define the weight \( w(a) \) of a vector \( a \) in \( V_n(K) \) as the number of non-zero coordinates of \( a \). It is immediate that \( w(a + b) \leq w(a) + w(b) \) and \( w(a) = 0 \) if and only if \( a = 0 \). We may define a metric on \( V_n(K) \) by putting \( d(a, b) = w(a + b) \). As in the binary symbol case, a \( (k, n) \) group code is said to be \( r \) error correcting if \( d(0, a) \geq 2r + 1 \) for \( a \), any non-zero vector. Thus, the error correcting properties are given by the minimum weight \( d \) of any non-zero \( a \), i.e., \( n \) minus the number of zero coordinates of the
vector $a$. Since to every vector of our imbedded space $V_k$ is associated a polynomial $g_a(x)$, we need only look at the number of zeros of $g_a(x)$ on our multiplicative group of $n$th roots of unity to ascertain its weight.

IV. General Results

Let $n$ be odd and let $f(x) \in K[x]$ (the ring of polynomials over $K$) divide $x^n + 1$. Let $\zeta$ be a primitive $n$th root of unity. We define

$$E[\zeta] = \{e; 0 \leq e < n, f(\zeta^e) = 0\}$$

Then if $f(x)$ defines the recursion which imbeds $V_k(K)$ into $V_n(K)$, the associated polynomials $g_a(x)$ have degree at most $m$, the largest integer in $E(\zeta)$. Then we have

Theorem 1:* Let $\beta^d_0$ be the least positive power of $\beta$ which is a root of $f(x)$ then $d \geq d_0$.

Proof: It suffices to prove that for some primitive $n$th root of unity $\zeta$, the set $E(\zeta)$ has $n-d_0$ as maximum. Then the number of zeros of $g_a(x)$ is at most $n-d_0$, so the weight of $a$ is at least $n - (n-d_0) \geq d_0$.

We are given that $\beta, \beta^2, \ldots, \beta^{d_0-1}$ are not roots of $f(x)$ and that $\beta^{-1}$ is a root of $f(x)$. It follows immediately that $E(\zeta)$ for $\zeta = \beta^{-1}$ does not contain $n-1, n-2, \ldots, n-(d_0-1)$ but does contain $n-d_0$. This proof is from Mattson-Solomon(2).

We note that the set $E(\zeta)$ which are the powers of $x$ in $g_a(x)$ contains $4e$ modulo $n$ if it contains $e$. If $E(\zeta)$ contains $2e$ modulo $n$ for every $e$, then the polynomial $g_a(x)$ has the same power of $x$ as the $g_a$ for $K = F$. This holds if $2 = 4s \mod n$ or $2 = 2^{2s}$ or $2^{2s-1} = 1 \mod n$, i.e., $2$ has odd order modulo $n$. For such $p$, the bound on $d$ one obtains without investigating the coefficients is the Bose-Chaudhuri bound for the binary cyclic code of the same dimension.

Now where $2$ does not have odd order, we get a very small general estimate of $d_0$, which we will improve here. In particular

*This theorem for $K = F$ was proven in a different form first by Bose-Chaudhuri. For $K = GF(p^m)$, the Galois field of $p^m$ elements, this was done by Zierler-Gorenstein.
for $p \equiv 3 \pmod{4}$ where $2$ has order $p-1$, we obtain $d \geq 3$. We can improve this for particular $p$ of this type and indeed give a general algorithm.

We now present two lemmas on polynomials which we shall need for error correcting properties.

**Lemma 2:** Let $g(x) = b_{p-1} x^{p-1} + b_m x^m + \ldots + b_0$ where $b_i \in F$, $i = 0, \ldots, p-1$ and $b_m b_{p-1} \neq 0$. Then $g(x)$ can have at most $m+1$ zeros on $Z$, the group of $p$th roots of unity. Translated into coding terms, if $g(x) = g_1(x)$ of a vector $a$, then $\omega(a) \geq p - (m + 1)$.

**Proof:** Let $r$ be the number of roots of $g(x) \{ \beta_1, \ldots, \beta_r \}$ in $Z$. Let $(\gamma_1, \ldots, \gamma_{p-r-1})$ be the other roots of $g(x)$ contained in some suitable extension field. Let $\beta_1', \ldots, \beta_{p-r}'$ denote the elements of $Z$ which are not roots of $g(x)$. Denote by $s(\beta', i)$, $s(\beta', j)$, $s(\gamma', i)$ respectively the sums of products of $(\beta, \beta', \gamma)$ taken $i$ at a time, $(s(-, 0) = 1)$. We have for the first $l \leq p-1 - (m+1)$ values

$$\sum_{i+j=l} s(\beta, i) s(\beta', j) = \sum_{i+j=l} s(\beta, i) s(\gamma, j) = 0$$

since the appropriate coefficients in $x^p + 1$ and $g(x)$ are both zero. It then follows that for $j \leq l$

$$s(\beta', j) = s(\gamma, j)$$

If $p-r \leq p-m-2$, $s(\beta', p-r) = 0$ since $s(\gamma, p-r) = 0$. $s(\beta', p-r) = \Pi \beta_1' \beta_{p-r}' = 0$ gives us a contradiction. Therefore $p-r \geq p-m-1$ or $r \leq m+1$. q.e.d.

**Lemma 3:** Let $g(x) = b_{p-2} x^{p-2} + b_m x^m + \ldots + b_0$ where $b_i \in F$, $i = 0, \ldots, p-2$ and $b_m b_{p-2} \neq 0$ and $m \geq 1$. Then for primes $p$ where $x^p + 1/x + 1$ is irreducible over $F$, $g(x)$ can have at most $(m+1)$ zeros on $Z$. $(d \geq p - (m+1))$. 
Proof: Let \( \{ \beta_1, \ldots, \beta_r \}, \{ \beta_1^1, \ldots, \beta_{p-r}^1 \}, \{ \gamma_1, \ldots, \gamma_{p-2-r} \} \)
be as in Lemma 2.

For \( l \leq (p-2) - (m+1) \), we have

\[
\sum_{i+j=l} s(\beta, i) s(\beta^1, \gamma) = \sum_{i+j=l} s(\beta, i) s(\gamma, \gamma) = 0
\]

and for \( j \leq l \) it follows that \( s(\beta^1, j) = s(\gamma, j) \).

If \( p-r \leq p-m-2 \) or \( p-r-1 \leq p-m-3 \), \( s(\beta^1, p-r-1) = 0 \) since
\( s(\gamma, p-r-1) = 0 \) but \( s(\beta^1, p-r-1) \) is the sum of \( (p-r) \) things taken
\( (p-r-1) \) at a time.

\[
\binom{p-r}{p-r-1} = (p-r) \text{ elements of } \mathbb{Z}.
\]

If \( p-r \leq p-1 \), i.e., \( r > 1 \), this is impossible since \( x^p + 1/l + x \) is
irreducible so we get contradiction. So

\[
p-r \geq p-m-1
\]

\[
r \leq m + 1 \quad \text{q.e.d.}
\]

Theorem 1: For \( p \) a prime where \( 2 \) has multiplicative order \( p-1 \),
there exist \( \binom{p+1}{2}, p \) cyclic quaternary codes which correct at
least one error.

The desired codes shall be vectors of the form \( g_a(\beta^i) \) where
\( g_a(x) \) is parametrized by a pair of constants \( (c_0, c) \) \( (c_0 \in K, c \in GF(2^{p-1})) \), \( \beta \) a primitive \( p \)th root of unity. The choice of the \( g \)
will depend upon the particular \( p \) and will exhibit the error correcting
properties immediately. The \( g \)'s chosen will be either of the type
in Lemma 2 or Lemma 3. The lower bound \( d_0 \) obtained will depend
clearly on the integer \( m \) since for both Lemmas 2 and 3 \( d \geq p-(m+1) \).
For particular \( p \), we would like a general algorithm for the value of
\( m \). It is in the nature of these particular \( p \), that we may use the
theory of quadratic residues to make simple decisions as to which set
of \( g \) to choose and what value of \( m \) occurs. We therefore make a necessary aside and include the appropriate data.

We introduce the Legendre symbol \( \left( \frac{a}{p} \right) \) for \( a \equiv 0 \). If \( x^2 \equiv a \) modulo \( p \) has solutions in the field of \( p \) elements, \( GF(p) \), we say that \( a \) is a quadratic residue of \( p \). Symbolically \( \left( \frac{a}{p} \right) = +1 \). If \( a \) is not a quadratic residue of \( p \) we write \( \left( \frac{a}{p} \right) = -1 \).

For primes \( p \) where 2 has multiplicative order \( p-1 \), i.e., 2 is a primitive generator of the multiplicative group of \( GF(p) \), the statement that \( a \in GF(p) \) is a power of 4 modulo \( p \) translates equivalently into \( \left( \frac{a}{p} \right) = +1 \) and vice versa. For \( \left( \frac{a}{p} \right) = 1 \) means \( x^2 \equiv a \) modulo \( p \) has solutions \( x_0 \) and \( p-x_0 \in GF(p) \). But \( x_0 = 2^l \) for some integer \( l \), since 2 is primitive. Therefore \( (2^l)^2 = (2^l l) = 4^l = a \) modulo \( p \) -- i.e., \( a \) is a power of 4. Note that 2 primitive implies \( \left( \frac{2}{p} \right) = -1 \) since \( \left( \frac{2}{p} \right) = 1 \Rightarrow 2 = 4^s = 2^{2s} \) or \( 2^{2s-1} = 1 \). \( 2s-1 \) odd divides \( p-1 \) and 2 not primitive. We also need** and use
\[
\left( \frac{a}{p} \right) \left( \frac{b}{p} \right) = \left( \frac{ab}{p} \right)
\]
for \( a \) and \( b \) prime to \( p \).

**Theorem 1**: For \( p \) a prime where 2 has multiplicative order \( p-1 \), there exist (\( \frac{p+1}{2} \), \( p \)) cyclic quaternary codes

- a, a') if \( \left( \frac{3}{p} \right) = -1 \),
  \( d \geq 3 \)
- b, b') if \( \left( \frac{3}{p} \right) = +1 \),
  \( d \geq 4 \)
- c) if \( \left( \frac{3}{p} \right) = +1 \) and \( \left( \frac{5}{p} \right) = +1 \)
  \( d \geq 5 \)

**Proof:**

\( a) \left( \frac{3}{p} \right) = -1 \)
\( p = 8n + 3 \)

Here \( \left( \frac{-1}{p} \right) = -1 \). So by the multiplication formula \( \left( \frac{-3}{p} \right) = 1 \)
\( \left( \frac{-4}{p} \right) = -1 \), \( \left( \frac{-2}{p} \right) = +1 \)

*See Appendix for properties of \( \left( \frac{a}{p} \right) \).

**Formula 1 in Appendix.
The polynomial \( g_a(x) = c_0 + c x^2 + c^4 x^4 + c^4 x^{2.4} + \ldots \) has highest degree \((p-1)\) and next highest power \(m = p-4\). Lemma 2 gives us that \( d \geq p - (p-4+1) = 3 \).

a') \( p = 8n + 5 \)

Here \( \left( \frac{-1}{p} \right) = 1 \) so \( \left( \frac{+3}{p} \right) = -1, \left( \frac{-2}{p} \right) = -1, \left( \frac{-4}{p} \right) = 1 \). Choose \( g_a(x) = c_0 + c x + c^4 x^4 + \ldots \). This polynomial again satisfies Lemma 2.

b) \( \left( \frac{3}{p} \right) = 1 \)

Case 1) \( p = 8n + 3 \), \( \left( \frac{-1}{p} \right) = -1, \left( \frac{-3}{p} \right) = -1, \left( \frac{-2}{p} \right) = +1, \left( \frac{-4}{p} \right) = -1 \)

Choose \( h_a(x) = c_0 + c x + c^4 x^4 + \ldots \).

Highest degree have is \((p-2)\) and next highest is at most \((p-5)\). So Lemma 3 yields \( d \geq 4 \).

b') \( p = 8n + 5 \) \( \left( \frac{-1}{p} \right) = 1, \left( \frac{-2}{p} \right) = -1, \left( \frac{-3}{p} \right) = 1, \left( \frac{-4}{p} \right) = 1, \left( \frac{-5}{p} \right) = ? \)

Choose \( h_a(x) = c_0 + c x^2 + c^4 x^{2.4} + \ldots \).

Lemma 3 again applies and \( d \geq 4 \).

c) If \( \left( \frac{5}{p} \right) = +1 \), Lemma 3 yields \( d \geq 5 \).

We note here that \( \left( \frac{6}{p} \right) = -1 \) for case b since we have \( \left( \frac{2}{p} \right) = -1 \).

We note that we need a detailed version of lemmas 2 and 3 plus new values of \( \left( \frac{3}{p} \right) \) to get sharper estimates on the bound.

V. Encoding

Corresponding to the desired \( g_a(x) \) or \( h_a(x) \) we choose the polynomial \( f(x) \) over \( k \) whose roots are the appropriate powers of \( \beta \) -- \( \beta \) a primitive \( p^{th} \) root of unity. The powers chosen are of course the exponents of \( x \) in \( g_a(x) \) or \( h_a(x) \). We then generate the codes by
associating the appropriate difference equation with \( f(x) \) subject to \( (\frac{p+1}{2}) \) initial conditions in \( K \).

VI. Examples

Ex. 1  \( p = 5 \)

Here we have a single error correcting (3-5) cyclic quaternary code. This (3, 5) code is also obtained by Golay in a different manner.

Here \( p \equiv 5 \) (modulo 8) and \( \left( \frac{3}{5} \right) = -1 \), so we choose, as in case a', \( g_a(x) = c_0 + cx + c_4 x^4, c_o \in K, c \in L = GF(2^4) \). Choose \( \gamma \) a generator of the multiplicative group \( L^* \) of \( L \) -- i.e., \( \gamma^{15} = 1 \) -- say \( \gamma \) satisfies \( \gamma^4 + \gamma + 1 = 0 \). Let \( \beta = \gamma^3 \) then \( \beta \) is a primitive 5th root of unity. Let \( f(x) = (x + 1)(x + \beta)(x + \beta^4) \) \( = (x + 1)(x^2 + (\beta + \beta^4)x + \beta^5) = (x + 1)(x^2 + (\beta + \beta^4)x + 1) \). Now \( \beta + \beta^4 \in K, \beta + \beta^4 = \gamma^{10} \) say and \( \gamma^{10} + \gamma^5 + 1 = 0 \). So \( f(x) = x^3 + \gamma^5 x^2 + \gamma^5 x + 1 \)

Consider the associated difference equation

\[
y_{n+3} + \gamma^5 y_{n+2} + \gamma^5 y_{n+1} + y_n = 0
\]

Any three initial values in \( K \) will generate sequences of period 5. This (3, 5) code will correct one error by the general theorem. It is optimum as a computation will verify that it is closely packed.

Ex. 2 The (6-11) c.q. code:

1. Since \( \left( \frac{3}{11} \right) = -1 \), we are in case b.

\[
h_a(x) = c_0 + cx + c_4 x^4 + c_4^2 x^5 + c_4^3 x^9 + c_4^4 x^{13}
\]

Here \( m = 5 \), so by Lemma 3, the number of roots of \( h(x) \) in \( Z \) is at most 6, so \( d \geq 11 - 6 = 5 \).

Putting it in terms of quadratic residues

\[
\left( \frac{3}{11} \right) = -1, \left( \frac{4}{11} \right) = -1, \left( \frac{5}{11} \right) = \left( \frac{6}{11} \right) = -1
\]
Generalization: Let $K = GF(p^m)$ be the Galois field of $p^m$ elements. Consider the group codes of $V_n(K)$ where $p$ and $n$ are relatively prime for $(p, n) = 1$. Each $(k, n)$ group code $A$ corresponds to a set of polynomials indexed by a set of constants $(c_0, c_1, c_{1^2}, \ldots, c_{1^{r-1}})$ where $r$ is the number of irreducible factors over $K$ of $(x^n + 1)/(1 + x)$; $c_0 \in K$ and $c_i \in L$, the smallest field over $K$ containing the $n$th roots of unity.* To any group code $A$ is assigned a subgroup $G$ of the direct product of $K$ with $r$ copies of $L$.

If $m = 2$, then $r(n) \geq 2$ for any $p$ and we have a set of non-trivial cyclic codes obtainable by setting some of the $c_i = 0$. This is also the case if $m (n - 1)$. Error correcting bounds are formulated then in number-theoretic terms analogous to the $2^2$ case. If $m$ and $n-1$ are relatively prime, we obtain the cyclic codes corresponding to the $p$ letter case and the general lower bound is the Zierler-Gorenstein one. Improvement on the bound may come from examination of the coefficients of the polynomials themselves.

For $n$ and $p^m$ for which $r(n) = 1$, we may use the procedure outlined in 3), and obtain pseudo-cyclic variations.

*As before, we choose $\beta$ a primitive $n^{th}$ root of unity. Then to each code word $c \in A$ we associate the polynomial $g(x, \beta, c_0, c_{1^0}, \ldots, c_{1^{r-1}})$ such that $g(\beta^i) = a_i$. 
Algebraic Appendix*

1. The Legendre symbol \(\left(\frac{a}{p}\right)\)

Def.: If \(p\) is a prime, we say that \(a \neq 0\) is a quadratic residue of \(p\) (symbolically \(\left(\frac{a}{p}\right) = +1\)) if the equation \(x^2 = a \mod p\) has solutions in the field of \(p\) elements. Clearly since \(x_0^2 = (p-x_0)^2\) there are \(\frac{p-1}{2}\) quadratic residues of \(p\). We put \(\left(\frac{a}{p}\right) = -1\) if \(a\) is not a quadratic residue.

The following properties of the Legendre symbol are well known.

1. \(\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)\) for \(a\) and \(b\) prime to \(p\)

2. \(\left(\frac{2}{p}\right) = 1\) if \(p \equiv \pm 1 \mod 8\)

\(\left(\frac{2}{p}\right) = -1\) if \(p \equiv \pm 3 \mod 8\)

3. \(\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}\)

4. Law of Quadratic Reciprocity

\(\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)\) if \(p\) and \(q\) are both of the from \(4k - 1\)

\(\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)\) all other cases.

*Le Veque, Topics in Number Theory, Vol. 1, Chapter 5, Addison-Wesley (1956).
Bibliography:


