Weight Distributions of Some Irreducible Cyclic Codes

L. D. Baumert
Communication Systems Research Section
J. Mykkeltveit
University of Bergen, Norway

Irreducible cyclic codes are one of the largest and most powerful known classes of block codes. For example, the celebrated Golay code now being studied for use on the Mariner Jupiter-Saturn Mission is an irreducible cyclic code. This article presents techniques for computing the weight enumerators of a large subclass of irreducible cyclic codes.

I. Introduction

Irreducible cyclic codes are binary and nonbinary block codes whose encoders are linear feedback shift registers, such that the polynomial that represents the feedback logic is irreducible. Irreducible cyclic codes have proved to be among the most useful block codes: the (32, 6) first-order binary Reed-Muller code currently in use on Mariner flight projects and the (24, 12) binary Golay code which has been proposed for a Mariner Jupiter/Saturn 1977 (MJS'77) concatenated coding system are both (essentially) irreducible cyclic codes. Nonbinary irreducible cyclic codes could be used to conserve bandwidth for low-rate, deep-space telemetry.

It is the object of this article to provide techniques for computing the weight enumerators of a large class of irreducible cyclic codes. The weight enumerator of a block code of length n is the polynomial

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

where A_i denotes the number of words of weight i in the code. The enumerator $A(Z)$ provides valuable information about the performance of the code, and is needed to compute the error probability associated with proposed decoding algorithms.

The results of this paper enable one to compute the weight enumerator of all (n, k) p-ary irreducible codes for which the integer $N = (p^k - 1)/n$ is a prime congruent to 3 (mod 4) for which p has order $(N - 1)/2$.

II. Preliminaries

Let p be a prime, $q = p^k$, F_q the finite field with q elements and $T(\xi) = \xi + \xi^p + \cdots + \xi^{p^{k-1}}$, the trace of F_q/F_p. If n divides $q - 1$ and if θ is a primitive n-th root of unity in F_q, the set C of n-tuples

$$c(\xi) = (T(\xi), T(\xi\theta), \cdots, T(\xi\theta^{n-1})), \qquad \xi \text{ in } F_q$$

in a vector space over F_p that is closed under the cyclic permutation $S: (v_0, v_1, \cdots, v_{n-1}) \to (v_1, \cdots, v_{n-1}, v_0)$. C is called an (n, k) irreducible cyclic code over F_p. (Cyclic because it is S-invariant and irreducible because no subspace of C is S-invariant).

Let N be a positive integer not divisible by p and let $k = \text{ord}_N(p)$, i.e., k is the least positive integer such that $p^k \equiv 1$ modulo N. Associate with N and p the sequence of (n_m, km) irreducible cyclic codes with $n_m = (p^{km} - 1)/N$. R. J. McEliece and H. Rumsey (Ref. 1) have shown that the calculation of the weight distributions for this whole sequence of codes reduces to a single calculation (essen-

tially that of calculating the weight distribution for the case $m = 1$). Explicitly, they show that we want to determine the polynomial

$$H^{(1)}(x) = H(x) = \sum_{i=0}^{N-1} \eta_i x^i \tag{1}$$

where the numbers η_i are defined as follows: let Ψ be a primitive root of F_q such that $\Psi^N = \theta$ (thus $nN = p^k - 1$), let $\zeta = \exp(2\pi i/p)$ and let $\epsilon(\xi) = \zeta^{T(\xi)}$, then

$$\eta_i = \eta(\Psi^i) = \sum_{j=0}^{n-1} \epsilon(\Psi^i \theta^j) = \sum_{j=0}^{n-1} \epsilon(\Psi^{Nj+i}) \tag{2}$$

Thus

$$H(x) \equiv \sum_{0 \neq \alpha \epsilon F_q} x^{\mathrm{ind}(\alpha)} \epsilon(\alpha) \qquad (\text{modulo } x^N - 1) \tag{3}$$

where if $\alpha = \Psi^i$, $\mathrm{ind}(\alpha) = i$.

Baumert and McEliece (Ref. 2) have determined this polynomial in many of the simpler cases. In particular, when $k = \phi(N)/2$ they indicate methods that can be used to solve the problem (at least for those cases with $(p^k - 1)/(p - 1) \equiv 0$ modulo N, as it always is for $p = 2$). Here, when N is a prime number of the form $4t + 1$ the code weight distributions are particularly nice. These are all contained in Theorem 6 (Ref. 2). When N is a prime of the form $4t + 3$, things are a bit more difficult. In this note we establish a general formula for $H(x)$ that covers all such primes $N = 4t + 3$ with the single exception $N = 3$. Furthermore, the analogous polynomials $H^{(m)}(x)$ are also determined as well as the associated code weight distributions for the whole sequence of (n_m, km) irreducible cyclic codes. To accomplish this we make use of the rule (Ref. 1):

$$-H^m(x) \equiv (-H(x))^m \qquad (\mathrm{mod}\, x^N - 1) \tag{4}$$

III. Statement and Proof of the Results

Let $\beta = \exp(2\pi ij/N)$, $\beta \neq 1$, then it is a classical result that

$$H^{(m)}(\beta)\,\overline{H^{(m)}(\beta)} = q = p^{mk} \tag{5}$$

where the bar denotes complex conjugation. Furthermore,

$$H^{(m)}(1) = -1 \tag{6}$$

(proofs can be found in Ref. 2 as well as many other places). Since N is a prime number it follows that the $\eta_i^{(m)}$ (i.e., $H^{(m)}(x)$) can easily be determined from the coefficients a_i in

$$H^{(m)}(\beta) = a_0 + a_1 \beta + \cdots + a_{N-1} \beta^{N-1} \tag{7}$$

where, for definiteness, we fix $\beta = \exp(2\pi i/N)$.

Equation (5) shows that it is useful to know the highest power of p that divides $H(\beta)$; let this be p^a. Stickelberger (Ref. 3) provides us with a way of determining a. Let $t = t_0 + t_1 p + \cdots$ be the expansion of t in the base p and let $w_p(t) = t_0 + t_1 + \cdots$. Then, Stickelberger tells us that

$$(p - 1)\, a = \min \{w_p(jn): 1 \leq j < N \text{ where } (j, N) = 1\} \tag{8}$$

Lemma (McEliece and Welch):

Let N and p be prime numbers, $N = 4t + 3$ and $3 \neq N \neq p$. Let $k = \mathrm{ord}_N(p) = (N - 1)/2$ and let p^a be the highest power of p that divides $H(\beta)$, $\beta = \exp(2\pi i/N)$. Then

$$a = w_p(n)/(p - 1) = \sum r_i/N \tag{9}$$

where the r_i are the quadratic residues of N.

Proof:

Note first that $r \equiv pj$ modulo N implies that $w_p(rn) = w_p(jn)$. For

$$jn = j_0 + j_1 p + \cdots + j_{k-1} p^{k-1} \tag{10}$$

$$pjn = 0 + j_0 p + \cdots + j_{k-2} p^{k-1} + j_{k-1} p^k$$

$$\equiv j_{k-1} + j_0 p + \cdots + j_{k-2} p^{k-1} \text{ modulo } nN\,(= p^k - 1)$$

But $pjn \equiv rn$ modulo nN as well, and since both of these are reduced modulo nN they must be equal. So $w_p(rn) = w_p(pjn) = w_p(jn)$ as asserted and

$$rn = j_{k-1} + j_0 p + \cdots + j_{k-2} p^{k-1} \tag{11}$$

In the case at hand p generates the quadratic residues modulo N and -1 is a quadratic nonresidue of N. So only $j = \pm 1$ need be considered in Eq. (8). We wish to show that $w_p(n) \leq w_p(-n)$. Let $r_i \equiv p^i$ modulo N ($i = 0, 1, \cdots, k - 1$) and let $s_i \equiv -r_i$ modulo N. Then, it follows from Eqs. (10) and (11) that, using $j = 1$,

$$n \sum r_i = w_p(n)(1 + p + \cdots + p^{k-1})$$

$$= w_p(n)(p^k - 1)/(p - 1) \tag{12}$$

and similarly

$$n \sum s_i = w_p(-n)(p^k - 1)/(p - 1)$$

So

$$w_p(n) < w_p(-n) \text{ if } \sum r_i < \sum s_i$$

But, for primes $N = 4t + 3$, this is a famous result of Gauss (see Weyl, Ref. 4). So

$$a = w_p(n)/(p-1) = \sum r_i/N$$

as was to be proved.

Theorem:

Let N and p be prime numbers, $N = 4t + 3$ and $3 \neq N \neq p$. Let $k = \text{ord}_N(p) = (N-1)/2$, $a = w_p(n)/(p-1)$ and $\beta = \exp(2\pi i/N)$. Then for each integer $m \geqq 1$, there exist unique positive integers c_m, d_m prime to p, which satisfy the diophantine equation

$$c_m^2 + Nd_m^2 = 4p^{m(k-2a)} \tag{13}$$

and

$$H^{(m)}(\beta) = \pm p^{ma}\left(\frac{c_m + d_m + 2d_m \sum \beta^i}{2}\right) \tag{14}$$

where i runs over the quadratic residues modulo N. Further, the integers $\eta_i^{(m)}$ are given by:

$$\begin{aligned} \eta_0^{(m)} &= \frac{\pm p^{ma} c_m (N-1) - 2}{2N} \\ \eta_1^{(m)} &= \frac{\pm p^{ma}(d_m N - c_m) - 2}{2N} \\ -\eta_{-1}^{(m)} &= \frac{\pm p^{ma}(d_m N + c_m) + 2}{2N} \end{aligned} \tag{15}$$

and this determines $H^{(m)}(x)$ completely, since $\eta_{ip}^{(m)} = \eta_i^{(m)}$ (all i).

Proof:

Since $N > 3$, we have $k > 1$ and so $(p-1, N) = 1$. By the Corollary of Theorem 2 (Ref. 2) it follows that $H(\beta)$ is an algebraic integer of $Q(\beta)$; in fact, an integer of its unique quadratic subfield $Q(\sqrt{-N})$. (Q denotes the field of rational integers here.) Now, every algebraic integer of $Q(\sqrt{-N})$ has a unique representation in the form $(c + d\sqrt{-N})/2$ where c, d are rational integers and $c \equiv d$ modulo 2. Conversely, every such expression is an algebraic integer of $Q(\sqrt{-N})$. Let $\alpha = H(\beta)/p^a$ with a defined by Eq. (9) above. Then,

$$4\alpha\bar{\alpha} = c^2 + Nd^2 = 4p^{k-2a} \tag{16}$$

and α can be determined from among the solutions of this diophantine equation.

As a first step towards determining α, note that p divides α if and only if p divides c and p divides d. This is trivial except for $p = 2$, where the assumption c, d even requires special handling. Since $\alpha\bar{\alpha}$ is the norm of an algebraic integer it must be a rational integer. So $k - 2a \geqq 0$. But k is odd, so $k - 2a \geqq 1$. Furthermore, p generates the quadratic residues of N. In particular then, p is a quadratic residue of N. If $p = 2$, quadratic reciprocity tells us that $N \equiv -1$ modulo 8. So for $p = 2$, with c, d even, we find in examining Eq. (16) that $c^2 \equiv d^2$ modulo 8. Thus $c \equiv d$ modulo 4 and 2 does indeed divide α as asserted.

Since p^a was the highest power of p dividing $H(\beta)$, among the solution pairs c, d of Eq. (16) we are only concerned with those c, d not divisible by p. Consider the prime ideal factorization of the principal ideal generated by p in $Q(\sqrt{-N})$. Here $(p) = PQ$, where P, Q are complex conjugate prime ideals (i.e., $Q = \bar{P}$). So if $\gamma = (e + f\sqrt{-N})/2$ with e, f solutions of Eq. (16) and e, f prime to p, it follows that the ideal (γ) can only be P^{k-2a} or Q^{k-2a}. Thus γ or $\bar{\gamma}$ generates the same ideal that α does. Say $(\gamma) = (\alpha)$; this implies that $\gamma = u\alpha$, where u is a unit of the field $Q(\sqrt{-N})$. But, for $N > 3$, this field has only ± 1 as units. So there are only 4 possibilities for α:

$$\alpha = \pm\left(\frac{c \pm d\sqrt{-N}}{2}\right)$$

The $\pm$ sign for d corresponds to the choice between α and α which is of no consequence, as it merely reflects the ambiguity between $H(\beta)$ and $\overline{H(\beta)}$ and does not affect the answer materially. So we may stipulate without loss, that c and d are the unique positive integers, prime to p, that satisfy Eq. (16) and that $\alpha = \pm(c + d\sqrt{-N})/2$. The remaining $\pm$ ambiguity is critical and shows up in the formulas for the η_i's. Fortunately, the requirement that all the η_i's must be rational integers always resolves this final ambiguity.

So we have determined that

$$H(\beta) = \pm p^a\left(\frac{c + d\sqrt{-N}}{2}\right) = \pm p^a\left(\frac{c + d + 2d\sum \beta^i}{2}\right)$$

where i runs over the quadratic residues modulo N, as follows from Gauss' representation of $\sqrt{-N}$ in the field $Q(\beta)$. This, together with $H(1) = -1$, suffices to determine the η_i as given in Eq. (15); the theorem is proved for $m = 1$.

With $m > 1$, the above reasoning together with Congruence (4) taken at $x = \beta$, shows that p^{ma} is the highest power of p dividing $H^{(m)}(\beta)$. So the argument above determines $H^{(m)}(\beta)$ exactly as indicated in Eqs. (13), (14), and (15).

Recalling the definition, Eq. (2), of the η_i and the definition of a code word $c(\xi)$ in one of these irreducible cyclic codes, it is clear that the η_i's determine the distribution of the elements of F_p amongst the codewords of C. Thus:

Theorem:

Let N and p be prime numbers, $N = 4t + 3$ and $3 \neq N \neq p$. Let $k = \mathrm{ord}_N(p) = (N-1)/2$, let $a = w_p(n)/(p-1)$, let $q = p^{mk}$, and let c_m, d_m be the unique positive integers prime to p that satisfy the diophantine equation $c_m^2 + Nd_m^2 = 4p^{m(k-2a)}$. Then there are three distributions of elements of F_p that occur in the nonzero codewords of the associated (n_m, km) irreducible cyclic code: (caution if $m = 1$ and $k \neq \mathrm{ord}_n p$ this code is degenerate in that some codewords are repeated).

Class 0 (containing n_m codewords):

$$N_0 = \frac{2q - 2p \pm (p-1)\,p^{ma}\,c_m\,(N-1)}{2pN}$$

$$N_i = \frac{2q \mp p^{ma}\,c_m\,(N-1)}{2pN} \qquad i = 1, \cdots, p-1$$

Class 1 (containing $n_m(N-1)/2$ codewords):

$$N_0 = \frac{2q - 2p \pm (p-1)\,p^{ma}\,(d_m N - c_m)}{2pN}$$

$$N_i = \frac{2q \mp p^{ma}\,(d_m N - c_m)}{2pN} \qquad i = 1, \cdots, p-1$$

Class -1 (containing $n_m(N-1)/2$ codewords):

$$N_0 = \frac{2q - 2p \mp (p-1)\,p^{ma}\,(d_m N + c_m)}{2pN}$$

$$N_i = \frac{2q \pm p^{ma}\,(d_m N + c_m)}{2pN} \qquad i = 1, \cdots, p-1$$

Here N_i is the number of times the element i of F_p appears in the codeword.

IV. Some Examples

Example 1: $N = 7$, $p = 2$, $k = 3$, $n = a = c = d = 1$. This code is degenerate and its 7 (supposed nonzero) codewords are 1,1,1,1,0,0,0. Nevertheless our formulas are valid. They give $\eta_0 = \eta_1 = -1$, $\eta_{-1} = +1$; $H(x) = -1 - x - x^2 + x^3 - x^4 + x^5 + x^6$. Class 0 contains 1 codeword ($N_0 = 0$, $N_1 = 1$). Class 1 contains 3 codewords ($N_0 = 0$, $N_1 = 1$). Class -1 contains 3 codewords ($N_0 = 1$, $N_1 = 0$.

It can be shown that these codes are degenerate only when $m = 1$ (and not always then). So let us consider $m = 2$. Here $N = 7$, $p = 2$, $mk = 6$, $n_2 = 9$, $a = d_2 = 1$, $c_2 = 3$. Equation (15) yields $\eta_0^{(2)} = 5$, $\eta_1^{(2)} = 1$, $\eta_{-1}^{(2)} = -3$ so $H^{(2)}(x) = 5 + x + x^2 + x^4 - 3(x^3 + x^5 + x^6)$. Thus there are 9 codewords ($N_0 = 7$, $N_1 = 2$), 27 codewords ($N_0 = 5$, $N_1 = 4$) and 27 codewords ($N_0 = 3$, $N_1 = 6$).

Example 2: $N = 11$, $p = 3$, $k = 5$, $n = 22$, $a = 2$, $c = d = 1$. Equation (15) yields $\eta_0 = \eta_1 = 4$, $\eta_{-1} = -5$. Class 0 contains 22 codewords ($N_0 = 10$, $N_1 = N_2 = 6$). Class 1 contains 110 codewords ($N_0 = 10$, $N_1 = N_2 = 6$). Class -1 contains 110 codewords ($N_0 = 4$, $N_1 = N_2 = 9$).

Example 3: $N = 79$, $p = 2$, $k = 39$, $n = 6\,958\,934\,353$, $a = 17$, $c = 7$, $d = 1$. Thus $\eta_0 = 452945$, $\eta_1 = 59729$, $\eta_{-1} = -71343$. Class 0 contains n codewords ($N_0 = 3479693649$, $N_1 = 3479240704$). Class 1 contains $39n$ codewords ($N_0 = 3479497041$, $N_1 = 3479437312$). Class -1 contains $39n$ codewords ($N_0 = 3479431505$, $N_1 = 3479502848$).

References

1. McEliece, R. J., and Rumsey, H., "Euler Products, Cyclotomy and Coding," *J. Number Theory*, Vol. 4, No. 3, pp. 302–311, June 1972.
2. Baumert, L. D., and McEliece, R. J., "Weights of Irreducible Cyclic Codes," *Inform. Contr.*, Vol. 20, No. 2, pp. 158–175, March 1972.
3. Stickelberger, L., "Über eine Verallgemeinerung der Kreisteilung," *Math. Ann.* Vol. 37, (1890), pp. 321–367.
4. Weyl, H., *Algebraic Theory of Numbers*, pp. 199–200. Princeton University Press, Princeton, N.J., 1940.