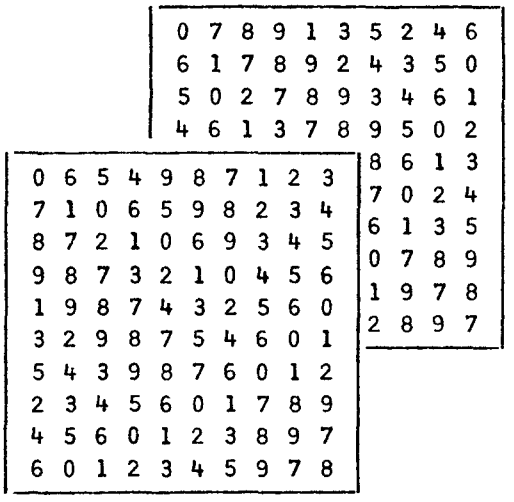
* *Part of this work was done while this author was with the Department of Statistics, University of North Carolina at Chapel Hill. The research done by him was partially supported by the Army Research Office, Durham, under Grant No. DA-ARO-D-31-124-G910 and the United States Air Force Office of Scientific Research under Contract No. AFOSR-68-1406.*



C O M B I N A T O R I A L
M A T H E M A T I C S
Y E A R

February 1969 - June 1970

IRREDUCIBLE BINARY CYCLIC CODES OF EVEN DIMENSION

by

P. Delsarte
MBLE Research Laboratory
Brussels, Belgium

J.-M. Goethals*
MBLE Research Laboratory
Brussels, Belgium

Department of Statistics
University of North Carolina at Chapel Hill

Institute of Statistics Mimeo Series No. 600.27

May 1970

IRREDUCIBLE BINARY CYCLIC CODES OF EVEN DIMENSION

by

P. Delsarte
MBLE Research Laboratory
Brussels, Belgium

and

J.-M. Goethals*
MBLE Research Laboratory
Brussels, Belgium, and
Department of Statistics
University of North Carolina

1. Introduction.

A cyclic code (n, k) is called irreducible when the reciprocal $(x^n-1)/g(x)$ of its generating polynomial g(x) is irreducible over the base field GF(q). Such a code is shown to be isomorphic to a finite field $GF(q^k)$. This isomorphism was used in [2] for the purpose of simplifying the analysis of weight-distributions. It is used here to characterize the weights of irreducible binary codes of even dimension in terms of weights of vectors of smaller length. Finally the existence is shown of a class of irreducible binary codes in which only two weights occur, and which contains the class discovered by McEliece [6].

2. The basic isomorphism.

Cyclic codes of length n over a finite field K are usually defined as ideals in the algebra $K[x]/(x^n-1)$ of polynomials modulo (x^n-1) over K.

---

* Part of this work was done while this author was with the Department of Statistics, University of North Carolina at Chapel Hill. The research done by him was partially supported by the Army Research Office, Durham, under Grant No. DA-ARO-D-31-124-G910 and the United States Air Force Office of Scientific Research under Contract No. AFOSR-68-1406.

These ideals are completely specified by their *generating polynomials* $g(x)$, or as well by their *associated polynomials* $h(x) = (x^n-1)/g(x)$, whose degree k determines the dimension of the ideal. The only cyclic codes considered here are those for which the block length n is relatively prime to the characteristic of the field K, which makes the algebra $K[x]/(x^n-1)$ semi-simple. The polynomials $g(x)$ and $h(x)$ are then relatively prime and there exist polynomials $\ell(x)$ and $m(x)$, which are relatively prime to $g(x)$ and $h(x)$ respectively, such that

$$m(x)g(x) + \ell(x)h(x) = 1 \mod(x^n-1). \tag{1}$$

The polynomial $e(x) = m(x)g(x)$ is a multiple of $g(x)$ and thus belongs to the code generated by $g(x)$. From (1), one deduces the following properties of $e(x)$:

$$e(x) \equiv 1 \mod h(x), \tag{2}$$

$$e^2(x) \equiv e(x) \mod(x^n-1). \tag{3}$$

As shown by MacWilliams [4], each cyclic code contains an unique element $e(x)$ having properties (2) and (3), which can be used as generator for the code. It is called the *idempotent* of the code. Its importance is emphasized in the following theorem.

THEOREM 1. *The mapping* $a(x) \to a(x)e(x)$ *is an isomorphism from* $K[x]/h(x)$ *to the code* $g(x)K[x]/(x^n-1)$, *that is the ideal generated by* $g(x) = (x^n-1)/h(x)$.

PROOF: Let $a(x)$ and $b(x)$ be any two distinct elements in the algebra $K[x]/h(x)$ of polynomials $\mod h(x)$ over K. Then, from (2),

$$a(x)e(x) \equiv b(x)e(x) \mod(x^n-1)$$

would imply $a(x) \equiv b(x)$ *mod* $h(x)$, a contradiction. Hence, the mapping is into. Since, from (3), one has

$$[a(x)e(x)][b(x)e(x)] = a(x)b(x)e(x) \quad mod(x^n-1) ,$$

and since obviously

$$a(x)e(x) + b(x)e(x) = [a(x) + b(x)]e(x),$$

the mapping is an homomorphism. Finally, since $K[x]/h(x)$ and $g(x)K[x]/(x^n-1)$ have the same dimension k (the degree of $h(x)$) over K, the mapping is one-to-one, hence an isomorphism.

Q.E.D.

It is well known that, when $h(x)$ is irreducible over $K = GF(q)$, the algebra $K[x]/h(x)$ is a faithful representation of $GF(q^k)$, the k-th extension of K. Hence, the following corollary is proved.

COROLLARY 2. *A cyclic code defined by an irreducible polynomial* $h(x)$ *of degree* k *is isomorphic to a finite field* $GF(q^k)$.

Such a code is called an *irreducible cyclic code*. Its isomorphism with $GF(q^k)$ can be exhibited in another way, using the so-called Mattson-Solomon mapping [5]. Let α be any root of $h(x)$; then α belongs to $GF(q^k)$ and $\alpha^n = 1$. If $K = GF(q)$, then $K[\alpha] = GF(q^k)$, that is the smallest extension field of K containing α. To each element c belonging to $K[\alpha]$, we associate the polynomial

$$v_c(x) = v_0 + v_1x + v_2x^2 + \ldots + v_{n-1}\,x^{n-1}, \tag{4}$$

where v_i is defined to be

$$v_i = \frac{1}{n} T_k(c\alpha^{-i}), \tag{5}$$

and where $T_k(z) = \Sigma_{j=0}^{k-1} z^{q^j}$ is the trace from $GF(q^k)$ to $GF(q)$. Then, as shown in [3], the mapping

$$c \in K[\alpha] \rightarrow v_c(x) \in K[x]/(x^n-1) \tag{6}$$

is an algebra isomorphism between two models of $GF(q^k)$. One model is $K[\alpha]$ where α is a root of an irreducible polynomial $h(x)$ of degree k, and the other is the irreducible cyclic code generated by $(x^n-1)/h(x)$ over K. One easily verifies that (6) maps the element 1 in $K[\alpha]$ onto $e(x)$, the idempotent of the code, and that, for $c = a(\alpha)$, one has

$$v_c(x) = a(x)e(x) \quad mod(x^n-1), \tag{7}$$

from which it follows that

$$c = a(\alpha) = v_c(\alpha). \tag{8}$$

REMARK: The mapping (6) can be applied to any extension field of K which contains α, in which case it is no longer an isomorphism, but rather an homomorphism.

3. WEIGHTS OF IRREDUCIBLE BINARY CYCLIC CODES.

Although many results apply to the q-ary case, only binary codes will be considered. Let ω be a primitive root in $GF(2^k)$ and let s be any divisor of 2^k-1. Then $\omega^s = \alpha$ is a primitive n-th root of unity, where n is defined to be

$$n = (2^k-1)/s. \tag{9}$$

Using (6), $GF(2^k)$ can be mapped onto the cyclic code of length n over $GF(2)$ whose nonzero vectors are the n-tuples

$$[T_k(\omega^i),\ T_k(\omega^{i-s}),\ T_k(\omega^{i-2s}),\ \ldots,\ T_k(\omega^{i-(n-1)s})], \tag{10}$$

whose components (5) are defined via the trace $T_k(z)$ from $GF(2^k)$ to $GF(2)$. Let us denote by $w(\omega^i)$ the weight of the vector (10), that is, since each component is 0 or 1, the summation over the integers

$$w(\omega^i) = \sum_{j=0}^{n-1} T_k(\omega^{i-sj}) . \tag{11}$$

Obviously, one has

$$w(\omega^i) = w(\omega^{i+sj}),\quad j = 0,1,2,\ldots,n-1. \tag{12}$$

It suffices thus to consider the values of i from 0 to $s-1$ in order to know the complete weight-distribution of the code.

From now on, we consider only even values of k, say $k = 2m$, and we define β and γ to be

$$\beta = \omega^{(2^m+1)2^{m-1}},\quad \gamma = \omega^{(2^m-1)2^{m-1}} . \tag{13}$$

It is easily verified that $\beta\gamma = \omega$, where β is a primitive root in $GF(2^m)$ and γ is a primitive (2^m+1)-th root of unity.

Suppose s divides 2^m-1 and let n_2 be

$$n_2 = (2^m-1)/s. \tag{14}$$

The field $GF(2^m)$ can be mapped onto the set of n_2-tuples

$$[T_m(\beta^j),\ T_m(\beta^{j-s}),\ \ldots,\ T_m(\beta^{j-(n_2-1)s})] \tag{15}$$

whose weights we denote by $w(\beta^j)$. The rest of this section will be devoted to the proof of the following theorem.

THEOREM 3. *If* s *divides* 2^m-1, *then the weights of the irreducible code of length* $(2^{2m}-1)/s$ *are given by*

$$w(\omega^i) = 2 \sum_{j=0}^{s-1} w(\beta^j)w(\beta^{i-j}). \tag{16}$$

The proof requires several preliminary steps, which we state as Lemmas 4 and 5.

LEMMA 4:

$$\prod_{i=1}^{2^{m-1}} [z - (\gamma^i+\gamma^{-i})] = z^{2^{m-1}} + \sum_{j=0}^{m-1} z^{2^{m-1}-2^j}.$$

PROOF: Let us denote by $Q_m(z)$ the above right-hand polynomial. We first show that

$$F_m(x) = x^{2^{m-1}} Q_m(x+x^{-1}) = (1+x^2)^{2^{m-1}} + \sum_{j=0}^{m-1} x^{2^j}(1+x^2)^{2^{m-1}-2^j}$$

is congruent to $1 + x + x^2 + \ldots + x^{2^m}$ *mod* 2. We prove it by induction on m, observing that the result is true for $m = 1$, and that one has $F_m(x) = x(1+x^2)^{2^{m-1}-1} + F_{m-1}(x^2)$, where the first term of the right-hand member is congruent to $x + x^3 + x^5 + \ldots + x^{2^m-1}$. So that, if the result is true for m-1, it is also true for m. A consequence is that $F_m(\gamma^i) = 0$, hence implying $Q_m(\gamma^i+\gamma^{-i}) = 0$, for $i \neq 0$. Now, it can be shown by the BCH argument [1] that $\gamma^i + \gamma^{-i} = \gamma^j + \gamma^{-j}$ is impossible unless $i \equiv \pm j$ *mod* (2^m+1). For otherwise the polynomial

$$v(x) = x^i + x^j + x^{2^m+1-i} + x^{2^m+1-j}$$

would have as roots the elements γ^{-2}, γ^{-1}, 1, γ, γ^2 and thus have weight at least 6, a contradiction. Therefore, $Q_m(z)$ being divisible by the 2^{m-1} distinct factors $[z - (\gamma^i+\gamma^{-i})]$ is divisible by their product, which having the same degree as $Q_m(z)$ must be indentical to it.

Q.E.D.

LEMMA 5. *The set* $\{\gamma^i+\gamma^{-i}: i = 1,2,\ldots,2^{m-1}\}$ *is identical to the set of elements of* $GF(2^m)$ *whose inverse have trace unity in* $GF(2)$.

PROOF: It suffices to observe that

$$Q_m(z) = z^{2^{m-1}} [1 + T_m(z^{-1})]$$

where $T_m(z)$ is the trace from $GF(2^m)$ to $GF(2)$. The result then follows from Lemma 4.

Q.E.D.

PROOF OF THEOREM 3. The weight $w(\omega^i)$ of the codevector associated with the element ω^i in $GF(2^{2m})$ is given by (11), which using (13) can be expressed as

$$w(\omega^i) = \sum_{\nu=0}^{n_2-1} \sum_{j=0}^{2^m} |T_{2m}(\beta^{i-s\nu}\gamma^{-j})|, \tag{17}$$

where $T_{2m}(z)$ is the trace from $GF(2^{2m})$ to $GF(2)$. Using the fact that for $\beta \epsilon GF(2^m)$, one has $T_{2m}(\beta\gamma) = T_m[\beta(\gamma+\gamma^{-1})]$, where $T_m(z)$ is the trace from $GF(2^m)$ to $GF(2)$, (17) can be rewritten as

$$w(\omega^i) = \sum_{\nu=0}^{n_2-1} \sum_{j=0}^{2^m} |T_m[\beta^{i-s\nu}(\gamma^j+\gamma^{-j})]|, \tag{18}$$

which, using Lemma 5, is equivalent to

$$w(\omega^i) = \sum_{\nu=0}^{n_2-1} \left\{ 2 \sum_{T_m(\beta^\ell)=1} \left| T_m(\beta^{i-s\nu}\beta^{-\ell}) \right| \right\}, \tag{19}$$

where the second summation runs through the 2^{m-1} elements of $GF(2^m)$ which have trace 1. But, this last summation can be replaced by

$$\sum_{\ell=0}^{2^m-2} |T_m(\beta^{i-s\nu}\beta^{-\ell})| \cdot |T_m(\beta^\ell)| ,$$

since $T_m(\beta^\ell)$ is either 0 or 1, and replacing ℓ by $(j-s\mu)$, where j runs from 0 to $(s-1)$ and μ from 0 to (n_2-1), finally gives

$$w(\omega^i) = 2 \sum_{j=0}^{s-1} \sum_{\rho} \sum_{\mu} |T_m(\beta^{(i-j)-s\rho})| \cdot |T_m(\beta^{j-s\mu})|,$$

where $\rho = \nu-\mu$. But now, the summations in ρ and μ are easily recognized to be $w(\beta^{i-j})$ and $w(\beta^j)$ respectively, hence proving the result.

Q.E.D.

REMARK: Let W_m be the circulant matrix of order s whose first row is given by

$$W_m = circ[w(1), w(\beta), w(\beta^2), \ldots, w(\beta^{s-1})] ,$$

and similarly

$$W_{2m} = Circ[w(\omega^i); (i = 0,1,2,\ldots,s-1)].$$

Then Theorem 3 is equivalent to

$$W_{2m} = 2W_m^2, \tag{20}$$

from which, by induction, one obtains

$$W_{2^t m} = 2^{2^t-1} W_m^{2^t}. \tag{21}$$

EXAMPLE: We briefly discuss hereunder two simple examples which emphasize that the mapping of $GF(2^m)$ onto the set of n_2-tuples (15) need not be an isomorphism. For both examples $m = 4$ and β is a primitive root in $GF(2^4)$. For the first, we choose $s = 5$ as divisor of 2^4-1; the triples $T(\beta^j)$, $T(\beta^{j-5})$, $T(\beta^{j-10})$ have respective weights 0,2,2,2,2, for $j = 0,1,2,3,4$; hence $W_4 = circ(0,2,2,2,2)$, and thus from (20), $W_8 = 2W_4^2 = circ(32,24,24,24,24)$, which shows that the (51,8) irreducible code has only two distinct weights, namely 24 and 32. For the second example, we chose $s = 2^4-1 = 15$, so that $n_2 = 1$ and $w(\beta^j)$ simply reduces to the trace $T_4(\beta^j)$. Hence, we have

$$W_4 = circ(0,0,0,1,0,0,1,1,0,1,0,1,1,1,1),$$

and from (20) we get

$$W_8 = circ(8,8,8,10,8,12,10,6,8,10,12,6,10,6,6),$$

which gives the weight-distribution of the irreducible (17,8) code, namely:

weight	0	6	8	10	12
number of vectors	1	4×17	5×17	4×17	2×17

.

4. TWO-WEIGHT IRREDUCIBLE CYCLIC CODES.

The (51,8) irreducible code discussed hereabove was shown to contain vectors of only two distinct weights. It was already shown by McEliece [6] that this property holds for all irreducible codes of length (9), when s is a prime for which 2 is a primitive root. This class of codes is extended here, as a result of the following theorem.

THEOREM 6. *Let* s *be any divisor of* 2^r+1, *and let* k *be an even multiple of* r, *say* k = 2mr. *Then the irreducible code of length* $n = (2^k-1)/s$ *and dimension* k *over* GF(2) *has only two distinct weights* w_0 *and* w_1 *which are the unique solution of the following equations*

$$\begin{aligned} w_0 + (s-1)w_1 &= 2^{k-1} \\ w_0^2 + (s-1)w_1^2 &= (n+1)2^{k-2} . \end{aligned} \tag{22}$$

PROOF: (i) We first prove the result for m odd, in which case s divides $(2^{mr}+1)$ so that n can be factorized as $n = n_1 n_2$, where $n_1 = (2^{mr}+1)/s$ and $n_2 = 2^{mr}-1$. Then, ([3], Theorem 1) the code (n,k) over GF(2) is isomorphic to the code $(n_1,2)$ over $GF(2^{mr})$. For any vector

$$(\beta_0, \beta_1, \beta_2, \ldots, \beta_{n_1-1}) \tag{23}$$

of this last code, the corresponding vector of the binary code (n,k) is permutation-equivalent to the vector of length $n_1 n_2$

$$(\bar{v}_o, \bar{v}_1, \bar{v}_2, \ldots, \bar{v}_{n_1-1}), \tag{24}$$

where $\bar{v}_i$ is obtained from $\beta_i \epsilon GF(2^{mr})$ by the mapping

$$\beta_i \rightarrow [T_{mr}(\beta_i), T_{mr}(\beta_i\alpha), \ldots, T_{mr}(\beta_i\alpha^{n_2-1})], \tag{25}$$

where α is a primitive root in $GF(2^{mr})$. But, since all vectors (25) which correspond to nonzero β_i have weight 2^{mr-1}, the weight of (24) is 2^{mr-1} times the weight of (23). If ω is the field element of which (23) is the image, and if γ is a primitive n_1-th root of unity, then β_i is given by

$$\beta_i = (\omega\gamma^{-i}) + (\omega\gamma^{-i})^{2^{mr}}, \tag{26}$$

which is zero iff $\omega\gamma^{-i} \epsilon GF(2^{mr})$. Consequently, the weight of (23) is either n_1 or n_1-1; it is n_1-1 when $\omega\epsilon\gamma^{i}[GF(2^{mr})]$ which occurs n_1n_2 times, and it is n_1 otherwise, that is $(s-1)n_1n_2$ times. Hence, the weights of the binary (n,k) code are

$$\begin{aligned} w_0 &= 2^{mr-1}(n_1-1) \\ w_1 &= 2^{mr-1} n_1, \end{aligned} \tag{27}$$

which occur n times and (s-1)n times, respectively.

(ii) For m even, we prove it by induction, observing that s divides $2^{k/2}-1$ in that case, so that Theorem 3 applies. Hence let us consider the case $k = 4mr$ and suppose the theorem is proved for $k = 2mr$, in which case we have

$$W_m = w_0 I + w_1 (J-I), \tag{28}$$

where I and J are the unit and all-one matrices of order s, and where w_0 and w_1 are given by (24). Then, from (20) we get by straightforward calculations

$$W_{2m} = 2^{2mr-1}[(n+1)I + n(J-I)], \tag{29}$$

where $n = (2^{2mr}-1)/s$, hence proving that the only two weights occurring are

$$w_0 = 2^{2mr-1}(n+1),$$
$$w_1 = 2^{2mr-1}n. \tag{28}$$

This completes the proof since (27) and (28) are the general solutions of (22) for the cases $k = 2mr$, and $k = 4mr$ respectively.

Q.E.D.

Some numerical results follow (Table 1).

TABLE 1:

Two-weight cyclic codes

r	s	k	n	w_0	w_1
1	3	4	5	4	2
1	3	6	21	8	12
1	3	8	85	48	40
1	3	10	341	160	176
1	3	12	1365	704	672
2	5	8	51	32	24
2	5	12	819	384	416
3	9	12	455	256	224
4	17	16	3855	2048	1920
5	33	20	31×1025	32×512	31×512
5	11	10	93	32	48
6	65	24	63×4097	64×2048	63×2048
6	13	12	315	128	160
7	43	14	381	128	192
9	27	18	19×511	18×256	19×256
9	171	18	3×511	2×256	3×256
9	57	18	9×511	8×256	9×256
9	19	18	27×511	26×256	27×256
10	205	20	5×1023	4×512	5×512
10	41	20	25×1023	24×512	25×512
11	683	22	3×2047	2×1024	3×1024
12	241	24	17×4095	16×2048	17×2048

REFERENCES

[1] BOSE, R.C. and RAY-CHAUDHURI, D.K., On a class of error correcting binary group codes, *Information Control*, 3 (1960), 68-79 and 279-290.

[2] GOETHALS, J.-M., Algebraic structure and weight distribution of binary cyclic codes, *University of North Carolina, Institute of Statistics Mimeo Series No. 484.4* (1966).

[3] GOETHALS, J.-M., Factorization of cyclic codes, *I.E.E.E., Trans. on Information Theory*, IT-13 (1967), 242-246.

[4] MacWILLIAMS, F.J., The structure and properties of binary cyclic alphabets, *Bell System Techn. J.*, 44 (1965), 303-333.

[5] MATTSON, H.F. and SOLOMON, G., A new treatment of Bose-Chaudhuri codes, *J. Soc. Indus. Appl. Math.*, 9 (1961), 654-669.

[6] McELIECE, R.J., A class of two-weight codes, *Jet Propulsion Laboratory Space Programs Summary 37-41, Vol IV*, 264-266.