LOW WEIGHTS IN QUADRATIC-RESIDUE CODES*

by

E.F. Assmus Jr, H.F. Mattson Jr, R. Turyn

University of North Carolina

Institute of Statistics Memeo Series No. 484.3

August 1966

This research was supported by the Air Force Office of Scientific Research Contract No. AF-AFOSR-760-65 and also partially supported by Contract No. AF19(604)-8516.

DEPARTMENT OF STATISTICS

UNIVERSITY OF NORTH CAROLINA

Chapel Hill, N. C.

* Work done with the cooperation of Prof. J. B. Muskat of the University of Pittsburgh with support of NSF grants G.P. 2091 and G.P. 2310.

This is a slightly revised version of the talk presented at the NATO summer school in coding in August 1965. The revisions consist of minor corrections and the new results for e = 24 recently found by Prof. Muskat.

INTRODUCTION

In order to realize Shannon's theorem on the attainability of channel capacity, it is necessary to construct codes of longer and longer block length with fixed information rate and good error-correcting properties. As yet there is no constructive method for obtaining such a sequence of codes. In fact, no one has as yet constructed a sequence of codes of longer and longer block lengths with information rate (k/n) and correction rate (d/n) bounded away from zero. For various reasons there has been hope of finding such a sequence from among the cyclic codes, in particular from among the quadratic-residue codes, whose groups of symmetries are known to be large.

The problem of finding the minimum distance for the quadratic-residue codes appears extremely difficult. So far there have been (to our knowledge) only fragmentary nontrivial results. The (23, 12) code of Golay over GF(2), is, of course, well-known to have minimum distance d = 7. Gleason has shown that d = 11 for the (47,24) code over GF(2). Mattson and Prange have shown the (41,21) code over GF(2) to have d = 9 and Pless and Prange have shown the (71,36) code over GF(2) to have d = 11.

We have recently shown that the (19,10) code over GF(4) has d = 7 and that the (23,12) code over GF(3) has d = 8.*

Our purpose here is to describe a method of finding vectors of low weights in quadratic-residue codes. Thus, the following results are by nature discouraging. The method, however, will <u>not</u> find low-weight vectors

* The (31,16) code over GF(2) has d=7; the (17,9) code over GF(2) has d=5; the (11,6) code and (13,7) code, both over GF(4), have d=5. These are the only nontrivial determinations of d we are aware of.

for those quadratic-residue codes of block length congruent to -1 modulo 4.

Instead of giving proofs for our results, we have tried to define and describe them in such a way that people not familiar with the number theory used may nevertheless have some understanding of what we have done.

A quadratic-residue code is defined as a cyclic code of prime block length ℓ over the field GF(q) with generator polynomial of the form $g(x) = \prod_{r \in R} (x - \zeta^r)$ or $(x-1)g(x)$, where R is the set of quadratic residues modulo ℓ, and ζ is a primitive ℓ^{th} root of 1 over GF(q). The dimension of such a code is $(\ell \pm 1)/2$, and there are two such codes of each of these dimensions provided only that q is a quadratic-residue modulo ℓ. The two codes of each dimension are equivalent to each other under the permutation $i \leftarrow ti$, $i = 0, 1, \ldots, \ell-1$, of coordinates mod ℓ, where t is any fixed element of R', the set of quadratic nonresidues. We denote the $(\ell, (\ell-1)/2)$ codes by A and B and the $(\ell, (\ell+1)/2)$ codes by A^+ and B^+, where we take $A^+ \supset A$ and $B^+ \supset B$.

It is necessary to consider only the cases $q = p$, and $q = p^2$ when p is in R', since quadratic-residue codes over $GF(p^n)$ are obtained from those over GF(p), or $GF(p^2)$, merely by taking tensor products (extending the coefficient field); and we know this process does not change the minimum weight.

If d and d_1 are the minimum distances in A^+ and A, respectively, then results of Gleason and Prange show that $d_1 = 1 + d$. Thus in particular the minimum weight in A^+ is not achieved by a vector in A.

The square-root bound on d is derived as follows. A polynomial $h_1(x)$ of weight d in A^+ multiplied by one $h_2(x)$ of the same weight in B^+ must give a constant multiple of $x^{\ell-1} + \ldots + 1$. When $\ell \equiv -1 \pmod 4$, we may take $h_2(x) = h_1(x^{-1})$, and then it is immediate that $d(d-1) \geq \ell-1$. When $\ell \equiv +1$

(mod 4), we conclude $d^2 > \ell$.

To our knowledge the square-root bound is the best lower bound on d for quadratic-residue codes. There is some hope that it may not be a very good lower bound, and that among these codes one could find an infinite sequence of values of ℓ such that for some fixed p the associated codes A had d/ℓ bounded away from 0.

This paper reports on an attempt to find out more about the minimum weight in quadratic-residue codes. The results are somewhat discouraging, because in some cases d/ℓ was found to be lower than expected. Previously d/ℓ was known to be as small as about 1/10 in some cases; this study finds that it can be as low as about 1/24.

BACKGROUND

We now introduce some elements of algebraic number theory in order to explain our method. Let Q denote the field of rational numbers and let z denote a primitive ℓ^{th} root of 1, where ℓ is an odd prime number as before. One may think of z as $\exp(2\pi i/\ell)$; $z^\ell = 1$ and no lower power of z is 1. Let K denote the field Q(z); K consists of all "numbers" of the form $a_o + a_1 z + \ldots + a_{\ell-2} z^{\ell-2}$ where $a_o, \ldots, a_{\ell-2}$ are in Q. K is the smallest field containing Q and z, and $z^{\ell-1} + z^{\ell-2} + \ldots + 1 = 0$. Therefore any ℓ-1 distinct powers of z form a basis of K as a vector space over Q.*

Any ℓ-1 distinct powers of z form an integral basis of K/Q.

For the rest of this paper, let p be a rational prime, $p \neq \ell$, such that p is in R. Then the $(\ell, (\ell+1)/2)$ quadratic-residue codes over GF(p) will be

---

* At this point the reader unfamiliar with number theory may wish to read the Appendix.

denoted by A_p^+ and B_p^+. The order h of p under multiplication modulo ℓ must divide $(\ell-1)/2$, so that g in $hg = \ell-1$ is even. The polynomial $x^{\ell-1} + x^{\ell-2} + \ldots + 1$ splits over GF(p) into the product of g distinct irreducible factors $\phi_0(x), \ldots, \phi_{g-1}(x)$ each of degree h.

The prime p splits in K into the product of g distinct prime ideals $p_0, \ldots, p_{g-1}$, which can be labelled in such a way that (Z denoting the rational integers)

LEMMA. For any j, an integer $a = \sum_0^{\ell-1} a_i z^i$ of K, $a_i \in Z$, is divisible by p_j if and only if the polynomial $\sum_0^{\ell-1} a_i' x^i$ is divisible by $\phi_j(x)$ over GF(p), where a_i' denotes the residue-class of a_i modulo p.

The Galois group G of K/Q is cyclic of degree $\ell-1$. If σ denotes a generator of G, it is convenient to label the p_i and $\phi_i(x)$ for any p as follows: Choose p_0 arbitrarily and let $\phi_0(x)$ be its corresponding polynomial. Then define $p_i = \sigma^i(p_0)$ and call $\phi_i(x)$ the polynomial with $\zeta^{\sigma-i}$ as a root, where ζ is a root of $\phi_0(x)$. Then p_i and $\phi_i(x)$ correspond under the Lemma. Under this labelling and correspondence, the generator polynomials of the quadratic-residue codes A_p^+ and B_p^+ over GF(p) correspond to $\pi = p_0 p_2 \ldots p_{g-2}$ and $\pi' = p_1 p_3 \ldots p_{g-1}$. The ideals π and π' are the prime ideals into which (p) splits in the quadratic field L contained in K (and this notation will be used throughout). L is the fixed field of σ^2. It is generated by $\eta = \sum z^r (r \in R)$ or by $\eta' = \sum z^t (t \in R')$. The irreducible polynomial of η and η' over Q is $x^2 + x + (1 \pm \ell)/4$, the sign being chosen so that the constant term is in Z.

Thus L is $Q(\sqrt{\pm\ell})$, where this sign is the same as that in the congruence $\ell \equiv \pm 1 \pmod 4$.

What we have observed is that when $(p) = \pi\pi'$ in L, the polynomial $\sum_0^{\ell-1} a_i' x^i$ over GF(p) is in A_p^+ or B_p^+ if and only if the integer $\sum_0^{\ell-1} a_i z^i$ of K is divisible by π or π', where a_i' is the residue-class of a_i modulo p.

It is not easy in general to tell whether an integer of K is divisible by π or π', but in the special case where the integer is a so-called cyclotomic period it is a feasible computation.

We shall use the following criterion.

PROPOSITION 1. Let θ be an integer of the field E lying between L and K, and let T denote the trace from E to L. Suppose that p is prime to the gcd $(T\theta\ ,\ \sigma T\theta\ )$. Then θ is divisible by π or π' if and only if $\theta \cdot \sigma^i(\theta)$ is divisible by p for each odd i.

The usefulness of this criterion is that in some cases, including that in which θ is a cyclotomic period, it is easy to express $\theta\ \sigma^i(\theta)$ in the form $\sum_1^{\ell-1} a_i z^i$; and this is divisible by p if and only if p divides each a_i.

(When $\theta = \sum_0^{\ell-1} a_i z^i$, the condition is that $a_o \equiv a_1 \equiv \ldots \equiv a_{\ell-1} \pmod p$.)

CYCLOTOMIC PERIODS

Let $\ell-1 = ef$. Then the Galois group G has a unique subgroup H of order f. By means of the action of G on the powers of z we identify G with the cyclic group of non-0 residues modulo ℓ under multiplication. H is then the subgroup of e^{th} powers of G. We may decompose G into a union of cosets H_i modulo H as $G = H_o \cup H_1 \cup \ldots \cup H_{e-1}$ and we then define the cyclotomic

periods for e as

$$\eta_i = \sum_{s \in H_i} z^s \qquad i = 0, 1, \ldots, e-1,$$

where we choose the labelling so that $\eta_0 = \sum z^s (s \in H)$ and $\eta_i = \sigma^i(\eta_0)$.

The cyclotomic periods for e are an integral basis for the field E over Q, where $E = Q(\eta_0)$ is the fixed field of H. Therefore for each $i = 0, 1, \ldots,$ e-1 there exist rational integers denoted by $(i,0), (i,1), \ldots, (i,e-1)$ such that

$$\eta_0 \eta_i = \sum_{j=0}^{e-1} (i,j)\eta_j + \epsilon_i f \tag{1}$$

where $\epsilon_i = 1$ when f is even and $i = 0$, or when f is odd and $i = e/2$; otherwise $\epsilon_i = 0$. (In other words, $\epsilon_i = 1$ if and only if -1 is in H_i.)

It follows that

$$\sum_{j=0}^{e-1} (i,j) + \epsilon_i = f \qquad \text{for all } i. \tag{2}$$

These non-negative rational integers (i,j) are called the cyclotomic numbers of order e. If w is the primitive element modulo ℓ corresponding to σ, then (i,j) is the number of solutions (x,y) with $0 \leq x, y < f$ of

$$w^{ex+i} + 1 \equiv w^{ey+j} \pmod{\ell}.$$

It is from this relation that Prof. Muskat has calculated the (i,j) for various e and ℓ.

The cyclotomic numbers satisfy

$$(i,j) = (-i,j-i) \text{ and } (i,j) = \begin{cases} (j,i) & f \text{ even} \\ (j+e/2,\ i+e/2) & f \text{ odd,} \end{cases}$$

where the entries are read modulo e.

AN APPLICATION TO QUADRATIC-RESIDUE CODES

From what we have seen, every time that η_0 is divisible by π or π', there is a vector of weight $f = (\ell-1)/e$ in A^+. Let us call $\eta_0(x)$ the polynomial $\sum x^s (s \in H)$. We shall now apply the foregoing to the integer $\theta = \eta_0$.

To see that the criterion of Proposition 1 holds, we note that $T\eta_0 = \eta$ and $\sigma T\eta_0 = \eta'$; $\eta + \eta' = -1$. Therefore η_0 is divisible by π or π' if and only if $\eta_0\eta_i$ is divisible by p for each odd i. The choice of the generator σ determines the labelling of $\eta_1, \ldots, \eta_{e-1}$, and the cyclotomic numbers change as σ changes; but whether π or π' divides η_0 is independent of the choice of generator, hence so is our criterion expressed in terms of cyclotomic numbers. In terms of the cyclotomic numbers this condition is that for each odd i we must have, from (1),

$$(i,0) \equiv (i,1) \equiv \ldots \equiv (i,e-1) \equiv \epsilon_i f \pmod{p}. \tag{3}$$

Some necessary conditions are:

PROPOSITION 2. If $\eta_0(x)$ is in A_p^+ or B_p^+ for some p, then e is even and p divides $(\ell \pm 1)/4$, the sign chosen to make this a rational integer. And if $e > 2$, then p divides f, which implies that $\eta_0(x)$ is in A_p or B_p.

Thus in searching for code-vectors by this means we restrict ourselves to the case when e is even. And furthermore, we have

COROLLARY. Let $\ell \equiv 1 \pmod 4$, and let $\ell - 1 = ef$ with $e > 2$. Then the cyclotomic period η_o of order e never satisfies $\eta_o(x) \in A_p^+$ or B_p^+ for any p.

In view of this we restrict ourselves to the case $\ell \equiv 1 \pmod 4$ and e even, $e > 2$. In this case $\epsilon_i = 0$ for all odd i, so that (3) becomes

> Let $\ell - 1 = ef \equiv 0 \pmod 4$, e even, $e > 2$.
> Then p divides (i,j) for all j and all odd i*
> if and only if $\eta_o(x)$ is in A_p^+ or B_p^+, where η_o is
> a cyclotomic period of order e.

The following result is a helpful sieve when one is searching for such code-vectors.

PROPOSITION 3. Let $\ell - 1 = 2ef$ with e even. Then the cyclotomic period η_o for 2e cannot yield a code-vector $\eta_o(x)$ in A_p^+ or B_p^+ for a given p unless a cyclotomic period of order e does so (for the same p).

There exist formulas for the (i,j) for certain values of e. For example, for $e = 4$ and f even, Gauss proved that $16(1,0) = \ell - 1 + 2(x-1) + 8y$, where $\ell = x^2 + 4y^2$ with $x \equiv 1 \pmod 4$. There are similar but more complicated formulas of more recent date for some other e up to $e = 20$. But for our purposes, which are to find examples of quadratic-residue codes having vectors of rather low weight, it is more appropriate to search through tables of values of the (i,j) for instances of (4) than to establish general conditions with the formulas and then compute solutions of ℓ = (some quadratic form).

* This condition implies that p is a quadratic residue modulo ℓ, since $p \mid f$.

For purposes not related to coding, Prof. Muskat has calculated the cyclotomic numbers for all primes less than 50,000 for various values of e up to e = 20. He very kindly gave us tables of these values, from which we found several instances ($10 \leq e \leq 20$) where $\eta_o(x)$ was in A_p^+ or B_p^+. Some examples of these findings are:

e=10,		e=12				e=14,		e=16		e=20,	e=24,	
f even		f even		f odd		f even		f even		f odd	f even	
ℓ	p	ℓ	p	ℓ	p	ℓ	p	ℓ	p		ℓ	p
761	2	2,521	2	8,221	5	1,289	2	4,801	2	ℓ = 8821,	9,601	2
1,361	2	8,089	2	18,541	3	6,301	3	15,937	3	p = 3, is the	18,433	2
1,381	3	47,521	3	22,621	5	49,057	2	47,713	2	only instance.	48,817	2
6,841	2,3	49,681	2	25,261	5							
8,821	3			44,269	7							
21,401	5											
30,941	7											
49,921	2											
N = 94		N = 81		N = 11		N = 27		N = 13		N = 1	N = 7	

N is the number of primes less than 50,000 in the table in question giving an instance where $\eta_o(x)$ is in A_p or B_p. The values of N for e = 10, 12, 14, and 24 were found on his computer by Prof. Muskat. We obtained the values for e = 16 and e = 20 by our own visual search of his tables (the same for e = 14, where our result agreed with his). The smallest and largest values of ℓ for each value of e are given, as well as an example for each value of p that arose.

When f is even, a large majority of the instances occur for p = 2; when f is odd, occurrences are rarer.

We also calculated several cases by hand for smaller values of e, using general formulas; in the same way we verified the entries in Prof. Muskat's tables for three values of ℓ, namely, ℓ = 3,821, e = 10; and for e = 12, ℓ = 1321 and 1657.

SUMMARY

To repeat: each instance we found yields a vector of weight $(\ell-1)/e$ in A_p or B_p. In each case these weights are far greater than $\sqrt{\ell}$, but there is no reason to suppose that the weights $(\ell-1)/e$ are the minimum weights in the A_p.

The lowest weight-to-block length ratio found, namely 1/20* (approximate), is lower, by a factor of about 1/2, than the lowest such ratio we knew of before this investigation.

The fact that this approach cannot yield low weights in A_p^+ when $\ell=4n-1$, plus similar resutls below, holds out a faint glimmer of hope for a sequence of A_p^+ with non-vanishing error-correcting rate in this class of codes.

Perhaps a word on the role of computation in this method is called for. One could get our results directly by first factoring $x^{\ell-1} + \ldots + 1$ over GF(p) into its two "quadratic-residue" factors $\gamma_1(x)$ and $\gamma_2(x)$,(*) and then computing whether $\gamma_i(x)$ divides $\sum x^s$, where the sum is over $s \in H$, and where it would usually be necessary to compute this for both i = 1 and i = 2. By the previous analysis one could restrict oneself to those p dividing f. Although we have not made careful estimates, it appears that perhaps the amount of "direct" computation required for a given ℓ and e ($ef = \ell-1$) to determine whether $\sum x^s$ ($s \in H$) is in A_p^+ or B_p^+ for all p dividing f might be about the same as that required to calculate the cyclotomic numbers of order e for ℓ. Perhaps the latter calculation would be significantly easier. In any case, the fact that the cyclotomic numbers have been studied since the time of Gauss, and the fact that those used by us were calculated by Prof. Muskat for a purpose entirely different, lead us to regard this approach as

(*) Now 1/24, as of early 1966.

less computational than the direct approach.

CODE-VECTORS FROM OTHER INTEGERS

We may consider by this approach any integer $\theta = c + \sum_{o}^{e-1} c_k \eta_k$, c, $c_k \in Z$, of the field E lying between K and L, of even degree e over Q.

A sufficient condition for the criterion of Proposition 1 to obtain is that p should not divide the gcd$(ce - \sum c_k, \sum c_{2i} - \sum c_{2i+1})$.

We define $\theta(x)$ in analogy with the previous definitions, and if Proposition 1 holds for θ, then $\theta(x)$ is in A_p^+ or B_p^+ if and only if for each odd i we have

$$c(c_j + c_{j-i}) + \sum_{k,m} c_k c_m (i+k-m,\ j-m) \equiv c^2 + f \sum_{k,m} \epsilon_{i+k-m} c_k c_m \pmod{p}, \tag{5}$$

$$j = 0, 1, \ldots, e-1.$$

A necessary condition for (5) to hold is

$$2c \sum c_k + f\left(\sum c_k\right)^2 \equiv c^2 e + \ell \sum_{k,m} \epsilon_{i+k-m} c_k c_m \pmod{p}.$$

This is obtained on adding (5) over j. In particular this implies that $\sum_{k,m} \epsilon_{i+k-m} c_k c_m$ is constant modulo p for odd i; therefore if only one c_k is non-0, and if $\ell \equiv -1 \pmod 4$, this condition cannot hold for even $e > 2$.

Another necessary condition is obtained on multiplying $T\theta$ and $\sigma T\theta$: Let E denote $\sum c_{2i}$ and I denote $\sum c_{2i+1}$; then $\theta(x)$ is in A_p^+ or B_p^+ implies

$$(ce/2)^2 + E(1 - \frac{1\pm\ell}{2}) - (ce/2)\sum c_k + (E^2 + I^2)\frac{1\pm\ell}{4} \equiv 0 \pmod{p}$$

where the $\pm$ signs are the same and are chosen to make $(1\pm\ell)/4$ in Z.

Obviously the condition (5) is more complicated when θ is a sum of more than one cyclotomic period. We have not searched very hard for code-vectors of this type, but we did find some instances where $\theta(x)$ was in A_2^+ or B_2^+ for $e = 14$, f even, and $e = 16$, f even, for $\theta = 1 + \eta_0$. There were none for $\theta = 1 + \eta_0$ for $e = 20$, f odd, however.

One is less interested in these more complicated θ's because they would give vectors of higher weights in the codes; on the other hand, it might be possible to use these θ's to find vectors of weight very near the minimum weight if one tried several sums for large values of e. For example, when $\ell = 29$ we could take $e = 14$ and look for code-vectors $\theta(x)$ arising from $\theta = c + c_0\eta_0 + \ldots + c_3\eta_3$ over $p = 5$ (or we could take θ as a sum of some other four periods). This would give weight 8 or 9 depending on whether $c = 0$ or not. (The minimum weight is at least 6 and is probably 8 or 9.)

As a further example, $\eta_0(x)$ (of weight 6) is in A_3 for $\ell = 13$; this code has minimum weight at least 5 and probably 6.

We plan to pursue this question in the future.

APPENDIX

In the rational integers Z every non-0 element is uniquely expressible as a product of prime numbers, apart from the ordering of the factors. This property holds more generally in fields of algebraic numbers such as the field $K = Q(z)$ considered here. One can define a subring $\mathcal{O}$ of K called the integers of K, but in general one needs to introduce <u>ideals</u> in order to get

unique factorization. The integral ideals are subrings of $\mathcal{O}$ which are closed under multiplication by elements from $\mathcal{O}$. One multiplies ideals $\underline{a}$ and $\underline{b}$ by taking the set of all sums of the products ab, with $a \in \underline{a}$ and $b \in \underline{b}$. The resulting set $\underline{a} \cdot \underline{b}$ is also an ideal. The sum $\underline{a} + \underline{b}$ is defined as the set of all $a + b$ with $a \in \underline{a}$ and $b \in \underline{b}$. Under these definitions the ideals form a ring containing an identity element $\mathcal{O}$. Certain of these ideals are called prime ideals, and they have the property that every ideal can be expressed uniquely as a product of prime ideals.

For the fields $K \supset L \supset Q$ with rings of integers $\mathcal{O} \supset \mathcal{O}_L \supset Z$, we know that the ideal in L of the rational prime p, namely the set $p \cdot \mathcal{O}_L$, is either itself a prime ideal of $\mathcal{O}_L$ (when p is a quadratic nonresidue modulo ℓ) or is the product of two different prime ideals π and π' of $\mathcal{O}_L$ (when p is a quadratic-residue mod ℓ). It is the latter case that we assume here. In this case the ideals $\pi \cdot \mathcal{O}$ and $\pi' \cdot \mathcal{O}$ consist of the product $p_0 p_2 \cdots p_{g-2}$ and $p_1 p_3 \cdots p_{g-1}$ of the prime ideals p_i defined in the text, and each p_i corresponds to a different irreducible factor $\phi_i(x)$ of $x^{\ell-1} + \ldots + 1$ over GF(p).

We say that an integer of K is divisible by a given ideal if it is an element of that ideal. The point of our method is that, for an integer $\theta = \sum_0^{\ell-1} a_i z^i$ of K, $a_i \in Z$, the associated polynomial $\theta(x) = \sum_0^{\ell-1} a_i' x^i$ over GF(p) is divisible by $\phi_0(x)\, \phi_2(x) \cdots \phi_{g-2}(x) = \Pi(x-\zeta^r)$, $r \in R$, or by $\phi_1(x)\, \phi_3(x) \cdots \phi_{g-1}(x) = \Pi(x-\zeta^t)$, $t \in R'$, if and only if the integer θ of K is divisible by $p_0 p_2 \cdots p_{g-2} = \pi\mathcal{O}$ or by $p_1 p_3 \cdots p_{g-1} = \pi'\mathcal{O}$. ($a_i'$ is the residue-class of a_i mod p.)

Thus we are able to use information about integers of K contained in the cyclotomic numbers to give us some information on the quadratic-residue codes.

For further explanation of the points sketched in this appendix, the reader is referred to any book on algebraic number theory, such as, for example, E. Hecke, Algebraische Zahlen, (Chelsea, New York, 1948), H. Weyl, Algebraic Theory of Numbers (Princeton, 1940), or H. B. Mann, Introduction to Algebraic Number Theory (Ohio State, 1955).

A reference on cyclotomic numbers is L. E. Dickson's "Cyclotomy, Higher Congruences, and Waring's Problem," Am. J. Math.; vol. 57, pp. 391-424; 1935.