INFORMATION AND CONTROL 20, 158–175 (1972)

Weights of Irreducible Cyclic Codes

L. D. BAUMERT AND R. J. MCELIECE*

Jet Propulsion Laboratory,
California Institute of Technology, Pasadena, California 91103

With any fixed prime number p and positive integer N, not divisible by p, there is associated an infinite sequence of cyclic codes. In a previous article it was shown that a theorem of Davenport–Hasse reduces the calculation of the weight distributions for this whole sequence of codes to a single calculation (essentially that of calculating the weight distribution for the simplest code of the sequence). The primary object of this paper is the development of machinery which simplifies this remaining calculation. Detailed examples are given. In addition, tables are presented which essentially solve the weight distribution problem for all such binary codes with $N < 100$ and, when the block length is less than one million, give the complete weight enumerator.

1. INTRODUCTION

With any fixed prime number p and positive integer N, not divisible by p, we associate an infinite sequence of cyclic codes. In a previous article (McEliece and Rumsey, 1972) it was shown that a theorem of Davenport–Hasse reduces the calculation of the weight distributions for this whole sequence of codes to a single calculation in $GF(p^{k_0})$, where $k_0 = \text{ord}_N(p) =$ least integer such that $p^{k_0} \equiv 1 \pmod{N}$. The primary object of this paper is the development of machinery which simplifies this remaining calculation; it turns out that the algebra of the cyclotomic number fields $Q(\zeta_N)$ can be brought to bear on the problem, with favorable results. In Section 2 the codes are introduced; in Section 3 some theoretical results are developed and in Section 4 we outline the way these results will be applied; in Sections 5 and 6 we give detailed examples of the technique; and in Section 7 we present a table which essentially solves the weight distribution problem for all irreducible binary cyclic codes with $N < 100$, and a table which gives the complete weight enumerator for all such codes of block length less than one million.

* This paper presents the results of one phase of research carried out at the Jet Propulsion Laboratory, California Institute of Technology, under Contract No. NAS 7-100, sponsored by the National Aeronautics and Space Administration.

2. Irreducible Cyclic Codes

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

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

is a cyclic code over F_p of dimension k', where $k' = \mathrm{ord}_n(p)$. We call C an (n, k) irreducible cyclic code. [Note that if $k \neq k'$ this code, as defined, is degenerate, in that the same codeword is repeated several times.] Now let $\zeta = \exp(2\pi i/p)$ and for ξ in F_q, let $\epsilon(\xi) = \zeta^{T(\xi)}$, where elements from F_p are regarded as integers in the set $\{0, 1,\ldots, p - 1\}$. With each codeword $c(\xi)$ we associate a complex exponential sum $\eta(\xi) = \sum_{i=0}^{n-1} \epsilon(\xi\theta^i)$; from η we can compute the weight of the codeword c. Let ψ be a primitive root of F_q such that $\psi^N = \theta$, where $N = (q - 1)/n$. Then if $i \equiv j \pmod N$ the codewords $c(\psi^i)$ and $c(\psi^j)$ differ only by a cyclic shift, so to compute the complete weight distribution of the code C it is sufficient to compute the N sums $\eta_i = \eta(\psi^i)$, $i = 0, 1,\ldots, N - 1$. Thus we are led to consider the generating function

$$H(x) = \sum_{i=0}^{N-1} \eta_i x^i = \sum_{i=0}^{N-1} x^i \sum_{j=0}^{n-1} \epsilon(\psi^i \psi^{Nj}) \equiv \sum_{\alpha \in F_q^*} x^{\mathrm{ind}(\alpha)} \epsilon(\alpha) \pmod{x^N - 1},$$

where the last sum is taken over the nonzero elements of F_q, and if $\alpha = \psi^i$, $\mathrm{ind}(\alpha) = i$.

Now let $k = \mathrm{ord}_N(p)$, $q = p^k$; the sequence of (n_m, km) irreducible cyclic codes where $n_m = (q^m - 1)/N$, contains all the nondegenerate (n, k) irreducible cyclic codes for which $(p^k - 1)/n = N$, one for each $m \geqslant 1$. [All codes which arise here when $m \geqslant 2$ are nondegenerate; when $m = 1$ the code may be degenerate.] If the associated generating functions are indexed $H^{(m)}(x) \pmod{x^N - 1}$, the main result of McEliece and Rumsey (1972) was that

$$-H^{(m)}(x) \equiv (-H^{(1)}(x))^m \pmod{x^N - 1} \tag{2.1}$$

provided that the primitive root ψ_m in F_{q^m} satisfied $\psi_m^{1+q+\cdots+q^{m-1}} = \psi_1 = \psi$. Thus the problem of computing the weight distributions of the whole family of irreducible cyclic codes with a fixed N (relatively prime to p) was reduced to that of computing a single polynomial $H^{(1)}(x)$, whose parameters n and k are determined uniquely by $k = \mathrm{ord}_N(p)$, $n = (p^k - 1)/N$.

Consider the trivial case $N = 1$. Here, for any prime power $q = p^m$, there are $p^m - 1$ nonzero codewords of word length $n = p^m - 1$ and in each of

these codewords 0 occurs $p^{m-1} - 1$ times and i occurs p^{m-1} times, $1 \leqslant i \leqslant p - 1$.

The codes for $N = 2$ are not trivial; however, the ground case (i.e., $m = 1$) is quite easy. So temporarily we limit ourselves to the determination of $H^{(1)}(x)$. (Complete weight distributions for these codes are given at the end of Section 5, below.) $N = 2$, $m = 1$ and so p is odd, $k = \operatorname{ord}_N(p) = 1$, $n = (p - 1)/2$. Under cyclic shift, the nonzero codewords divide themselves into two sets of n codewords each. Every codeword of one set contains as coordinates each of the nonzero squares modulo p precisely once [i.e., i^2 modulo p for $1 \leqslant i \leqslant (p - 1)/2$]. Every codeword of the other set contains each of the remaining $(p - 1)/2$ nonzero elements precisely once. Let $p^* = (-1)^{(p-1)/2}p$, then, Gauss has shown that,

$$\eta_0 = \zeta + \zeta^4 + \cdots + \zeta^{[(p-1)/2]^2} = \frac{\sqrt{p^*} - 1}{2}; \qquad \eta_1 = -\frac{\sqrt{p^*} + 1}{2}.$$

So

$$2H^{(1)}(x) \equiv \sqrt{p^*} - 1 - (\sqrt{p^*} + 1)x \pmod{x^2 - 1}.$$

3. Some Theoretical Results

We now present a theorem which will aid in the calculation of $H^{(1)}(x)$.

Theorem 1. *$H(1) = -1$, and*

$$H(x)\,H(x^{-1}) \equiv qx^{\operatorname{ind}(-1)} - n(1 + x + \cdots + x^{N-1}) \pmod{x^N - 1}.$$

Proof. $H(1) = \sum_{\alpha \neq 0} \epsilon(\alpha) = -1$ follows from $\sum_\alpha \epsilon(\alpha) = 0$.
We now consider the second assertion.

$$\begin{aligned} H(x)H(x^{-1}) &= \sum_{\alpha \neq 0} x^{\operatorname{ind}(\alpha)}\epsilon(\alpha) \sum_{\beta \neq 0} x^{-\operatorname{ind}(\beta)}\epsilon(\beta) \\ &= \sum_{\alpha \neq 0, \beta \neq 0} x^{\operatorname{ind}(\alpha/\beta)}\epsilon(\alpha + \beta) = \sum_{\gamma \neq 0, \beta \neq 0} x^{\operatorname{ind}(\gamma)}\epsilon(\beta(\gamma + 1)) \\ &= \sum_{\gamma \neq 0} x^{\operatorname{ind}(\gamma)} \sum_{\beta \neq 0} \epsilon(\beta(\gamma + 1)). \end{aligned}$$

Now

$$\sum_{\beta \neq 0} \epsilon(\beta(\gamma + 1)) = \begin{cases} q - 1 & \text{if } \gamma = -1 \\ -1 & \text{if } \gamma \neq -1. \end{cases}$$

Therefore

$$H(x)H(x^{-1}) = x^{\mathrm{ind}(-1)}(q-1) - \sum_{\gamma \neq 0,-1} x^{\mathrm{ind}(\gamma)} = qx^{\mathrm{ind}(-1)} - \sum_{\gamma \neq 0} x^{\mathrm{ind}(\gamma)}$$

$$\equiv qx^{\mathrm{ind}(-1)} - n(1 + x + \cdots + x^{N-1}) \pmod{x^N - 1},$$

since $nN = q - 1$.

COROLLARY. *If β is any complex N-th root of unity $\neq 1$,*

$$H(\beta)\, H(\beta^{-1}) = q \cdot \beta^{\mathrm{ind}(-1)} = \pm q.$$

The minus sign can occur only when N is even and n is odd. Also

$$H(\beta)\overline{H(\beta)} = q.$$

Proof. $\mathrm{ind}(-1) = 0$ for even q. When q is odd, $\mathrm{ind}(-1) = (q-1)/2$ and then $(\exp(2\pi ij/N))^{Nn/2} = \exp(\pi ijn) = -1$ only if j and n are odd. Let $\sigma : \beta \to \beta^{-1}$. Then σ commutes with complex conjugation, so

$$|\, H(\beta)|^2 = \overline{H(\beta)}H(\beta) = [\overline{H(\beta)}H(\beta)]^{\sigma} = \overline{H(\beta^{-1})}H(\beta^{-1}) = |\, H(\beta^{-1})|^2$$

from which the second equation follows.

The corollary provides a factorization of q in the field $Q(\zeta, \beta)$, the cyclotomic field generated by ζ and β. Under certain circumstances $H(\beta)$ lies in a small subfield of $Q(\zeta, \beta)$. We now investigate these circumstances.

THEOREM 2. *Fix $\beta = \exp(2\pi i/N)$. Let λ be the automorphism of $Q(\zeta, \beta)/Q$ which maps $\beta \to \beta^p$, let $g = \psi^{(q-1)/(p-1)}$ (g in F_q is a generator of $F_p{}^*$, thus g^i is an integer modulo p) and let $\sigma_i : \zeta \to \zeta^{g^i}$. Then*

$$\lambda H(\beta) = H(\beta), \qquad \sigma_i H(\beta) = \beta^{-i(q-1)/(p-1)} H(\beta).$$

Proof.

$$\lambda H(\beta) = \sum_{\alpha \neq 0} \beta^{p \cdot \mathrm{ind}(\alpha)} \epsilon(\alpha)$$

$$= \sum_{\alpha \neq 0} \beta^{\mathrm{ind}(\alpha^p)} \epsilon(\alpha) = \sum_{\alpha \neq 0} \beta^{\mathrm{ind}(\alpha)} \epsilon(\alpha^{1/p})$$

$$= H(\beta) \text{ since } \epsilon(\alpha^{1/p}) = \epsilon(\alpha).$$

$$\sigma_i H(\beta) = \sum_{\alpha \neq 0} \beta^{\mathrm{ind}(\alpha)} \zeta^{g^i T(\alpha)} = \sum_{\alpha \neq 0} \beta^{\mathrm{ind}(\alpha)} \zeta^{T(g^i \alpha)}$$

$$= \sum_{\alpha \neq 0} \beta^{\mathrm{ind}(\alpha g^{-i})} \epsilon(\alpha) = \sum_{\alpha \neq 0} \beta^{\mathrm{ind}(\alpha) + \mathrm{ind}(g^{-i})} \epsilon(\alpha)$$

$$= \beta^{-i(q-1)/(p-1)} H(\beta),$$

as asserted.

COROLLARY. *If* $(q-1)/(p-1) \equiv 0 \pmod{N}$, $\sigma_i H(\beta) = H(\beta)$, *and* $H(\beta)$ *lies in* $Q(\beta)$.

In this case, $H(\beta)$ in fact lies in a K-th degree subfield Ω of $Q(\beta)$ where $kK = \phi(N)$; viz., the fixed field of the automorphism $\beta \to \beta^p$ of $Q(\beta)/Q$. [Here ϕ denotes Euler's function.]

Proof. The first assertion follows from the fact that the fixed field of the group $\{1, \sigma_1, \ldots, \sigma_{p-1}\}$ of automorphisms of $Q(\zeta, \beta)/Q$ is $Q(\beta)$. The second follows from the fact that λ generates a group of automorphisms of order k of $Q(\beta)/Q$, and $\deg[Q(\beta) : Q] = \phi(N)$.

In order to exploit these facts about $H(\beta)$, we now need to import without proof several theorems from algebraic number theory. In view of the factorization $H(\beta)\overline{H(\beta)} = q = p^k$ provided by the corollary to Theorem 1, it will be useful to know something about the way the ideal (p) decomposes in the ring of integers of the subfield Ω of $Q(\beta)$.

The Galois group of the extension $Q_N = Q(\beta)/Q$ is isomorphic to Φ_N, the multiplicative group of the residues prime to N. Thus the Galois group of Ω/Q is isomorphic to the factor group $\Phi_N/\{p\}$, where $\{p\} = \{1, p, \ldots, p^{k-1}\}$ is the subgroup of Φ_N generated by p. If a is an element of Φ_N, let $\bar{a}$ be its image under the homomorphism of Φ_N onto $\Phi_N/\{p\}$, and let $a_1, a_2, \ldots, a_K$ be a complete set of coset representatives of $\{p\}$ in Φ_N. We can now describe the decomposition of (p).

THEOREM 3 [see, for example, Mann (1955, Chapter 8)]. *In the ring of integers of* Ω, (p) *decomposes into a product of* K *distinct prime ideal factors. They can be labeled* $P_1, P_2, \ldots, P_K$ *in such a way that under the automorphism* $\lambda_a : \beta \to \beta^a$ *of* Ω/Q *the* P*'s are permuted according to the rule* $\lambda_a : P_i \to P_j$ *if* $\bar{a} \cdot \bar{a}_i = \bar{a}_j$ *in* $\Phi_N/\{p\}$.

It turns out that the sum $H(\beta) = \sum_{\alpha \in F^*} \beta^{\mathrm{ind}(\alpha)} \zeta^{T(\alpha)}$ has been studied extensively under the name of *generalized Gauss sum* (a.k.a. Jacobi function or generalized Lagrange resolvent!). In particular Stickelberger (1890) [Lang

(1970, pp. 90 ff) is perhaps a more convenient reference] completely settled the question of the prime ideal decomposition of the ideal $(H(\beta))$ in the ring of integers of the field $Q(\beta, \zeta)$. If m is an arbitrary integer $\geqslant 0$, let $m = m_0 + m_1 p + \cdots$ be the expansion of m in the base p, and let $w_p(m) = m_0 + m_1 + \cdots$. Then Stickelberger's theorem, in the case that interests us, is

THEOREM 4 (Stickelberger, 1890). *If $H(\beta)$ lies in Ω, then there is a labeling of the prime ideal factors of p which is consistent with Theorem 3 and such that*

$$(H(\beta)) = P_1^{e_1} P_2^{e_2} \cdots P_K^{e_K},$$

where

$$e_i = w_p(a_i n)/(p-1).$$

COROLLARY. *$H(\beta)$ is exactly divisible by p^t, where*

$$(p-1)t = \min\{w_p(jn) : 1 \leqslant j < N \text{ and } (j, N) = 1\}.$$

Proof. This follows since $\min e_i = t$ and $(p) = P_1 \cdots P_K$.

Remark. Let $t' = \min\{w_p(jn) : 1 \leqslant j < N\}/(p-1)$. Then it can be shown that $p^{t'}$ is the highest power of p such that $\eta_i \equiv n \pmod{p^{t'}}$ for all i. It is interesting that $H(\beta) = \eta_0 + \eta_1\beta + \cdots + \eta_{N-1}\beta^{N-1}$ can sometimes be divisible by a higher power of p than t'. [See Example a in Section 6 below. There $w_2(5n) = 4$ but $t = 5$.]

Theorem 4 is not as helpful in computing $H(\beta)$ as one might at first suppose, since in general the P_i are not principal ideals, and in addition the question of units is troublesome. However, there is one fact about units which we will find useful.

THEOREM 5 [Mann (1955, Chapter 14) contains a proof]. *The only units of absolute value 1 in $Q_N = Q(\beta)/Q$ are the roots of unity $\pm\beta^i$. Thus in Ω the only such units are $\pm$ the $(p-1, N)$-th roots of unity. In particular if $(p-1, N) = 1$ or 2 only ± 1 are possible.*

4. THE PLAN OF ATTACK

We now outline how the theorems of Section 3 can be used to compute the polynomials $H(x)$.

Step 1. Compute the values $H(\beta_d)$, $\beta_d = \exp(2\pi i/d)$, for all divisors d of N. In general this can only be done up to an ambiguity of sign and of conjugation of the ideals P_i. Some examples are given in Sections 5 and 6.

Step 2. Compute the values of $H(x_d) \equiv H(x) \pmod{f_d(x)}$, where $f_d(x)$ is the d-th cyclotomic polynomial. This follows trivially from step 1, since if $H(\beta_d) = a_0 + a_1\beta_d + \cdots + a_{d-1}\beta_d^{d-1}$, then

$$H(x_d) \equiv a_0 + a_1 x + \cdots + a_{d-1}x^{d-1} \pmod{f_d(x)}.$$

Step 3. Synthesize $H(x)$ from its values modulo $f_d(x)$ via the Chinese remainder theorem. The exact form of the CRT in this situation is given below for the reader's convenience, but see Section III.D of Baumert (1971) for a proof. Incidentally, at this stage it is usually possible to resolve the ambiguity which occurred at step 1, since inconsistent choices of the various $H(x_d)$'s usually lead to an $H(x)$ whose coefficients are not integers.

The explicit form of the Chinese remainder theorem in this case is

$$H(x) \equiv \frac{1}{N} \sum_{d|N} H(x_d) B_{N,d}(x) \qquad (\text{mod } x^N - 1), \tag{4.1}$$

where

$$B_{N,d}(x) = \sum_{r|d} \mu\left(\frac{d}{r}\right) r \frac{x^N - 1}{x^r - 1},$$

with μ the Möbius function. One way to use this formula is to compute $H(x)$ modulo $x^d - 1$ for all divisors d of N starting with $d = 1$ and working up to $d = N$. This process allows the resolution of the ambiguities of Step 1 at a lower level than N. It is facilitated by the criterion given below [see Baumert (1971) for a proof of this], which permits those candidates for $H(x_d)$, not yielding integer coefficients in $H(x)$ modulo $x^d - 1$, to be discarded prior to its computation.

Integer Coefficient Criterion. Suppose that, for each prime divisor r of d, an integral polynomial $g_{d/r}(x)$ is known such that $H(x) \equiv g_{d/r}(x)$ modulo $x^{d/r} - 1$. Then a necessary and sufficient condition for the existence of an integral polynomial congruent to $H(x)$ modulo $x^d - 1$ is that

$$H(x_d) \equiv g_{d/r}(x) \qquad (\text{mod } r, f_{d_1}^{r^{a-1}}(x)) \tag{4.2}$$

for all prime divisors r of d. Here $d = r^a d_1$ with d_1 prime to r.

5. The Semiprimitive Case

In this section we assume that there is a j such that $p^j \equiv -1 \pmod{N}$. Take j to be the least such positive integer, then for $N > 2$, $k = 2j$, $q = p^{2j}$, $n = (p^{2j} - 1)/N$. ($N = 1$ is solved in Section 2 above and $N = 2$ is discussed at the end of this section.) Here $H(\beta_d)$ is an integer of Q_d by Theorem 2 and its corollary. Furthermore, it is easy to see that the P_i are fixed under complex conjugation, for by Theorem 3 they are fixed by all automorphisms $\beta_d \to \beta_d^{p^i}$ and so in particular by $\beta_d \to \beta_d^{-1}$. Thus the factorization $H(\beta_d)\overline{H(\beta_d)} = p^{2j}$ forces $(H(\beta_d)) = (p)^j$ and since $(p - 1, N)$ divides $(p^j - 1, p^j + 1)$ which is at most 2, Theorem 5 implies

$$H(\beta_d) = \pm p^j \qquad \text{for all} \quad d \neq 1,$$
$$H(x) \equiv \pm p^j \qquad (\mathrm{mod}\, f_d(x)).$$

Frequently the choice of signs is forced by the requirement that the η_i are integers; to determine signs for various d, we use congruence (4.2). We claim that for each divisor d of N,

$$H^{(1)}(x) \equiv p^j x^s - \frac{p^j + 1}{d}(1 + x + \cdots + x^{d-1}) \qquad (\mathrm{mod}\, x^d - 1), \quad (5.1)$$

where $s = 0$ or $d/2$, and proceed by induction on the number l of (not necessarily distinct) primes dividing d. If $l = 0$ this is just the statement $H(1) = -1$, which is true by Theorem 1. For $l \geqslant 1$, we use the criterion of Section 4 together with the induction hypothesis:

$$\pm p^j \equiv p^j x^s - \frac{p^j + 1}{(d/r)}(1 + x + \cdots + x^{(d/r)-1}) \qquad (\mathrm{mod}\, r, f_{d_1}^{r^{a-1}}(x))$$

for all primes r dividing d. (Here $d = r^a d_1$ with d_1 prime to r.) Now since d divides $p^j + 1$, this is equivalent to

$$\pm p^j \equiv p^j x^s \qquad (\mathrm{mod}\, r, f_{d_1}^{r^{a-1}}(x)). \quad (5.2)$$

When d is odd, the induction hypothesis only allows $s = 0$ and since r is necessarily odd if d is, the "+" sign obtains. So $H^{(1)}(x) \equiv p^j$ modulo $f_t(x)$ for all divisors $t \neq 1$ of d, thus the Chinese remainder theorem assures us that

$$H^{(1)}(x) \equiv p^j - \frac{p^j + 1}{N}(1 + x + \cdots + x^{N-1}) \qquad (\mathrm{mod}\, x^N - 1), N \text{ odd}.$$

When d is even there are four cases to consider in the induction, according as the prime r is 2 or odd and according as $s = 0$ or $d/2r$. When $s = 0$ and r is odd then $H^{(1)}(x_d) = p^j$ as above. When $s = 0$ and $r = 2$ both $\pm p^j$ satisfy congruence (5.2) so either form of (5.1) can occur. When $s = d/2r$ and r is odd, then $d = r^a d_1 = 2r^a d_0$ by assumption and since $f_{2d_0}(x)$ divides $x^{d_0} + 1$, it follows that only $-p^j$ satisfies congruence (5.2). When $r = 2$ and $s = d/4$ congruence (5.2) becomes

$$\pm p^j \equiv p^j x^{2^{a-2}d_1} \qquad (\text{mod } 2, f_{d_1}(x^{2^{a-1}}))$$

which clearly has no solutions. This shows that $s = d/4$ does not occur, i.e., $H^{(1)}(x_{d/2})$ cannot be $-p^j$.

This last case shows that for $d = 2^i$ the only solutions are those given in congruence (5.1), i.e., $H^{(1)}(x_1) = -1$, $H^{(1)}(x_t) = p^j$ for all proper divisors t of d and $H^{(1)}(x_d) = \pm p^j$. Since d odd was handled previously the only remaining possibility is that d has both even and odd divisors. Here, since $r = 2$, $s = d/4$ cannot occur, $s = 0$ at the $d/2$ level and both $\pm p^j$ satisfy congruence (5.2). However when r is odd, it follows from the discussion above that $H^{(1)}(x_{d/r}) = H^{(1)}(x_d) = p^j$ when $s = 0$ and $H^{(1)}(x_{d/r}) = H^{(1)}(x_d) = -p^j$ for $s = d/2r$. Thus, there are two possibilities. Either $H^{(1)}(x_t) = p^j$ for all divisors $t(\neq 1)$ of d or $H^{(1)}(x_t) = -p^j$ whenever 2^a divides t and $H^{(1)}(x_t) = p^j$ for all the other divisors $t(\neq 1)$ of d. These are, then, the two solutions of congruence (5.1), as can be seen by substituting primitive t-th roots of unity in that congruence. Thus the induction is complete and we finally arrive at

$$H^{(1)}(x) \equiv p^j x^s - \frac{p^j + 1}{N}(1 + x + \cdots + x^{N-1}) \qquad (\text{mod } x^N - 1),$$

where $s = 0$ or $N/2$. [As we shall see later, $s = 0$ unless N is even and $(p^j + 1)/N$ is odd.]

To compute the $\eta_i^{(m)}$ for the sequence of codes with parameters $((p^{2jm} - 1)/N, 2jm)$, we use formula (3.4) in McEliece and Rumsey (1972), with β a complex primitive N-th root of unity, viz.,

$$\eta_i^{(m)} = -\frac{1}{N} \sum_{t=0}^{N-1} \beta^{-it} \omega_t^m, \tag{5.3}$$

where $\omega_t = -H^{(1)}(\beta^t)$. [This formula is an immediate consequence of congruence (2.1) above.] When $s = 0$, $\omega_0 = -H^{(1)}(1) = 1$, $\omega_1 = \cdots = \omega_{N-1} = -H^{(1)}(\beta) = -p^j$ and when $s = N/2$, $\omega_0 = 1$, $\omega_1 = \omega_3 = \cdots = \omega_{N-1} = p^j$, $\omega_2 = \omega_4 = \cdots = \omega_{N-2} = -p^j$. Thus, we calculate that, with a

single exception, the $\eta_i^{(m)} = ((-1)^m p^{jm} - 1)/N$ and the exceptional value is $((-1)^{m+1}(N-1)p^{jm} - 1)/N$. The exceptional η is $\eta_0^{(m)}$ unless $s = N/2$ and *m is odd*, in which case it is $\eta_{N/2}^{(m)}$. To calculate the *weights* of these codes, we note that the $\eta_i^{(m)}$ here are rational integers and so [from $\eta(\xi) = \sum_{i=0}^{p-1} a_i \zeta^i$] it follows that every nonzero element occurs equally often in the code words. We arrive at the following:

THEOREM 6. *Let C be an (n, k) irreducible cyclic code over F_p with $Nn = p^k - 1 = q - 1$, $N > 2$. If there exists a divisor j of $k/2$ for which $p^j \equiv -1 \pmod N$, then there are only two distributions of elements from F_p which occur in the nonzero codewords of C: (caution, as noted above, if $k \neq \operatorname{ord}_n p$ this code is degenerate).*

Class s. (Containing n codewords)

$$N_0 = \frac{q-1}{pN} + \frac{1 - p + u(1-p)(N-1)\sqrt{q}}{pN},$$

$$N_i = \frac{q-1}{pN} + \frac{1 + u(N-1)\sqrt{q}}{pN} \qquad i = 1,\ldots, p-1.$$

Class *. [containing $n(N-1)$ codewords]

$$N_0 = \frac{q-1}{pN} + \frac{1 - p - u(1-p)\sqrt{q}}{pN},$$

$$N_i = \frac{q-1}{pN} + \frac{1 - u\sqrt{q}}{pN} \qquad i = 1,\ldots, p-1.$$

Here N_i is the number of times i occurs in the codeword, and $u = \pm 1$. For any particular code this sign is determined uniquely by the requirement that *all* the N_i must be nonnegative integers.

Note that the formulas for the N_i have been arranged so as to clearly show their deviation from the expected value $(q-1)/pN$. Also, from the derivation above it follows that $u = (-1)^m$. However, since the weight distribution can be uniquely determined from the fact that all the N_i's must be nonnegative integers, there is no need to determine explicitly the value of m in any particular case.

Remark. A similar result holds for irreducible cyclic codes over $GF(q)$ for arbitrary prime powers q, but since the proof involves character sums instead of the exponential sums η, we will not present it. Theorem 6 for $p = 2$ was proved by Delsarte and Goethals (1970).

The above computation of the weight distribution in this "semiprimitive" case was meant to demonstrate the general methods which we shall need for the examples of Section 6. However, the semiprimitive case can easily be handled in a less synthetic fashion and since it provides additional insight into the answers we present this derivation here. Clearly it is only necessary to compute $H^{(1)}(x)$ since the weight distribution is derived from $H^{(1)}(x)$ exactly as above.

LEMMA. *In the semiprimitive case, with* $N > 2$,

$$H^{(1)}(x) \equiv p^j x^s - \frac{p^j + 1}{N}(1 + x + \cdots + x^{N-1}) \qquad (\text{mod } x^N - 1)$$

with $s = 0$ *unless* N *is even and* $(p^j + 1)/N$ *is odd; then* $s = N/2$.

Proof. First consider what happens when $N = p^j + 1$. Here $n = p^j - 1$, $\psi^N = \theta$ generates the multiplicative group of $GF(p^j)$ and, of course,

$$\eta_i = \zeta^{\mathrm{Tr}(\psi^i)} + \zeta^{\mathrm{Tr}(\psi^i\theta)} + \cdots + \zeta^{\mathrm{Tr}(\psi^i\theta^{n-1})}.$$

Now $\mathrm{Tr}(\xi\,\cdot)$ is a linear functional on $GF(p^j)$ and for y in $GF(p^j)$ we have $\mathrm{Tr}(\xi \cdot y) = T_1^j((\xi + \xi^{p^j}) \cdot y)$, where T_1^j denotes the trace from $GF(p^j)$ to F_p. Since T_1^j is a *nontrivial* linear functional so is $\mathrm{Tr}(\xi\,\cdot)$ unless ξ satisfies $x^{p^j} + x = 0$. Thus $\eta_i = -1$ unless ψ^i satisfies $x^n + 1 = 0$. The solutions of this equation constitute a coset of the nonzero elements of $GF(p^j)$ in the multiplicative group of $GF(p^{2j})$ since ψ^{i+N} is a solution whenever ψ^i is, and so the linear functional $\mathrm{Tr}(\psi^i\,\cdot)$ is trivial for precisely one value of i, $0 \leqslant i \leqslant N - 1$. When N is even, it follows from $-1 = \psi^{(q-1)/2} = (\psi^{N/2})^n$ that this distinguished value is $i = N/2$ and so $\eta_{N/2} = n = p^j - 1$. When $N = p^j + 1$ is odd $p = 2$ necessarily, thus $-1 = +1 = \psi^{q-1} = (\psi^N)^n$ and so $\eta_0 = n$. Thus $H^{(1)}(x)$ has the desired structure in the special case $N = p^j + 1$.

If N is a proper divisor of $p^j + 1$ observe that $H^{(1)}$ can be computed by reducing the solution for $p^j + 1$ modulo $x^N - 1$. From this, the lemma follows.

Finally we consider the case $N = 2$. Here, when m is even (say $m = 2v$), we have, in reality, the semiprimitive case with $H^{(2)}(x)$ the basic polynomial and v playing the role of m. $H^{(2)}(x)$ is easily computed by means of the Davenport–Hasse result [i.e., from congruence (2.1)] from the value of $H^{(1)}(x)$ given in Section 2 above. With $p^* = (-1)^{(p-1)/2}p$, $\zeta = \exp(2\pi i/p)$,

$\eta_0 = \sum \zeta^a$, $\eta_1 = \sum \zeta^b$, where a ranges over the nonzero squares and b ranges over the nonzero nonsquares of $GF(p)$, it follows that

$$\begin{aligned}
2H^{(1)}(x) &= 2\eta_0 + 2\eta_1 x \equiv \sqrt{p^*} - 1 - (\sqrt{p^*} + 1)x && (\text{mod } x^2 - 1),\\
2H^{(2)}(x) &\equiv -p^* - 1 + (p^* - 1)x && (\text{mod } x^2 - 1),\\
2H^{(2v)}(x) &\equiv -(p^*)^v - 1 + [(p^*)^v - 1]x && (\text{mod } x^2 - 1),\\
2H^{(2v+1)}(x) &\equiv [(p^*)^v + 1]\eta_0 - [(p^*)^v - 1]\eta_1 \\
&\quad + \{[(p^*)^v + 1]\eta_1 - [(p^*)^v - 1]\eta_0\}x && (\text{mod } x^2 - 1).
\end{aligned}$$

Thus $\eta_0^{(2v)}$ is always one of $(p^v - 1)/2$, $(-p^v - 1)/2$ and $\eta_1^{(2v)}$ takes the other value. Similarly $2\eta_0^{(2v+1)}$ and $2\eta_1^{(2v+1)}$ share the values

$$(p^v + 1)\,\eta_0 - (p^v - 1)\,\eta_1 \qquad \text{and} \qquad (p^v + 1)\,\eta_1 - (p^v - 1)\,\eta_0\,.$$

So we have

THEOREM 7. *Let C be an irreducible cyclic code with $N = 2$, $q = p^m$, $n = (q - 1)/2$. Then, there are n nonzero codewords of C with each of the following distributions of elements from F_p. For m even*

$$\begin{aligned}
N_0 &= \frac{q-1}{2p} + \frac{(1-p)(1+\sqrt{q})}{2p},\\
N_i &= \frac{q-1}{2p} + \frac{1+\sqrt{q}}{2p} \qquad i = 1,\ldots, p-1,
\end{aligned}$$

and

$$\begin{aligned}
N_0 &= \frac{q-1}{2p} + \frac{(1-p)(1-\sqrt{q})}{2p},\\
N_i &= \frac{q-1}{2p} + \frac{1-\sqrt{q}}{2p} \qquad i = 1,\ldots, p-1,
\end{aligned}$$

where N_j denotes the number of times j appears in the codeword. For m odd one distribution is

$$\begin{aligned}
N_0 &= \frac{q-1}{2p} + \frac{1-p}{2p},\\
N_a &= \frac{q-1}{2p} + \frac{1+\sqrt{(pq)}}{2p} \qquad a \text{ a nonzero square of } F_p,\\
N_b &= \frac{q-1}{2p} + \frac{1-\sqrt{(pq)}}{2p} \qquad b \text{ a nonzero nonsquare of } F_p,
\end{aligned}$$

and in the other distribution the values for N_a and N_b are interchanged.

6. More Examples

(a) $p = 2, N = 35$.

Since $\text{ord}_N(p) = 12$ we have $(n, k) = (117, 12)$, and since $\phi(35) = 24$, Theorem 3 above tells us that the ideal (2) splits into a product of $K = 2$ prime ideals in Q_{35}. Now, for each divisor d of 35, let $H_{[d]}$ denote the value of $H(x) = H^{(1)}(x) \pmod{x^d - 1}$. Then

$$H_{[1]} = -1 \qquad \text{(Theorem 1)},$$

$$H_{[5]} = 51 - 13x - 13x^2 - 13x^3 - 13x^4 \qquad \text{(By the semiprimitive case)},$$

$$H_{[7]} = -7 - 23x - 23x^2 + 25x^3 - 23x^4 + 25x^5 + 25x^6$$

[by the remarks in Section 3 and by the calculation at the end of Section 3 in McEliece and Rumsey (1972). This assumes the primitive root ψ in $GF(2^{12})$ has been chosen properly.]

Now if β is a primitive 35-th root of unity, the corollary to Theorem 1 gives $H(\beta)\overline{H(\beta)} = 2^{12}$; and the corollary to Theorem 4 tells us that 2^5 divides $H(\beta)$, but 2^6 does not. Now since $(2) = P\bar{P}$ in the quadratic subfield Ω of Q_{35} for a prime ideal P, the only possibilities are $(H(\beta)) = P^5\bar{P}^7 = 32\bar{P}^2$ or $P^7\bar{P}^5 = 32P^2$. Now it is easy to verify that

$$2 = (\beta^5 + \beta^{10} + \beta^{20})(\beta^{15} + \beta^{25} + \beta^{30})$$

in Ω, [Reuschle (1875) is a good source for this kind of information], and so $P = (\beta^5 + \beta^{10} + \beta^{20})$ or $(\beta^{15} + \beta^{25} + \beta^{30})$. Since Theorem 5 allows only ± 1 as units of absolute value 1 in Ω, $H(\beta) = \pm 32(\beta^5 + \beta^{10} + \beta^{20})^2$ or else $\pm 32(\beta^{15} + \beta^{25} + \beta^{30})^2$, and thus

$$H(x_{35}) = \pm 32(x^5 + x^{10} + x^{20})^2 \qquad \text{or} \qquad \pm 32(x^{15} + x^{25} + x^{30})^2.$$

To resolve the ambiguity we apply criterion (4.2) above and decide that only the alternative

$$\begin{aligned} H(x_{35}) &\equiv 32(x^5 + x^{10} + x^{20})^2 \\ &\equiv 32(x^5 + x^{10} + 2x^{15} + x^{20} + 2x^{25} + 2x^{30}) \qquad (\text{mod } f_{35}) \end{aligned}$$

will lead to an $H_{[35]}(x)$ with integer coefficients. We omit the calculations, and present the coefficients η_i of $H(x) \pmod{x^{35} - 1}$;

$$\eta_0 = -27, \quad \eta_1 = -11, \quad \eta_3 = 5, \quad \eta_5 = 5, \quad \eta_7 = 5, \quad \eta_{15} = 21;$$

here the subscripts represent a complete set of inequivalent residues mod 35 under the map $j \to 2j$. Thus for example since $13 \equiv 3 \cdot 2^4 \pmod{35}$ $\eta_{13} = \eta_3 = 5$. Correspondingly the weights of the codewords are: $W_0 = 72$, $W_1 = 64$, $W_3 = 56$, $W_5 = 56$, $W_7 = 56$, $W_{15} = 48$ and so the codeword weight enumerator for the (117, 12) irreducible cyclic code is

$$A(x) = 1 + 351x^{48} + 2223x^{56} + 1404x^{64} + 117x^{72}.$$

(b) $p = 3$, $N = 11$.

Since $(p - 1, N) = 1$, the sums $H(\beta)$ lie in Q_{11}. $3^5 \equiv 1(11)$ and so $(n, k) = (22, 5)$. $\phi(11) = 10$ so $K = 2$ and $[\Omega : Q] = 2$. Thus in Ω, $(3) = P_1P_2$ for prime ideals P_i. In Theorem 4 we can choose $a_1 = 1$, $a_2 = 2$; we compute $w_3(22) = 4$, $w_3(44) = 6$ and so by Theorem 4, if β is a primitive 11-th root of unity, $(H(\beta)) = P_1^2P_2^3 = 9P_2$. To actually find P_1 and P_2 we make use of the quadratic (period) equation defining $\Omega : z^2 + z + 3 = 0$, where $z = \beta + \beta^3 + \beta^4 + \beta^5 + \beta^9$. Thus we are free to assume that $P_2 = (z)$ and so $H(\beta) = \pm 9z$; i.e., $H(x_{11}) = \pm 9(x + x^3 + x^4 + x^5 + x^9)$. To resolve the ambiguity in the sign we use congruence (4.2) and $H_{[1]} = -1$. So we calculate $H(x) = 4 - 5x + 4x^2 - 5x^3 - 5x^4 - 5x^5 + 4x^6 + 4x^7 + 4x^8 - 5x^9 + 4x^{10} \pmod{x^{11} - 1}$. Hence the code has $6 \times 22 = 132$ words with distribution $N_0 = 10$, $N_1 = 6$, $N_{-1} = 6$ and $5 \times 22 = 110$ words with distribution $N_0 = 4$, $N_1 = N_{-1} = 9$.

7. Two Tables

According to the result of McEliece and Rumsey (1972), the calculation of the weight distribution of any irreducible cyclic code over $GF(p)$ with a fixed $N = (p^k - 1)/n$ is reduced to a calculation in $GF(p^{k_0})$, where $k_0 = \text{ord}_N(p)$. In this paper we have seen that this calculation can in fact be done in a K-th degree subfield of the cyclotomic field Q_N, where $k_0K = \phi(N)$ [at least when $(p^{k_0} - 1)/(p - 1) \equiv 0 \pmod{N}$], and that if N divides an integer of the form $p^j + 1$ the calculation can be done explicitly. We should admit that while these results in principle apply to every N and p, so far we have only successfully applied these techniques where $K = 1$ or 2.

Thus for $p = 2$, the H-polynomial [i.e., $H^{(1)}(x)$] can be computed if (a) k_0 is small enough so that the calculation in $GF(2^{k_0})$ can be carried out directly, (b) if $2^j \equiv -1 \pmod{N}$ for some j, or (c) if $\phi(N) = 2k_0$. The smallest N which cannot be handled by any of these methods is $N = 187$, for which $K = 4$, $k_0 = 40$. Table I gives all of these H-polynomials for

$N < 100$. In Table I a considerably condensed format has been adopted, which is best explained by example. Thus consider the entry $N = 51$: (0, 5)(1, 1)(3, 1)(5, −3)(9, −3)(11, 1)(17, 5)(19, 1). This means that if we set $H^{(1)}(x) \equiv \eta_0 + \eta_1 x + \cdots + \eta_{50} x^{50} \pmod{x^{51} - 1}$, that $\eta_0 = 5$, $\eta_1 = 1$, $\eta_3 = 1$, $\eta_5 = -3, \ldots, \eta_{19} = 1$. To find an η_j not listed, one uses the relation $\eta_j = \eta_{2j}$; e.g., $\eta_{41} = \eta_{11} = 1$ since $41 \equiv 11 \cdot 2^6 \pmod{51}$. Also, because of the complete solution to the weight distribution problem in the semiprimitive case given in Section 5, we omit those values of N which divide an integer

TABLE I

Binary H-Polynomials, $N < 100$ (See text for key)

N	$H(x)$
7	(0, −1)(1, 1)(3, −1)
15	(0, 1)(1, 1)(3, −1)(5, 1)(7, −1)
21	(0, −1)(1, −1)(3, 3)(5, −1)(7, 3)(9, −1)
23	(0, −23)(1, −7)(5, 9)
31	(0, −1)(1, 1)(3, 1)(5, −1)(7, −1)(11, −1)(15, 1)
35	(0, −27)(1, −11)(3, 5)(5, 5)(7, 5)(15, 21)
39	(0, 41)(1, 9)(3, −7)(7, −7)(13, 9)
45	(0, −5)(1, −5)(3, 19)(5, 11)(7, 3)(9, −13)(15, −5)(21, −13)
47	(0, −2255)(1, −207)(5, 305)
49	(0, −337)(1, 47)(3, −81)(7, 687)(21, −337)
51	(0, 5)(1, 1)(3, 1)(5, −3)(9, −3)(11, 1)(17, 5)(19, 1)
55	(0, −391)(1, −135)(3, 121)(5, 121)(11, −135)
63	(0, 1)(1, 1)(3, 1)(5, −1)(7, 1)(9, 1)(11, −1)(13, 1)(15, −1)(21, −1)(23, −1)(27, 1)(31, −1)
69	(0, 1651)(1, 115)(3, 115)(5, −141)(15, −141)(23, −397)
71	(0, 169609)(1, 5769)(7, −10615)
73	(0, −1)(1, −1)(3, −1)(5, −1)(9, −1)(11, −1)(13, −1)(17, 7)(25, −1)
75	(0, 541)(1, 29)(3, −67)(5, 221)(7, −3)(15, 29)(25, 221)(35, −291)
77	(0, 27515)(1, −133)(3, 891)(7, −5253)(11, −133)(33, 891)
79	(0, 452945)(1, 59729)(3, −71343)
85	(0, 3)(1, −1)(3, −1)(5, −1)(7, 3)(9, −1)(13, 3)(15, −1)(17, 3)(21, −1)(29, −1)(37, −1)
87	(0, 13465)(1, 1177)(3, −871)(5, −871)(29, 1177)
89	(0, −1)(1, −1)(3, 7)(5, 7)(9, −1)(11, −1)(13, −9)(19, −1)(33, −1)
91	(0, 29)(1, −3)(3, −3)(7, −3)(9, −3)(11, −3)(13, −3)(17, 13)(19, −3)(39, 13)
93	(0, −9)(1, −1)(3, 7)(5, −5)(7, −1)(9, 3)(11, 3)(15, 3)(17, −1)(21, −5)(23, 3)(31, −1)(33, −1)(45, −1)
95	(0, 42081)(1, 25697)(5, 9313)(7, −23455)(19, −72607)

Table II: Complete Weight Enumerators for all Binary Irreducible Cyclic Codes,
With $n < 10^5$, $N < 100$
(See text for key)

n	k	N	Weight Enumerator
1	1	1	1^1
3	2	1	2^1
5	4	3^s	$2^2 4^1$
7	3	1	4^1
9	6	7	$2^1 4^3 6^3$
11	10	93	$2^5 4^{30} 6^{42} 8^{15} 10^1$
15	4	1	8^1
17	8	15	$6^4 8^5 10^4 12^2$
21	6	3^s	$8^1 12^2$
23	11	89	$8^{22} 12^{56} 16^{11}$
31	5	1	16^1
33	10	31	$12^5 14^5 16^5 18^{10} 20^5 22^1$
45	12	91	$8^1 16^{15} 24^{75}$
51	8	5^s	$24^4 32^1$
63	6	1	32^1
65	12	63	$26^6 28^7 30^{12} 32^{12} 34^6 36^9 38^8 40^3$
73	9	7	$28^1 36^3 40^3$
85	8	3^s	$40^2 48^1$
89	11	23	$40^{11} 48^{11} 56^1$
91	12	45	$36^4 40^6 44^{12} 48^{15} 52^8$
93	10	11^s	$32^1 48^{10}$
105	12	39	$32^1 48^{14} 56^{24}$

n	k	N	Weight Enumerator
8191	13	1	4096^1
9709	18	27^s	$4608^1 4864^{26}$
11275	20	93	$5384^1 5576^{10} 5600^{10} 5608^5 5616^{10} 5624^{20} 5648^5 5672^2 5680^{15} 5688^{10} 5760^5$
12483	18	21	$6144^3 6176^1 6240^{12} 6304^3 6336^2$
13107	16	5^s	$6528^4 6656^1$
13797	18	19^s	$6656^1 6912^{18}$
16383	14	1	8192^1
19065	20	55	$9472^{30} 9600^{24} 9728^1$
21845	16	3^s	$10880^2 11008^1$
25575	20	41^s	$12288^1 12800^{40}$
29127	18	9^s	$14336^1 14592^8$
31775	20	33^s	$15872^{32} 16384^1$
32767	15	1	16384^1
33825	20	31	$16728^1 16760^5 16872^5 16912^5 16960^5 17000^5 17008^5$
37449	18	7	$18624^3 18784^3 18848^1$
41943	20	25^s	$20480^1 20992^{24}$
42799	21	49	$21056^3 21376^{21} 21440^{21} 21568^4$
47127	22	89	$23328^{11} 23520^{23} 23552^{11} 23584^{11} 23648^{11} 23680^{22}$
60787	22	69	$29568^1 30336^{33} 30464^{33} 30592^2$
65535	16	1	32768^1
69905	20	15	$34624^1 34880^4 34912^2 34960^4 35120^4$
87381	18	3^s	$43520^1 43776^2$
95325	20	11^s	$47616^{10} 48128^1$
131071	17	1	65536^1

n	k	N	Weight Enumerator
117	12	35	$48^3 56^{19} 64^{12} 72^1$
127	7	1	64^1
195	12	21	$88^6 96^5 104^{10}$
255	8	1	128^1
273	12	15	$120^2 132^4 140^4 144^5$
315	12	13^s	$128^1 160^{12}$
341	10	3^s	$160^1 176^2$
381	14	43^s	$128^1 192^{42}$
455	12	9^s	$224^8 256^1$
511	9	1	256^1
585	12	7	$280^3 296^1 304^3$
771	16	85	$360^8 376^{24} 384^{17} 392^{24} 408^8 416^4$
819	12	5^s	$384^1 416^4$
1023	10	1	512^1
1057	15	31	$484^1 504^5 520^5 532^5 540^{10} 544^5$
1285	16	51	$616^8 632^8 640^{16} 648^8 664^8 672^2 704^1$
1365	12	3^s	$672^2 704^1$
2047	11	1	1024^1
3591	18	73	$1760^{28} 1792^9 1824^{36}$
3855	16	17^s	$1920^{16} 2048^1$
4095	12	1	2048^1
4161	18	63	$2000^3 2028^6 2052^8 2072^7 2088^9 2100^{12} 2108^6 2112^{12}$
4369	16	15	$2144^4 2184^4 2192^2 2200^4 2272^1$
4599	18	57^s	$2048^1 2304^{56}$
4681	15	7	$2320^3 2336^3 2416^1$
5461	14	3^s	$2688^1 2752^2$

n	k	N	Weight Enumerator
178481	23	47	$89088^{23} 89344^{23} 90368^1$
182361	22	23	$90752^1 91008^{11} 91392^{11}$
184365	24	91	$91776^{12} 92032^{24} 92288^{37} 92416^{15} 92544^3$
197379	24	85	$98304^5 98336^8 98528^{16} 98624^8 98720^{16} 98784^8 98912^8 98976^8 99008^8$
209715	20	5^s	$104448^1 104960^4$
258111	24	65^s	$129024^{64} 131072^1$
262143	18	1	131072^1
266305	24	63	$132432^1 132760^2 132888^6 132920^6 132992^6 133040^6 133120^6 133160^6 133200^6$ $133320^6 133472^3 133560^6 133680^3$
299593	21	7	$149440^1 149632^3 150080^3$
328965	24	51	$163584^1 163968^2 164064^8 164448^8 164480^8 164640^8 164736^8 164768^8$
349525	20	3^s	$174592^2 175104^1$
372827	24	45	$185952^4 185984^1 186144^{12} 186464^4 186496^{12} 186560^6 186976^4 187008^2$
430185	24	39	$214656^{12} 215168^{12} 215296^{12} 215552^1 215808^2$
479349	24	35	$239232^4 239360^3 239488^{12} 239744^1 239872^{12} 240512^3$
524287	19	1	262144^1
798915	24	21	$397952^1 399232^6 399360^2 399488^6 399872^3 400000^3$
986895	24	17^s	$491520^1 493568^{16}$

of the form $2^j + 1$; i.e., $N = 3, 5, 9, 11, 13, 17, 19, 25, 27, 33, 37, 41, 43, 53, 57, 59, 61, 65, 67, 81, 83, 97, 99$.

Finally, in Table II we give the complete weight enumerators for the 89 irreducible binary cyclic codes with $N < 100$ and $n < 1000000$, listed in order of increasing n. In such codes, the nonzero codewords divide themselves into N equivalence classes of n words each under the cyclic shift. The enumerator tells how many of these equivalence classes have each weight. Thus, for the (23, 11) $N = 89$ code the entry $8^{22}12^{56}16^{11}$ means that there are 22×23 words of weight 8, 56×23 of weight 12, and 11×23 of weight 16. A superscript "s" on a value of N means that N divides $2^j + 1$, and so only two different weights occur, according to Delsarte and Goethals (1970), or Section 5.

References

BAUMERT, L. D. (1971), "Cyclic Difference Sets," Springer-Verlag, Berlin.

DELSARTE, P., AND GOETHALS, J.-M. (1970), "Irreducible Binary Cyclic Codes of Even Dimension," U. North Carolina, Dept. Statistics Mimeo, Series No. 600.27.

LANG, S. (1970), "Algebraic Number Theory," Addison-Wesley, Reading.

MANN, H. B. (1955), "Introduction to Algebraic Number Theory," Ohio State University Press, Columbus.

MCELIECE, R. J., AND RUMSEY, H., JR. (1972), Euler products, cyclotomy, and coding, *J. Number Theory*, to appear.

REUSCHLE, C. G. (1875), "Tafeln Complexer Primzahlen, Welche aus Wurzeln der Einheit Gebildet Sind," Königl. Akademie der Wissenschaften, Berlin.

STICKELBERGER, L. (1890), Über eine Verallgemeinerung der Kreisteilung, *Math. Ann.* **37**, 321.