MATHEMATICS OF COMPUTATION
VOLUME 46, NUMBER 173
JANUARY 1986, PAGES 341–354

Weight Distributions of Some Irreducible Cyclic Codes

By Robert Segal and Robert L. Ward

Abstract. The theory of weight distributions of irreducible cyclic codes over a finite field has been extensively developed by R. J. McEliece and others. We apply that theory to compute the weight enumerators of some binary codes which have hitherto not been possible. In so doing, we correct an error by McEliece and describe his process in somewhat more detail.

1. Introduction. Given a prime p and a natural number N not a multiple of p, let k be the order of p modulo N, denoted $k = \operatorname{ord}_N p$. Set $q = p^k$ and $n = (q-1)/N$. Then there is an irreducible polynomial of degree k over GF(q) which has N cycles of length n (and the zero cycle of length 1). These cycles are equivalence classes of n-tuples of the form

$$\left(T(\xi), T(\xi\theta), T(\xi\theta^2), \ldots, T(\xi\theta^{n-1})\right)$$

under the equivalence relation generated by the cyclic shift operator. Here $\xi \in \mathrm{GF}(q)$, θ is a primitive nth root of unity in GF(q), and

$$T(\xi) = \xi + \xi^p + \xi^{p^2} + \cdots + \xi^{p^{k-1}}$$

is the trace function from GF(q) to GF(p). These n-tuples form an (n, k) irreducible cyclic linear error-correcting code. We wish to find the weight enumerator of the code, or the weights of the cycles.

Let $\zeta = e^{2\pi i/p}$, and set

$$\eta(\xi) = \sum_{i=0}^{n-1} \zeta^{T(\xi\theta^i)}.$$

If ψ is a primitive root in GF(q) such that $\psi^N = \theta$, set $\eta_i = \eta(\psi^i)$. Notice that $i \equiv j \pmod N$ implies $\eta_i = \eta_j$. Set up the generating function

$$H(x) = \sum_{i=0}^{N-1} \eta_i x^i \equiv \sum_{\alpha \in \mathrm{GF}(q)^*} x^{\mathrm{ind}(\alpha)} \zeta^{T(\alpha)} \pmod{x^N - 1}.$$

Let $\beta = e^{2\pi i/N}$. Then

$$H(\beta) = \sum_{\alpha \in \mathrm{GF}(q)^*} \beta^{\mathrm{ind}(\alpha)} \zeta^{T(\alpha)}$$

is a *Gauss sum*.

Received January 17, 1985.
1980 *Mathematics Subject Classification*. Primary 94B15; Secondary 12-04, 12A35, 12A45, 12C10.

For each codeword, the frequency of occurrence of the element $y \in \mathrm{GF}(p)$ will be the coefficient of ζ^y in the expression for $\eta(\xi)$. The frequencies will be the same for each of the n codewords in any equivalence class, since they are only cyclic shifts of each other, so we need only find the values of η_i for $0 \leqslant i < N$. This will give us the value for one codeword from each equivalence class.

The η_i values can be determined if we can determine the generating function $H(x)$ modulo $x^N - 1$. This can be done if $H(x)$ is known modulo $\Phi_d(x)$, the cyclotomic polynomial of order d, for each divisor d of N, by Moebius inversion. The hardest part of this is for $d = N$. This can be determined if we know $H(x)$ evaluated at any primitive Nth root of unity, for example, β. Thus we seek to determine $H(\beta)$. As a first step in that direction, we compute the ideal $(H(\beta))$ in the ring of integers of a certain algebraic number field of small degree, as defined below. This can be done using Stickelberger's theorem. Next, we can give a short list of possibilities for the actual value of $H(\beta)$ by considering the units in the ring. Finally, we can shorten the list of possibilities by using the integer coefficient criterion of Baumert, together with the known $H(x)$'s for divisors of N. Each of these possibilities remaining will lead to a possibly different generating function $H(x)$, but all will finally give the same weight enumerator for the code. In fact, there will be an isomorphism of the code which will carry any generating function found in this way into any other, which is induced by a change in the choice of the nth root of unity θ.

2. Applying Stickelberger's Theorem. The quantity $H(\beta)$ whose value we seek lies in $\mathbf{Q}(\beta, \zeta)$, a cyclotomic number field generated by the Npth roots of unity. Baumert and McEliece have shown [1, Corollary to Theorem 2] that if $(q-1)/(p-1) \equiv 0 \pmod{N}$, then $H(\beta)$ lies in a subfield Ω of $\mathbf{Q}(\beta)$ whose degree over $\mathbf{Q}$ is $K = \phi(N)/k$. In fact, Ω is merely the fixed field of the Frobenius automorphism of $\mathbf{Q}(\beta)$ over $\mathbf{Q}$ defined by $\lambda_p(\beta) = \beta^p$. More precisely, $H(\beta)$ lies in the ring of integers of the field Ω, which we denote by O_Ω.

Another useful fact given by Baumert and McEliece [1, Corollary to Theorem 1] is that $H(\beta)\overline{H(\beta)} = p^k$. This implies that the prime ideal divisors of the ideal $(H(\beta))$ in the ring O_Ω are among the prime ideal divisors of the ideal (p).

We are thus interested in knowing what the decomposition of (p) into prime ideal factors in O_Ω might be. Once again, Baumert and McEliece give the answer to this question [1, Theorem 3]. In O_Ω, (p) decomposes into a product of K distinct prime ideal factors. They can be labelled $P_1, P_2, \ldots, P_K$ in such a way that under the automorphism λ_a of Ω over $\mathbf{Q}$ defined by $\lambda_a(\beta) = \beta^a$, the P_i's are permuted according to the rule $\lambda_a(P_i) = P_j$ if $\lambda_{a_i} = \lambda_{-a}\lambda_{a_j}$. Here the a_i's are a complete set of K coset representatives of the cyclic subgroup generated by p in the multiplicative group of units modulo N, which is isomorphic to the Galois group of $\mathbf{Q}(\beta)$ over $\mathbf{Q}$. The quotient group is isomorphic to the Galois group of Ω over $\mathbf{Q}$.

Here we must call attention to a misprint in [1], which gives a different numbering than the above, defined by $\lambda_{a_j} = \lambda_a\lambda_{a_i}$. This slip would have no effect at this point, but would make the application of Stickelberger's theorem incorrect whenever one of the elements of the Galois group had order greater than two.

We have now established sufficient notation to state

STICKELBERGER'S THEOREM. *There is a labelling of prime ideals consistent with the above notation such that*

$$(H(\beta)) = \prod_{i=1}^{K} P_i^{w_p(a_i n)/(p-1)},$$

where, if $z = \sum z_i p^i$, *with* $0 \leqslant z_i < p$, *then* $w_p(z) = \sum z_i$.

Now let us describe the computational procedure we use to solve those cases we can with these tools.

Start with the given values of N and p. Compute k, q, n, $\phi(N)$, and K. Next we want to know the structure of the Galois group of Ω over $\mathbf{Q}$, so we find the subgroup generated by p of the multiplicative group of units modulo N, and a complete set $\{a_i\colon 1 \leqslant i \leqslant K\}$ of coset representatives. The group structure of the Galois group is then apparent, since the parameters we have chosen insure that its order K will be small (usually 4 or 6). We then construct the lattice of subfields of Ω, and attempt to factor the ideal (p) in the rings of integers of an increasing tower of subfields by applying

KUMMER'S THEOREM. *Let E be a separable simple field extension of F, $E = F(\omega)$, $f(x)$ the minimal polynomial of ω over F, $\{1, \omega, \ldots, \omega^{n-1}\}$ an integral basis for O_E over O_F, and let P be a prime ideal in O_F. Then the irreducible factorization of $f(x)$ over O_F/P is of the form*

$$f(x) = \prod_{i=1}^{r} G_i(x)^{e_i},$$

where r is the number of prime ideals Q_i lying over P in O_E, $G_i(x) \neq G_j(x)$ for $i \neq j$, $\deg G_i(x)$ is the degree of Q_i over P, and e_i is the ramification index of Q_i over P. Moreover, if $g_i(x) \in O_F[x]$ is a monic polynomial such that $g_i(x) \equiv G_i(x) \pmod{P}$, then

$$PO_E = \prod_{i=1}^{r} (P, g_i(\omega))$$

is the factorization of PO_E into prime ideals in O_E [3, 4-9-1, *p.* 168].

The application of this theorem takes the following form. Start in $\mathbf{Q}$, and pass to a quadratic extension. Find a simple generator of the field, call it ω. Find the minimal polynomial of ω and factor it modulo p. Find a monic polynomial with coefficients in $\mathbf{Z}$ which is congruent to each factor mod p. Use each of these polynomials together with p as generators of all ideals lying over (p). This gives the prime ideals in a quadratic extension of $\mathbf{Q}$. Next, try to extend each of these ideals by the same process to the next level of extension also using Kummer's theorem. For quadratic extensions, this is no problem, but for higher degrees, one must verify that an integral basis of powers of ω exists, which may be false.

If this fails, the next fall-back is to cast about in O_Ω for random elements, looking for a z whose norm

$$N_{\Omega/\mathbf{Q}}(z) = \prod_{i=1}^{K} \lambda_{a_i}(z)$$

(which lies in $\mathbf{Z}$) contains p to exactly the first power in its prime factorization. Then the ideal $I = (z, p)O_\Omega$ must have norm

$$N_{\Omega/\mathbf{Q}}(I) = \prod_{i=1}^{K} \lambda_{a_i}(I),$$

exactly $(p)\mathbf{Z}$, a prime ideal in $\mathbf{Z}$, and hence be a prime ideal $P_1 = I$. The remaining prime ideals P_i can then be obtained by applying the automorphisms from the known Galois group. In either case, the numbering is assigned according to the scheme described above.

Notice that here we have a K-fold ambiguity in the choice of P_1, corresponding to applications of the K automorphisms of the Galois group.

Once we have successfully identified the prime ideals P_i, we can multiply their appropriate powers given in Stickelberger's theorem and obtain a representation for the ideal $(H(\beta))$ in terms of its generators. Unfortunately, although we know in advance that the ideal is principal, in general we are left with a set of K generators, and no good way to find a single generator of which they are all multiples.

An alternative is to borrow an idea from Dedekind via an example in Weiss [3, p. 170]. Search for principal ideals with norms of the form p^a for some a. First we want to find an integral basis for O_Ω over $\mathbf{Q}$. We can begin by considering the basis of integers

$$B = \{\lambda_{a_i}(z): 1 \leqslant i \leqslant K\},$$

and triangularize it by an integral row-reduction process, to get a new version of B. Next we construct all the characters of the Galois group of Ω over $\mathbf{Q}$ and their conductors, whose product is then the absolute value of the discriminant of Ω over $\mathbf{Q}$, $\Delta_{\Omega/\mathbf{Q}}$. Given this number, we can test whether the basis of integers B forms an integral basis. This has been successful in all examples worked so far, though a proof is lacking. If B is not an integral basis, we can find what rational prime factors are missing from the denominators of the integers in a triangularized version of B, and find a true integral basis. Say $B = \{b_i: 1 \leqslant i \leqslant K\}$. Now we can take

$$z = \sum_{i=1}^{K} c_i b_i, \qquad c_i \in \mathbf{Z},$$

as generators for principal ideals (z) and compute their norms, selecting those whose norms are of the form p^a.

We then factor the ideal (z) into powers of the prime ideals P_i by using the following technique. Compute $A_{ij} \in \mathbf{Z}$ such that $\lambda_{a_i}(z) \equiv A_{ij} \pmod{P_j^t}$ for some moderate value of t (say 16). Now

$$(z) = \prod_{j=1}^{K} P_j^{e_j},$$

where

$$p^{e_j} = \text{g.c.d.}\left(\sum_{i=1}^{K} c_i A_{ij}, p^t \right),$$

if $e_j \leqslant t$. We can also use the additional fact that $a = \sum_{j=1}^{K} e_j$ in case one $e_j > t$.

Once a long enough list of useful factorizations of ideals has been compiled, the matrices

$$M_1 = \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_r \end{bmatrix} \quad \text{and} \quad M_2 = \begin{bmatrix} e_1(z_1) & \cdots & e_K(z_1) & a(z_1) \\ e_1(z_2) & \cdots & e_K(z_2) & a(z_2) \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ e_1(z_r) & \cdots & e_K(z_r) & a(z_r) \end{bmatrix},$$

whose rows contain the elements z_i and the corresponding exponents e_j and a, hold much information concerning products of powers of the prime ideals P_j which are principal. Now, addition or subtraction of two rows of M_2 corresponds to multiplication or division of the corresponding principal ideals, and hence, to multiplication or division of their generators z_i appearing in the same row of M_1. An interchange of two rows of M_1 and M_2 corresponds to an interchange of the ideal generators z_i. Thus we can perform additive row operations on M_2 as long as we perform the corresponding multiplicative row operations on M_1. We do this in such a way that we create a row in M_2 of the form

$$\left[w_p(a_1 n) \cdots w_p(a_K n) \; k/2 \right],$$

and then the corresponding generator in M_1 is a principal generator of the required ideal $(H(\beta))$.

3. Resolving the Unit Ambiguity. Given that we know a generator z of $(H(\beta))$, we wish to calculate the value of $H(\beta)$ itself. In general, this is not possible without some ambiguity. Recall the K-fold ambiguity which was available in our choice of the prime ideal P_1. This is equivalent to an ambiguity in the choice of z in that a conjugate of z, $\lambda_a(z)$, will also work (so far). This gives us a list of at most K possibilities for the value of z. We do know that the equation $H(\beta) = uz$ must hold, where u is a unit in O_Ω.

In order to proceed, we need some detailed information about what the units in O_Ω are. They form a group U about whose structure we know a few facts. U can be decomposed into a direct sum of its torsion subgroup T (consisting of all elements of finite order) with a free group U'. In the case at hand, T is the set of all units of absolute value one, viz., $\pm$ the elements of the cyclic group of all $(p-1, N)$th roots of unity. The remaining part U' is a free group of rank $R = r + s - 1$, where $K = r + 2s$, and $s = 0$ if $\Omega \subseteq \mathbf{R}$. Here r is the number of real isomorphs of Ω, and s is the number of conjugate pairs of complex isomorphs of Ω. This is the Dirichlet unit theorem [3, p. 207]. Thus, we must find what is called a system of fundamental units for the ring of integers of the algebraic number field Ω, that is, a set of generators of U'.

In general, this is a nontrivial task. Much effort has been spent in calculating fundamental units for various algebraic number fields. One can start with units in any of the subfields of Ω. We have employed two techniques for finding units. The first is not particularly elegant or efficient, but has served its purpose. We simply search for integral linear combinations of the integral basis with small coefficients and having norm ± 1. The second is to use the matrices M_i above and to create as many all-zero rows in M_2 as possible. Then the corresponding generators in M_1 will

be units. Once some units are found, others may be generated by multiplying positive or negative powers of known ones together. Redundant ones can be removed from the set until the number of generators remaining is equal to the rank we need.

Actually, as long as we are "close" to having a system of fundamental units, that is good enough for our purposes. We do need to have R independent units, but it suffices to have a set which generates a subgroup of the unit group U' of small finite index. Let $E = \{\varepsilon_1, \ldots, \varepsilon_R\}$ be the set of independent units that are known. There may be units not in the subgroup generated by E, e.g., a square root of ε_i. Then

$$H(\beta) = z\varepsilon_0 \prod_{i=1}^{R} \varepsilon_i^{x_i/x_0},$$

where ε_0 is a unit of absolute value one. We can take absolute values of both sides and then logarithms to any convenient base, and obtain the following Diophantine equation with real coefficients:

$$\sum_{i=1}^{R} x_i \log|\varepsilon_i| = x_0\big(\log|H(\beta)| - \log|z|\big).$$

Now we can use another result of Baumert and McEliece [1]: $|H(\beta)| = q^{1/2}$. The solution we seek consists of an $(R+1)$-tuple of integers $(x_0, \ldots, x_R)$. x_0 must be a divisor of the index of the subgroup of U' generated by E. If E generates U', this guarantees that each x_i/x_0 will be an integer.

The solution of this Diophantine equation may be accomplished by a direct search, since the x_i's tend to be small (and x_0 is usually 1). Another technique which we have used is based on a generalized continued fraction algorithm to find approximate solutions, i.e., sets of integers x_i which make our equation nearly true. With the proper choice of algorithm, we quickly arrive at the correct solution.

There remains the ambiguity in the choice of the torsion unit ε. There are $[2, (p-1, N)]$ choices for ε. Combined with the choices for z, this gives at most $[2, (p-1, N)]K$ possibilities for the value of $H(\beta)$. Some of these will be eliminated as impossible in the next section.

4. Constructing the Generating Function from Its Values. We are now given one of a list of possible values for $H(\beta)$, and wish to construct the generating function $H(x)$ modulo $x^N - 1$, whenever that is possible, and determine when it is not possible. The main tools for this task are the following theorems of Baumert and McEliece [1]:

Semiprimitive Case. If $N > 2$, and there exists a divisor j of $k/2$ for which $p^j \equiv -1 \pmod N$, then

$$H(x) \equiv p^j x^c - \frac{p^j + 1}{N}(1 + x + \cdots + x^{N-1}) \pmod{x^N - 1}$$

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

Quadratic Residue Case. If $N = 2$ and k is even,

$$H(x) \equiv \left\{\left[-(-1)^{k(p-1)/4} p^{k/2} - 1\right]/2\right\} + \left\{\left[(-1)^{k(p-1)/4} p^{k/2} - 1\right]/2\right\} x \pmod{x^2 - 1}.$$

If $N = 2$ and k is odd,

$$H(x) \equiv \left\{\left[(-1)^{k(p-1)/4}p^{k/2} - 1\right]/2\right\} + \left\{\left[-(-1)^{k(p-1)/4}p^{k/2} - 1\right]/2\right\}x \pmod{x^2 - 1}.$$

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

$$H(x) \equiv g_{N/d}(x) \left(\mathrm{mod}\, d, \Phi_{N_1}^{d^{a-1}}(x)\right)$$

for all prime divisors d of N, where $N = d^a N_1$ with $(d, N_1) = 1$.

The idea is to apply these theorems according to the following process. First, compute the values of $H(\beta^{N/d})$, where d ranges over all divisors of N. This is the place that we use the semiprimitive and quadratic residue cases (and possibly the table given by Baumert and McEliece [1] of all $H(x)$ for $N < 100$ with $p = 2$). We then know what $H(x)$ is congruent to modulo $\Phi_d(x)$, call it $H_d(x)$. Next, we apply the integer coefficient criterion to eliminate some of the possibilities for $H(\beta)$. Lastly we reconstruct $H(x)$ modulo $x^N - 1$ by applying the Chinese Remainder Theorem and Moebius inversion:

$$H(x) \equiv \frac{1}{N}\sum_{d|N} H_d(x) \sum_{d'|d} \mu\left(\frac{d}{d'}\right) d' \frac{x^N - 1}{x^{d'} - 1}.$$

The result of this procedure may still be a short list of possibilities for $H(x)$. It can happen that not all the ambiguities in the value of $H(\beta)$ can be removed. This is not a problem, however, as the weight enumerators calculated in the next section will be independent of the remaining choice of $H(x)$.

5. Finding the Weight Enumerator. At this point we know the values of η_i for $0 \leqslant i \leqslant N - 1$. They are polynomials in ζ, say

$$\eta_i = \sum_{j=0}^{p-1} \alpha_{ij}\zeta^j,$$

where α_{ij} is the number of occurrences of the field element j in the ith codeword. Thus the weight of codeword i is $W_i = n - \alpha_{i0}$. We can compute the coefficients α_{i0} in the following way. Let σ_j for $1 \leqslant j \leqslant p - 1$ be the automorphism of $\mathbf{Q}(\zeta)$ over $\mathbf{Q}$ defined by $\sigma_j(\zeta) = \zeta^j$. Then

$$\alpha_{it} = \frac{1}{p}\left(n + \sum_{j=1}^{p-1} \sigma_j(\eta_i)\zeta^{-jt}\right).$$

From this we now know that

$$W_i = n - \frac{1}{p}\left(n + \sum_{j=1}^{p-1} \sigma_j(\eta_i)\right).$$

If η_i is in fact a rational integer, then $\alpha_{i0} = (n + (p - 1)\eta_i)/p$, and

$$W_i = (n - \eta_i)(p - 1)/p.$$

Now we can compute the weight enumerator polynomial

$$A(z) = 1 + n \sum_{i=0}^{N-1} z^{W_i},$$

and we are finished.

6. An Illustrative Example. As an exercise of this method, we solve the case with $N = 187$, $p = 2$.

First we readily find that $k = \operatorname{ord}_{187} 2 = 40$, $q = 2^{40}$, and $n = 5{,}879{,}741{,}325$. Let $\beta = e^{2\pi i/187}$. Its minimum polynomial is $\Phi_{187}(x)$ which has degree $\phi(187) = 160$. Since $p = 2$ and $N | q - 1$, we have $(q-1)/(p-1) \equiv 0 \pmod{N}$, so $H(\beta)$ lies in a subfield Ω of $\mathbf{Q}(\beta)$ of degree over $\mathbf{Q}$, $K = 160/40 = 4$.

We wish to know exactly what the Galois group of Ω over $\mathbf{Q}$ is, and we can do this by explicitly constructing the automorphisms.

They are defined by the equations $\lambda_a(\beta) = \beta^a$, where $(a, 187) = 1$. Since $\lambda_a[\lambda_b(\beta)] = \lambda_{ab}(\beta)$, the Galois group is isomorphic to the multiplicative group of units modulo 187 modulo its subgroup of powers of 2. The cosets have representatives 1, 3, 9, and 27 (among other choices), so it is cyclic, and is generated by λ_3.

We next construct the lattice of fields contained in Ω and containing $\mathbf{Q}$. Since the Galois group has only one element of order two, there must be exactly one subfield which is a quadratic extension of $\mathbf{Q}$. Since the Legendre symbols $(2/11) = -1$ and $(2/17) = +1$, that quadratic extension must be $\mathbf{Q}(\sqrt{17}) = \mathbf{Q}(\omega)$, where $\omega^2 + \omega - 4 = 0$. We introduce ω here because $\{1, \omega\}$ is an integral basis of $O_{\mathbf{Q}(\sqrt{17})}$ over $\mathbf{Z} = O_{\mathbf{Q}}$. Thus the lattice must look like the following diagram.

$$\begin{array}{c} \Omega \\ | \\ \mathbf{Q}(\omega) \\ | \\ \mathbf{Q} \end{array}$$

Next we must try to factor the ideal (p) in the ring O_Ω. Here we can use Kummer's theorem, since each extension field is quadratic over the last, and each ring of integers has a basis consisting of powers of a single element. In fact, if we express Ω as a quadratic extension of $\mathbf{Q}(\omega)$, we find that we can get Ω by adjoining ω_1, where

$$\omega_1^2 + \omega_1 + 22\omega + 58 = 0.$$

Once again, we introduce ω_1 here because $\{1, \omega_1\}$ is an integral basis of O_Ω over $O_{\mathbf{Q}(\omega)} = \mathbf{Z}[\omega]$. Thus $O_\Omega = \mathbf{Z}[\omega, \omega_1]$. Now in $O_{\mathbf{Q}(\omega)}$, we have

$$(2) = (\omega + 2)(\omega - 1),$$

and in O_Ω,

$$(2) = (\omega_1, \omega + 2)(\omega_1, \omega - 1)(\omega_1 + 1, \omega + 2)(\omega_1 + 1, \omega - 1).$$

Kummer's theorem guarantees that these are all prime ideals in O_Ω. Now we arbitrarily pick $P_1 = (\omega_1 + 1, \omega + 2)$. We now compute the effect of λ_3, the generator of the Galois group:

$$\lambda_3(\omega) = -\omega - 1,$$

$$\lambda_3(\omega_1) = 2\omega\omega_1 - 3\omega_1 + \omega - 2.$$

Now we find that

$$P_2 = \lambda_3^3(P_1) = (\omega_1 + 1, \omega - 1),$$
$$P_3 = \lambda_3^2(P_1) = (\omega_1, \omega + 2),$$
$$P_4 = \lambda_3(P_1) = (\omega_1, \omega - 1).$$

We also compute the exponents

$$w_2(n) = 21, \qquad w_2(3n) = 16,$$
$$w_2(9n) = 19, \qquad w_2(27n) = 24,$$

so that

$$(H(\beta)) = P_1^{21}P_2^{16}P_3^{19}P_4^{24}.$$

Now we hunt for principal ideals whose norms are powers of 2. A short search reveals the following:

$$(\omega - 1) = P_2P_4, \qquad (\omega + 2) = P_1P_3,$$
$$(\omega_1 + 2\omega + 3) = P_1^8P_2^2, \qquad (\omega_1 + 2\omega + 6) = P_3^3P_4^5.$$

The matrices M_1 and M_2 now look like

$$M_1 = \begin{bmatrix} \omega - 1 \\ \omega + 2 \\ \omega_1 + 2\omega + 3 \\ \omega_1 + 2\omega + 6 \end{bmatrix} \quad \text{and} \quad M_2 = \begin{bmatrix} 0 & 1 & 0 & 1 & 2 \\ 1 & 0 & 1 & 0 & 2 \\ 0 & 0 & 3 & 5 & 8 \\ 8 & 2 & 0 & 0 & 10 \end{bmatrix},$$

which lead us, after suitable row operations, to the equation

$$P_1^{21}P_2^{16}P_3^{19}P_2^{24} = (\omega - 1)^{14}(\omega + 2)^{13}(\omega_1 + 2\omega + 3)(\omega_1 + 2\omega + 6)^2$$
$$= 2^{16}(\omega\omega_1 + 4\omega_1 - 28\omega - 72).$$

Our next task is to determine the units in the ring O_Ω. The only units of absolute value 1 are ± 1. The rank of the group of units is $R = r + s - 1$, where $K = 4 = r + 2s$, and since Ω is not a subfield of $\mathbf{R}$, $r = 0$ and $s = 2$. The rank of the group of units in O_Ω is thus $R = 1$. In the subfield $\mathbf{Q}(\omega)$, a real quadratic number field, the units also have rank one, and a fundamental unit can be found from the solution of the Pellian equation $x^2 - 17y^2 = -4$. In this case, we find that in $O_{\mathbf{Q}(\omega)}$, a fundamental unit is $2\omega + 5$. We suspect that this is also a fundamental unit in O_Ω, but, as indicated above, as long as we allow the parameter x_0 to be bigger than one, we do not really care. At any rate,

$$H(\beta) = \pm 2^{16}(2\omega + 5)^{x_1/x_0}(\omega\omega_1 + 4\omega_1 - 28\omega - 72).$$

We need to solve the Diophantine equation

$$x_1 \log|2\omega + 5| = x_0\left(\log 2^4 - \log|\omega\omega_1 + 4\omega_1 - 28\omega - 72|\right).$$

When we substitute in the complex values of $\omega = 1.561552813$ and $\omega_1 = -.5 \pm 9.597091324i$, we obtain the equation $x_1 = -x_0$. Thus we may take the solution $x_0 = 1$ and $x_1 = -1$. Therefore,

$$H(\beta) = \pm 2^{16}(3\omega\omega_1 - 4\omega_1 - 4\omega - 8).$$

Next we need to express both ω and ω_1 in terms of β. The first part is easy, using a famous theorem of Gauss:

$$\sqrt{(-1)^{(p-1)/2}p} = \sum_{j=1}^{(p-1)/2} \zeta_p^{j^2},$$

where $\zeta_p = e^{2\pi i/p}$. In our case this takes the form

$$\sqrt{17} = \sum_{j=1}^{8} \beta^{11\cdot j^2},$$

whence

$$\omega = -\beta^{154} - \beta^{132} - \beta^{121} - \beta^{110} - \beta^{77} - \beta^{66} - \beta^{55} - \beta^{33} - 1.$$

We cannot repeat this process in the next higher extension field Ω, but we can compute

$$z = \mathrm{Trace}_{\mathbf{Q}(\beta)/\Omega}(\beta) = \sum_{i=0}^{39} \beta^{2^i},$$

which is an element of Ω. Then we use linear algebra to find the minimal polynomial of z over $\mathbf{Z}[\omega]$, which must be monic and of degree 2. It is then simple to compute what linear combination of $\{1, z\}$ our ω_1 must be and thus find ω_1 as a polynomial in β modulo $\Phi_{187}(\beta)$. In fact,

$$\begin{aligned}\omega_1 = {} & \beta^{159} - 2\beta^{158} - 2\beta^{155} + \beta^{154} + \beta^{153} - 2\beta^{144} + \beta^{143} + \beta^{142} - 2\beta^{141} - 2\beta^{140} \\ & + 2\beta^{137} - 2\beta^{133} + \beta^{132} + 2\beta^{131} - 2\beta^{129} + 2\beta^{126} + \beta^{125} - 2\beta^{124} - 2\beta^{123} \\ & - 2\beta^{122} + 2\beta^{120} - 2\beta^{118} + 2\beta^{115} - 2\beta^{112} - 2\beta^{111} + 2\beta^{109} + \beta^{108} - 2\beta^{107} \\ & - 2\beta^{106} + 2\beta^{103} - 2\beta^{101} - 2\beta^{100} + 2\beta^{98} - 2\beta^{96} - 2\beta^{95} + 2\beta^{92} + \beta^{91} \\ & - 2\beta^{90} - 2\beta^{89} + 2\beta^{87} + 2\beta^{86} - \beta^{85} - 2\beta^{84} + 2\beta^{81} - 2\beta^{79} - 2\beta^{78} + 2\beta^{76} \\ & + 2\beta^{75} - \beta^{74} - 2\beta^{73} - 2\beta^{72} + 2\beta^{69} - \beta^{68} - 2\beta^{67} + 2\beta^{65} + 2\beta^{64} - 2\beta^{62} \\ & - 2\beta^{61} + 2\beta^{58} - \beta^{57} - 4\beta^{56} - \beta^{55} + 2\beta^{54} - \beta^{51} - 2\beta^{50} + 2\beta^{47} - 2\beta^{45} \\ & - \beta^{44} + 2\beta^{43} - \beta^{40} - 2\beta^{39} - 2\beta^{34} - \beta^{33} + 2\beta^{32} - 2\beta^{28} - \beta^{23} - 2\beta^{22} \\ & - \beta^{17} - 2\beta^{12} - \beta^{11} - \beta^{6} - 2\beta^{5} - 1.\end{aligned}$$

Direct substitution will now yield an explicit expression for $H(\beta)$:

$$\begin{aligned}H(\beta) = {} & \pm(8\beta^{159} - \beta^{158} - 4\beta^{155} + 6\beta^{154} - \beta^{153} - 3\beta^{149} + 9\beta^{148} - 3\beta^{147} - 4\beta^{144} \\ & - \beta^{143} + 8\beta^{142} - \beta^{141} - 4\beta^{140} - 3\beta^{138} + 10\beta^{137} - 3\beta^{136} - \beta^{133} \\ & + 3\beta^{132} + 7\beta^{131} - 3\beta^{130} - \beta^{129} - 3\beta^{127} + 7\beta^{126} + 5\beta^{125} - \beta^{124} - 4\beta^{123} \\ & - \beta^{122} + \beta^{121} + 7\beta^{120} - 3\beta^{119} - 4\beta^{118} - 3\beta^{116} + 7\beta^{115} + 6\beta^{114} \\ & - 3\beta^{113} - \beta^{112} - 4\beta^{111} + \beta^{110} + 7\beta^{109} + 5\beta^{108} - 4\beta^{107} - 4\beta^{106} \\ & - 3\beta^{105} + 3\beta^{104} + 7\beta^{103} - 3\beta^{102} - 4\beta^{101} - 4\beta^{100} - 3\beta^{99} + 4\beta^{98} \\ & + 6\beta^{97} - 4\beta^{96} - \beta^{95} - 3\beta^{94} + 3\beta^{93} + 4\beta^{92} + 5\beta^{91} - 4\beta^{90} - 4\beta^{89} \\ & - 3\beta^{88} + 4\beta^{87} + 7\beta^{86} - 5\beta^{85} - 4\beta^{84} - 3\beta^{83} + 6\beta^{82} + 4\beta^{81} + 6\beta^{80} \\ & - 4\beta^{79} - 4\beta^{78} + \beta^{77} + 4\beta^{76} + 4\beta^{75} + 4\beta^{74} - 4\beta^{73} - 7\beta^{72} + 6\beta^{71} \\ & + 7\beta^{69} - 5\beta^{68} - 4\beta^{67} + \beta^{66} + 4\beta^{65} + 4\beta^{64} + 3\beta^{63} - 4\beta^{62} - 4\beta^{61} \\ & + 3\beta^{60} + 4\beta^{58} + 4\beta^{57} - 5\beta^{56} - \beta^{55} + 4\beta^{54} + 3\beta^{52} - 5\beta^{51} - 7\beta^{50} \\ & + 3\beta^{49} + 3\beta^{48} + 4\beta^{47} + 3\beta^{46} - 7\beta^{45} - 5\beta^{44} + 4\beta^{43} + 3\beta^{41} + 4\beta^{40} \\ & - 7\beta^{39} + 3\beta^{38} + 3\beta^{37} + 3\beta^{35} - 7\beta^{34} - \beta^{33} + 4\beta^{32} + 3\beta^{31} + 3\beta^{29} \\ & - 7\beta^{28} + 3\beta^{27} + 3\beta^{24} + \beta^{23} - 7\beta^{22} + 3\beta^{20} + 3\beta^{18} - 8\beta^{17} + 3\beta^{16} \\ & + 3\beta^{14} + 2\beta^{12} - 8\beta^{11} + 3\beta^{10} + 3\beta^{7} + \beta^{6} + 2\beta^{5} + 3\beta^{3} + 3\beta - 9).\end{aligned}$$

Call this expression $\pm f_0(\beta)$. Alternate choices of the ideal P_1 would give the expressions

$$H(\beta) = \pm f_j(\beta) = \pm f_0\left[\lambda_3^j(\beta)\right],$$

for $0 \leqslant j \leqslant 3$. Then $H(x) \equiv \pm 2^{16} f_j(x) \pmod{\Phi_{187}(x)}$. This gives us the eight cases for $d = 187$. Now since $11|2^5 + 1$, and $17|2^4 + 1$, $d = 11$ and $d = 17$ are both semiprimitive cases, so $H(x) \equiv -2^{20} \pmod{\Phi_{11}(x)}$, and $H(x) \equiv 2^{20} \pmod{\Phi_{17}(x)}$. Also, $H(x) \equiv -1 \pmod{\Phi_1(x)}$.

Now we apply the integer coefficient criterion. We can eliminate the "$-$" sign in this way for each j, leaving four possible choices for $H(\beta)$, namely $+f_j(\beta)$. Lastly we apply Moebius inversion, and reconstruct the function $H(x)$ modulo $x^{187} - 1$, obtaining its coefficients. Recall that $\eta_i = \eta_{2i}$, so that the η_i's are equal for any two subscripts whose quotient is a power of 2 modulo 187. Thus, we list the coefficient and the weight for only one subscript from each coset of the multiplicative subgroup of powers of 2 in the multiplicative semigroup of integers modulo 187:

$$\begin{aligned}
\eta_0 &= -148595, && \text{number} = 1,\\
\eta_1 &= 48013, && = 40,\\
\eta_3 &= 48013, && = 40,\\
\eta_9 &= -83059, && = 40,\\
\eta_{11} &= -214131, && = 8,\\
\eta_{17} &= 113549, && = 10,\\
\eta_{23} &= -17523, && = 40,\\
\eta_{33} &= 113549, && = 8.
\end{aligned}$$

Now we use the formula $W_i = (n - \eta_i)/2$ to compute the codeword weights:

$$\begin{aligned}
W_0 &= 2939944960, && \text{number} = 1,\\
W_1 &= 2939846656, && = 40,\\
W_3 &= 2939846656, && = 40,\\
W_9 &= 2939912192, && = 40,\\
W_{11} &= 2939977728, && = 8,\\
W_{17} &= 2939813888, && = 10,\\
W_{23} &= 2939879424, && = 40,\\
W_{33} &= 2939813888, && = 8.
\end{aligned}$$

Then the weight enumerator polynomial will be

$$A(z) = 1 + 5879741325 z^{2939813888}(18 + 80z^{32768} + 40z^{65536} + 40z^{98304} + z^{131072} + 8z^{163840}).$$

7. More Examples. As another example, let us take $N = 161 = 7 \cdot 23$, $p = 2$. Then $k = 33$, $q = 2^{33}$, $K = 4$, and $n = 53{,}353{,}631$. Let $\beta = e^{2\pi i/161}$. Its minimum polynomial is $\Phi_{161}(x)$ which has degree $\phi(161) = 132$. Then $H(\beta)$ lies in a subfield of $\mathbf{Q}(\beta)$ of degree 4 over $\mathbf{Q}$, call it Ω. The Galois group of Ω over $\mathbf{Q}$ is the noncyclic Abelian group of order 4 consisting of $\{1, \lambda_3, \lambda_5, \lambda_{15}\}$. Since there are three elements of order 2 in the Galois group, there are three quadratic subfields of Ω over $\mathbf{Q}$, namely $\mathbf{Q}(\sqrt{-7}) = \mathbf{Q}(\omega_1)$, $\mathbf{Q}(\sqrt{-23}) = \mathbf{Q}(\omega_2)$, and $\mathbf{Q}(\sqrt{161}) = \mathbf{Q}(\omega)$, where

$$\omega_1^2 + \omega_1 + 2 = 0, \quad \omega_2^2 + \omega_2 + 6 = 0, \quad \omega^2 + \omega - 40 = 0.$$

For no particular reason we work with the last of these. We introduce ω here because $\{1, \omega\}$ is an integral basis of $O_{\mathbf{Q}(\sqrt{161})}$ over $\mathbf{Z} = O_{\mathbf{Q}}$. Now Ω is a quadratic extension of $\mathbf{Q}(\omega)$, and we may take $\Omega = \mathbf{Q}(\omega, \omega_1)$. Now we need to find an integral basis of O_Ω over $\mathbf{Z}$. As a first approximation we try the set $B = \{1, \omega, \omega_1, \omega\omega_1\}$. These are certainly linearly independent integers, but they may not generate the set of all integers in O_Ω. Now the discriminant of this set is computed to be 1127^2, and the discriminant of the field Ω is 161^2, there being an extra factor of 7^2 present. This implies that B is not an integral basis, and that there exists an integer of the form $\gamma = (\omega\omega_1 + i\omega_1 + j\omega + k)/7$, where $0 \leqslant i, j, k \leqslant 6$. This integer must satisfy a monic quartic polynomial equation, and congruence considerations modulo 7 then lead us to the unique solution $i = 4$, $j = 4$, $k = 2$, satisfying the equation $\gamma^4 + \gamma^3 - 16\gamma^2 + 12\gamma + 144 = 0$. We change the set B to $B = \{1, \omega, \omega_1, \gamma\}$, and now we have an integral basis. We can express each of these in terms of β by using Gauss's theorem:

$$\omega_1 = \beta^{23} + \beta^{46} + \beta^{92},$$

$$\omega_2 = \beta^7 + \beta^{14} + \beta^{21} + \beta^{28} + \beta^{42} + \beta^{56} + \beta^{63} + \beta^{84} + \beta^{91} + \beta^{112} + \beta^{126},$$

$$\omega = -2\omega_1\omega_2 - \omega_1 - \omega_2 - 1, \qquad \gamma = -\omega_1\omega_2.$$

Next we try to factor (2) in O_Ω. We can observe tha $(2) = (\omega + 7)(\omega - 6)$ and that $(2) = (\omega_1 + 1)(\omega_1)$. Likely candidates for prime ideals are the greatest common divisors of any two of these principal ideals, one from each equation. These work, as can be readily verified by checking norms, and all four possible choices form the four prime ideal divisors of (2). We arbitrarily select

$$P_1 = (\omega_1, \omega + 7),$$

and then compute

$$P_2 = \lambda_3^{-1}(P_1) = (\omega_1 + 1, \omega - 6),$$
$$P_3 = \lambda_5^{-1}(P_1) = (\omega_1 + 1, \omega + 7),$$
$$P_4 = \lambda_{15}^{-1}(P_1) = (\omega_1, \omega - 6).$$

We can now compute that

$$\omega_1 \equiv 10 \quad \text{and} \quad \omega_2 \equiv 6 \pmod{P_1^4},$$
$$\omega_1 \equiv 5 \quad \text{and} \quad \omega_2 \equiv 6 \pmod{P_2^4},$$
$$\omega_1 \equiv 5 \quad \text{and} \quad \omega_2 \equiv 9 \pmod{P_3^4},$$
$$\omega_1 \equiv 10 \quad \text{and} \quad \omega_2 \equiv 9 \pmod{P_4^4}.$$

We have the following factorizations into prime ideals:

$$(\omega + 7) = P_1P_3, \qquad (\omega - 6) = P_2P_4,$$
$$(\omega_1 + 1) = P_2P_3, \qquad (\omega_1) = P_1P_4,$$

and a short search reveals that

$$(\gamma + 4) = P_1^3P_2P_4, \qquad (\gamma + 2) = P_1P_2^2P_4^3,$$
$$(\gamma - 2) = P_1P_2^4P_4^2, \qquad (\gamma - 4) = P_1^6P_2P_4.$$

Now we apply Stickelberger's theorem, and obtain

$$(H(\beta)) = P_1^{15}P_2^{15}P_3^{18}P_4^{18}.$$

Using the matrices M_1 and M_2 we can get the following:

$$(H(\beta)) = 2^{18}(\gamma + 2)/(\gamma - 2)(\gamma + 4) = 2^{15}(1 - \omega_2),$$

and we can also find the unit

$$\varepsilon = -58\omega_1 - 32\omega_2 - 45.$$

The only units of absolute value 1 are ± 1. As above, the group of units U' has rank 1, so that ε or some root of it will generate it. We have the following equation:

$$H(\beta) = \pm 2^{15}\varepsilon^{x_1/x_0}(1 - \omega_2).$$

We need to solve the Diophantine equation

$$x_1 \log|\varepsilon| = x_0(\log 2^{3/2} - \log|1 - \omega_2|).$$

When we substitute in the complex values of ω_1, ω_2, and ε, the result is $x_1 = 0$.

Thus

$$H(\beta) = \pm 2^{15}(1 - \omega_2),$$

and $H(\beta) \in \mathbf{Q}(\omega_2)$, a quadratic extension of $\mathbf{Q}$. Other possibilities for P_1 would yield

$$H(\beta) = \pm 2^{15}(2 + \omega_2),$$

so we have four possible values of $H(\beta)$.

Next we apply the integer coefficient criterion to determine which of these values is correct. Reducing modulo 23 and $\Phi_7(x)$, we find that the upper sign holds in both equations. Reducing modulo 7 and $\Phi_{23}(x)$, we find that only the second equation holds. This implies that

$$H(x) \equiv 32768(x^{126} + x^{112} + x^{91} + x^{84} + x^{63} + x^{56} + x^{42} + x^{28} + x^{21} + x^{14} + x^7 + 2) \pmod{\Phi_{161}(x)}.$$

We use the known generating functions $H(x)$ for codes with $N = 7$ and $N = 23$ to compute that

$$H(x) \equiv -32768 - 28672(x^{18} + x^{16} + x^{13} + x^{12} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + x^1) \pmod{\Phi_{23}(x)},$$

and that

$$H(x) \equiv -45056 + 47104(x^4 + x^2 + x^1) \pmod{\Phi_7(x)}.$$

Now Moebius inversion yields the desired result:

$$\begin{aligned}
\eta_0 &= 50335, & \text{number} &= 1,\\
\eta_1 &= 3231, & &= 33,\\
\eta_3 &= 1183, & &= 33,\\
\eta_5 &= -2913, & &= 33,\\
\eta_7 &= 9375, & &= 11,\\
\eta_{11} &= -865, & &= 33,\\
\eta_{23} &= 7327, & &= 3,\\
\eta_{35} &= -19397, & &= 11,\\
\eta_{69} &= 5279, & &= 3.
\end{aligned}$$

Now we use the formula $W_i = (n - \eta_i)/2$ to compute the codeword weights:

$$\begin{aligned} W_0 &= 26651648, && \text{number} = 1,\\ W_1 &= 26675200, && = 33,\\ W_3 &= 26676224, && = 33,\\ W_5 &= 26678272, && = 33,\\ W_7 &= 26672128, && = 11,\\ W_{11} &= 26677248, && = 33,\\ W_{23} &= 26673152, && = 3,\\ W_{35} &= 26686464, && = 11,\\ W_{69} &= 26674176, && = 3. \end{aligned}$$

Then the weight enumerator polynomial will be

$$A(z) = 1 + 53353631z^{26651648}(1 + 11z^{20480} + 3z^{21504} + 3z^{22528} + 33z^{23552} + 33z^{24576} + 33z^{25600} + 33z^{26624} + 11z^{34816}).$$

Other cases which would be amenable to this technique, which have $k \geqslant 28$, $K \geqslant 3$, and are neither semiprimitive nor degenerate, are:

N	$\phi(N)$	k	K
$215 = 5 \cdot 43$	168	28	6
223	222	37	6
$231 = 3 \cdot 7 \cdot 11$	120	30	4
233	232	29	8
$247 = 13 \cdot 19$	216	36	6
$259 = 7 \cdot 37$	216	36	6
$279 = 3^2 \cdot 31$	180	30	6
$285 = 3 \cdot 5 \cdot 19$	144	36	4
$287 = 7 \cdot 41$	240	60	4
$291 = 3 \cdot 97$	192	48	4

The restriction $k \geqslant 28$ is due to the table of MacWilliams and Seery [2] covering all smaller values of k. This exhausts all such cases with $N < 300$.

903 Lamberton Drive
Silver Spring, Maryland 20902

12236 Shadetree Lane
Laurel, Maryland 20708

1. L. D. BAUMERT & R. J. MCELIECE, "Weights of irreducible cyclic codes," *Inform. and Control*, v. 20, 1972, No. 2, pp. 158–175.

2. F. JESSIE MACWILLIAMS & JUDITH SEERY, "The weight distributions of some minimal cyclic codes," *IEEE Trans. Inform. Theory*, v. IT-27, 1981, No. 6, pp. 796–806.

3. EDWIN WEISS, *Algebraic Number Theory*, McGraw-Hill, New York, 1963.