

On the Weight Enumerators of Quadratic Residue Codes

J. Mykkeltveit¹, C. Lam², and R. McEliece
Communications Systems Research Section

Binary quadratic residue codes, some of which are currently being studied for use in the Mariner Jupiter-Saturn 1977 mission, are among the most powerful known block codes. They are, however, notoriously difficult to analyze. In this paper a method is developed for obtaining information about the weights of these codes by exploiting the fact that they are left invariant by the linear fractional group.

I. Introduction

Binary quadratic residue codes are codes with rate $1/2$ and exist for all block lengths of the form $n = p + 1$, where p is a prime congruent to $\pm 1 \pmod{8}$. For example the $(8, 4)$ extended Hamming code and the $(24, 12)$ Golay code currently being studied for use in the Mariner Jupiter-Saturn 1977 mission are quadratic residue codes. These codes are very powerful, but are quite hard to decode. Practical decoding algorithms can be invented for them only after their fine structure is fully understood. In par-

ticular it is very important to have techniques for calculating the weight enumerator

$$A(Z) = \sum_{i=0}^n A_i Z^i$$

of the codes, A_i denoting the number of words of weight i in the code. The enumerator $A(Z)$ provides valuable information about the performance of the code (Ref. 1, pp. 397-400).

In this article, we develop a technique which yields valuable new information about the weight enumerators of quadratic residue codes. Our method relies heavily on the fact that every quadratic residue code is left invariant by a very large permutation group.

¹Postdoctoral Research Fellow in mathematics, California Institute of Technology.

²Graduate student in mathematics, California Institute of Technology.

II. Preliminaries

Let p be a prime congruent to $+1$ or $-1 \pmod{8}$, and let R_0 denote the set of nonzero quadratic residues \pmod{p} . Let α be a primitive p th root of unity in an extension field of $GF(2)$, and let the polynomial $h(x)$ be defined by

$$h(x) = \prod_{r \in R_0} (x - \alpha^r)$$

Then $h(x)$ is a polynomial with coefficients in $GF(2)$. The binary cyclic code of length p with check polynomial $h(x)$ is called the *expurgated quadratic residue code* (EQR code), and the code with check polynomial $(x+1)h(x)$ is called the *augmented quadratic residue code* (AQR code). The *extended quadratic residue code* (LQR code) is defined to be the set of binary n -vectors of the form $(C_0, C_1, \dots, C_{p-1}, C_\infty)$, where $(C_0, C_1, \dots, C_{p-1})$ is a codeword in the AQR code, and $C_0 + C_1 + \dots + C_{p-1} + C_\infty = 0$.

Berlekamp (Ref. 1, Theorem 15.26) proves the following theorem about LQR codes.

THEOREM: Every LQR code is invariant under the doubly transitive linear fractional group $LF(2, p)$,

$$C_u \longrightarrow C_{(au+b)/(cu+d)}$$

where $u \in GF(p) \cup \{\infty\}$; $a, b, c, d \in GF(p)$; $ad - bc = 1$. The group $G = LF(2, p)$ has order $p(p^2 - 1)/2$.

Let

$$A(Z) = \sum_{i=0}^{p+1} A_i Z^i$$

be the weight enumerator of the LQR code of length $p+1$; i.e., A_i is the number of words of weight i in the code. It is the object of this paper to show that it is possible to compute $A(Z) \pmod{p(p^2 - 1)/2}$ for many values of p which are so large that it is not possible to compute $A(Z)$ itself.

In order to compute $A(Z) \pmod{|G|}$, it is clearly sufficient to compute $A(Z) \pmod{|S_q|}$ for all primes q dividing $|G|$, S_q being a Sylow- q -subgroup of G . For $A(Z) \pmod{|G|}$ can then be computed from the $A(Z) \pmod{|S_q|}$ via the Chinese remainder theorem.

Now to find $A(Z) \pmod{|S_q|}$, we must count the number of codewords $A_i(q)$ of each weight i which are pointwise fixed by some element $g \neq 1$ of S_q . Clearly the codewords

of weight i which are fixed by no such element divide themselves into S_q -orbits of size $|S_q|$ and so

$$A_i \equiv A_i(q) \pmod{|S_q|}$$

It is known (Ref. 2, Sections 315-321) that for $q \neq 2$, the Sylow subgroups S_q of G are all cyclic. This makes it particularly easy to handle odd primes q . For example, let g_0 be an element of order q of S_q . Then if $g \neq 1$ is any other element of S_q , some power of g will equal g_0 . Thus the set of codewords fixed by some non-identity element of S_q is identical with the set of codewords fixed by g_0 . The subcode of the LQR code consisting of the codewords fixed by g_0 can then be found by solving a system of linear equations in $C_0, C_1, \dots, C_{p-1}, C_\infty$ over $GF(2)$ consisting of the parity-check equations for the LQR code together with the $p+1$ equations

$$C_u = C_{g \cdot u}, \quad u = 0, 1, \dots, p-1, \infty$$

The dimension of this subcode typically turns out to be small enough so that it is possible to calculate its weight enumerator by direct computer enumeration.

The Sylow-2 subgroup S_2 of G is dihedral of order 2^{m+1} , where 2^m is the highest power of 2 that divides $\frac{1}{2}(p-1)$ or $\frac{1}{2}(p+1)$. In order to compute the weight enumerator $\pmod{|S_2|}$, we prove a lemma which is a special case of Möbius inversion on a partially ordered set (Ref. 3, Chapter 2).

LEMMA: Let G be a finite group and let $f(H)$ be a function defined on all subgroups H of G . Let $g(\cdot)$ be a function defined on subgroups of G by

$$g(K) = \sum_{H \supseteq K} f(H)$$

Then if $\mu(\cdot)$ is the function on subgroups defined by the property $\mu(1) = 1$,

$$\sum_{K \leq H} \mu(K) = 0 \quad \text{if } H \neq 1$$

we have

$$f(1) = \sum_{K \supseteq 1} g(K) \mu(K)$$

Proof:

$$\begin{aligned} \sum_{K \supseteq 1} g(K) \mu(K) &= \sum_{K \supseteq 1} \mu(K) \sum_{H \supseteq K} f(H) \\ &= \sum_{H \supseteq 1} f(H) \sum_{K \leq H} \mu(K) \\ &= f(1) \end{aligned}$$

If C is any LQR codeword, the set of elements in $LF(2, p)$ which fix C is a subgroup, called the *stabilizer* of C . We now apply our lemma with $G =$ the S_2 - subgroup of $LF(2, p)$, $f_i(H)$ = the number of codewords of weight i with stabilizer H ,

$$g_i(K) = \sum_{H \cong K} f_i(H)$$

= the number of codewords of weight i fixed by every element of K . Then if $A_i(G)$ denotes the number of codewords of weight i of LQR fixed by some element of G , the lemma yields

$$\begin{aligned} A_i(G) &= A_i - f_i(1) = g_i(1) - f_i(1) \\ &= - \sum_{H > 1} \mu(H) g_i(H) \end{aligned} \quad (1)$$

Furthermore, it is not difficult to calculate the function μ for a dihedral group G of order 2^{m+1} generated by $\{a, b\}$ with $a^{2^m} = 1, b^2 = 1, bab = a^{-1}$. It turns out that $\mu(1) = 1, \mu(H) = -1$ for all subgroups of order 2, and $\mu(H) = 2$ for all subgroups of order 4 except for the unique cyclic subgroup of order 4 for which $\mu(H) = 0$, and $\mu(H) = 0$ for all subgroups of order 8 or more.

Thus to compute the weight enumerator mod $|S_2|$ we need only compute the subcodes fixed by the various subgroups of order 2 and 4 of S_2 and apply Eq. (1). There are $2^m + 1$ subgroups of order 2 in S_2 , viz.,

$$\begin{aligned} G_2^i &= \{1, a^i b\}, & i = 0, 1, \dots, 2^m - 1 \\ H_2 &= \{1, a^{2^{m-1}}\} \end{aligned}$$

Furthermore, these subgroups are all conjugate in $LF(2, p)$ (see Burnside, Ref. 2, Section 318), and so the weight enumerators of the LQR subcodes fixed by these groups are all identical.

Aside from the cyclic group of order 4, S_2 has 2^{m-1} subgroups of order 4, viz.,

$$G_4^i = \{1, a^{2^{m-1}}, a^i b, a^{i+2^{m-1}} b\}, \quad i = 0, 1, \dots, 2^{m-1} - 1$$

It can be shown that G_4^i and G_4^j are conjugate in S_2 if $i \equiv j \pmod{2}$ and so in order to compute the weight enumerators of the LQR subcodes corresponding to the G_4^i one needs only those of G_4^0 and G_4^1 . Thus if $A_i(S_2)$ denotes the number of codewords of weight i fixed by some element of S_2 , we have

$$A_i(S_2) = (2^m + 1) g_i(H_2) - 2^{m-1} g_i(G_4^0) - 2^{m-1} g_i(G_4^1) \quad (2)$$

In summary, let $Z_{q_1}, Z_{q_2}, \dots, Z_{q_r}$ be any set cyclic subgroups of $LF(2, p)$ of odd prime orders q_i , one for each odd prime dividing $p(p^2 - 1)/2$. Then we have shown that in order to compute the weight enumerator of LQR mod $p(p^2 - 1)/2$, it is sufficient to compute the weight enumerators of the subcodes fixed by $Z_{q_1}, Z_{q_2}, \dots, Z_{q_r}, H_2, G_4^0$ and G_4^1 . In the next section, we apply these techniques to the cases $p = 97$ and $p = 103$.

III. Applications

A. Case 1

Let $p = 97$, the smallest prime for which the weight enumerator for LQR is not known. Here $p(p^2 - 1)/2 = 456,288 = 2^5 \cdot 3 \cdot 7^2 \cdot 97$. Now according to Gleason's theorem on self-dual codes (Ref. 4) the weight enumerator $A(Z)$ of LQR (97) has the form

$$A(Z) = \sum_{k=0}^{12} K_k (1 + Z^2)^{49-4k} (Z^2 - 2Z^4 + Z^6)^k \quad (3)$$

for certain integers K_k . Now it is known (Ref. 1, p. 360), that

$$A_0 = 1, A_2 = A_4 = A_6 = \dots = A_{14} = 0$$

and this determines K_0, K_1, \dots, K_7 , leaving $K_8, K_9, K_{10}, K_{11}, K_{12}$ undetermined. However, it is possible to show that if

$$a(Z) = \sum_{i=0}^p a_i Z^i$$

is the weight enumerator for the AQR code, $p \equiv 1 \pmod{8}$, that

$$a(i) = \pm (1 + i) 2^{(p-1)/4}$$

The "+" sign holds if $k = \text{ord}_p(2)$ is even and $m = p - 1/2k$ is also even. The "-" sign holds in all other cases. On page 70 of Ref. 5 it is proved that

$$a(Z) = A(Z) + \frac{1 - Z}{p + 1} A'(Z)$$

$A(Z)$ being the weight enumerator of the LQR code. Now $A(i) = 0$ and so $A'(i) = \pm (n + 1) 2^{(n-1)/4} i$. Now if we differentiate Gleason's theorem

$$A(Z) = \sum_{k=0}^{(p-1)/8} K_k (1 + Z^2)^{(p+1)/2-4k} (Z^2 - 2Z^4 + Z^6)^k$$

and set $Z = i$, we obtain

$$A'(i) = (-1)^{(p-1)/8} 2^{(p+3)/4} i K_{(p-1)/8}$$

and so

$$\begin{aligned} K_{(p-1)/8} &= \pm (-1)^{(p-1)/8} \cdot (n+1)/2 \\ &= (n+1)/2 \text{ for } p = 41, 113, 137, 257, 281, \dots \\ &= -(n+1)/2 \text{ } p = 17, 73, 89, 97, 193, 233, 241, \dots \end{aligned}$$

In particular, $K_{12} = -49$ for the LQR of length 98. Thus only K_8, K_9, K_{10}, K_{11} remain unknown, and so it is sufficient to know $A_{16}, A_{18}, A_{20}, A_{22}$ to find $A(Z)$.

We now compute $A_{16}, A_{18}, A_{20}, A_{22} \pmod{456288}$. It is shown in Burnside (Ref. 2) Section 317 that if q divides $p+1$, an element of order q has no fixed points. Thus no code words of weight i can be fixed by S_q unless q divides i . Thus

$$A_{16} \equiv A_{18} \equiv A_{20} \equiv A_{22} \equiv 0 \pmod{49}$$

Also, the translation $u \rightarrow u+1$ is of order 97 and fixes only $(0, 0, \dots, 0)$ and $(1, 1, \dots, 1)$. Hence

$$A_{16} \equiv A_{18} \equiv A_{20} \equiv A_{22} \equiv 0 \pmod{97}$$

To handle the prime 3, we observe that $u \rightarrow 2^{16}u$ is an element of order 3. By computer it was found that the corresponding subcode has dimension 17, with

$$\begin{aligned} A_{16} &= 0 \\ A_{18} &= 8 \\ A_{20} &= 16 \\ A_{22} &= 128 \end{aligned}$$

Thus

$$\begin{aligned} A_{16} &\equiv 0 \pmod{3} \\ A_{18} &\equiv 2 \pmod{3} \\ A_{20} &\equiv 1 \pmod{3} \\ A_{22} &\equiv 2 \pmod{3} \end{aligned}$$

This completes the work with odd prime divisions of $p(p^2-1)/2$.

For $p=2$, we must compute the weight enumerators of the three subcodes corresponding to H_2, G_4^0 , and G_4^1 . These subcodes were calculated by computer, with these results:

Subgroup	Dimension of Subcode	A_{16}	A_{18}	A_{20}	A_{22}
H_2	25	54	161	420	1740
G_4^0	13	6	3	6	0
G_4^1	14	0	15	18	38

Combining these results via the Chinese remainder theorem, we obtain:

$$\left. \begin{aligned} A_{16} &\equiv 28518 \pmod{456288} \\ A_{18} &\equiv 80801 \pmod{456288} \\ A_{20} &\equiv 19012 \pmod{456288} \\ A_{22} &\equiv 437276 \pmod{456288} \end{aligned} \right\} \quad (4)$$

Finally we used the only other known condition on the A_i 's, namely that they are non-negative, and by linear programming concluded that $A_{16} = 28518$. (If $A_{16} \geq 28518 + 456288$, some A_i would turn out to be negative). Furthermore, there are only two possibilities for A_{18} :

$$A_{18} = 80801 \text{ or } 537089$$

The latter possibility can be ruled out if we make the plausible assumption that

$$A_i < A_{i+2}, i = 16, 17, \dots, 46$$

Altogether there are 323 possible values for $A(Z)$ consistent with Eq. (4), and 162 of them satisfy the additional constraint $A_i < A_{i+1}$.

B. Case 2

Let $p=103$. In this case, all weights in LQR are divisible by 4 and Gleason's theorem takes the simpler form

$$A(Z) = \sum_{k=0}^4 K_k (1 + 14Z^4 + Z^8)^{13-3k} (Z^4(1-Z^4))^k$$

It is known (Ref. 1, p. 360) that the minimum weight in this LQR is 16 or 20, and there is compelling statistical evidence that it is in fact 20 (Ref. 6). In any event, the conditions

$$A_0 = 1, A_4 = A_8 = A_{12} = 0$$

determine all the K 's but K_4 . In order to find $A(Z)$, therefore, it is sufficient to find A_{16} .

In this case,

$$p(p^2-1)/2 = 2^3 \cdot 3 \cdot 13 \cdot 17 \cdot 103$$

As before, $A_{16} \equiv 0 \pmod{97}$ because no code word is fixed by $u \rightarrow u+1$ except 0^{98} and 1^{98} . Also, since 13 divides $p+1=104$, an element of order 13 has no fixed points, and so only words of weight divisible by 13 can be fixed by elements of order 13. Thus $A_{16} \equiv 0 \pmod{13}$.

Also, $A_{16} \equiv 0 \pmod{17}$ since no element of G has more than two fixed points and $16 \not\equiv 0, 1, 2 \pmod{17}$. Finally, the permutation $u \rightarrow 56u$ is of order 3, and its subcode turns out to be of dimension 18. However, it contains no words of weight 16. Thus $A_{16} \equiv 0 \pmod{3}$ as well. This completes the odd primes.

For $q = 2$, it turns out that the subcode corresponding to H_2 has dimension 26, but no words of weight 16. Since H_2 is a subgroup of both G_4^0 and G_4^1 , it follows that $A_{16} \equiv 0 \pmod{8}$. Thus

$$A_{16} \equiv 0 \pmod{546312}$$

Hence $A_{16} = 546312n$ for some integer n . The weight enumerator corresponding to $n = 0$ is given by Mallows and Sloane (Ref. 7). Using their calculations, we find that $n > 1$ always forces A_{20} to be negative. The possibilities turn out to be, therefore,

$$\begin{aligned} A_{20} &= 1138150 \\ &= 45526 \end{aligned}$$

LEMMA: $A_{20} > 45526$ and so $A_{20} = 1138150$.

Proof: We immediately see that no element of order 13, 17, or 103 can fix a word of weight 20. If a is a word of weight 20, let a^g denote its images under G , and S_a its stabilizer in G . Then

$$|a^g| = |G|/|S_a|$$

Since $13 \cdot 17 \cdot 103$ divides $|a^g|$, we see that

$$|S_a| = 24, 12, 8, 6, 4, 2, \text{ or } 1$$

If $|S_a| \leq 8$, then $|a^g| > 45526$, and we are through. Thus $|S_a| = 12$ or 24 . Next, our calculations in the H_2 subcode yielded 423 words of weight 20. Since the number of words of weight 20 fixed by any of the $103 \cdot 51 = 5253$ elements of order 2 is the same, and since $|S_a| \leq 24$ for any word of weight 20, the code must contain $\geq 423 \cdot 5253/24 \approx 90000$ words of weight 20. This completes the proof of the lemma.

Corollary: The minimum distance of the (104,52) LQR code is 20, and its weight enumerator is given by the following:

i	A_i
0,104	1
20,84	1138150
24,80	206232780
28,76	15909698064
32,72	567725836990
36,68	9915185041320
40,64	88355709788905
44,60	413543821457520
48,56	1036378989344140
52	1406044530294756

Proof: This calculation was performed by Mallows and Sloane (Ref. 7).

References

1. Berlekamp, E. R., *Algebraic Coding Theory*, McGraw-Hill, New York, 1968.
2. Burnside, W., *Theory of Groups of Finite Order*, 2nd ed. 1911. Reprinted by Dover, New York, 1955.
3. Hall, M., Jr., *Combinatorial Theory*, Ginn-Blaisdell, Waltham, 1967.
4. Gleason, A., "Weight Polynomials of Self-Dual Codes and the MacWilliams Identities," *Actes, Congres intern. Math.*, 1970, Vol. 3, pp. 211-215; Gauthier-Villars, Paris, 1971.
5. vanLint, J. H., *Coding Theory*, Springer Lecture Notes in Mathematics No. 201, Berlin 1970.
6. Karlin, M., "New Binary Coding Results by Circulants," *IEEE Trans. Inform. Theory IT-15*, 1969, pp. 81-92.
7. Mallows, C. L., and Sloane, N. J. A., *An Upper Bound for Self-Dual Codes*, in press.