$1 + S_1 z + S_1^2 z^2$. However, this polynomial factors into $(1 + S_1\omega z)(1 + S_1\omega^2 z)$, where $\omega = \alpha^{17}$ is a primitive third root of unity. So the two errors are at locations $S_1\omega$ and $S_1\omega^2$. This explains rule 4) in Algorithm 12.

Algorithm 12: Compute S_0, S_1, and S_5 and with these also $S_7 = S_5^{(2^5)}$.

1) IF $S_5 \neq S_1^5$, THEN

$$\sigma_1 = S_1,$$

$$\sigma_2 = \frac{S_7 + S_1^2 S_5}{S_5 + S_1^5}.$$

2) IF $S_5 = S_1^5$ and $S_0 = 1$ THEN

$$\sigma_1 = S_1,$$

$$\sigma_2 = 0.$$

3) IF $S_5 = S_1^5$ and $S_0 = S_1 = 0$ THEN

$$\sigma_1 = \sigma_2 = 0.$$

4) IF $S_5 = S_1^5$, $S_0 = 0$ and $S_1 \neq 0$ THEN

$$\sigma_1 = S_1,$$

$$\sigma_2 = S_1^2.$$

The two errors are at locations $S_1\omega$ and $S_1\omega^2$, where $\omega = \alpha^{17}$ is a primitive third root of unity.

IV. Conclusion

For a number of binary cyclic codes with $e > e_{\mathrm{BCH}}$, algebraic algorithms are given to find the error locator polynomial. Thus for these codes more errors can be corrected algebraically than by the Berlekamp–Massey algorithm. In some cases all error patterns of weight up to e can be decoded, in other cases only error patterns of weight up to e' with $e_{\mathrm{BCH}} < e' \leq e$. The correctness of three of these algorithms is (partly) based on an exhaustive computer search; in all other cases the algebraic proof is given in detail. It seems likely that many more cyclic codes can be decoded with the methods discussed here.

Acknowledgment

The authors wish to express their gratitude towards the referees who have increased the readability of this manuscript by their constructive criticism. Also the remark at the end of the description of code Number 25 is due to one of the referees.

References

[1] M. Elia, "Algebraic decoding of the (23,12,7) Golay code," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 150–151, Jan. 1987.

[2] G. L. Feng and K. K. Tzeng, "A generalized iterative algorithm for decoding cyclic codes beyond the BCH-bound," *IEEE Int. Symp. Inform. Theory*, San Jovite, Canada, 1983.

[3] ____, "A generalized Euclidean algorithm for multisequence shift-register synthesis," *IEEE Int. Symp. Inform. Theory*, Brighton, England, 1985.

[4] J. C. M. Janssen, "Decoding linear cyclic codes beyond the BCH bound," Masters Degree Thesis, Dept. of Math. and Comp. Science, Eindhoven University of Technology, Eindhoven, The Netherlands, 1988.

[5] F. J. MacWilliams and M. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam: North Holland, 1977.

[6] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes*, 2nd ed. Cambridge: The MIT Press, 1972.

[7] J. H. van Lint, "Introduction to coding theory," *Graduate Texts in Mathematics 86*. New York: Springer Verlag, 1982.

[8] J. H. van Lint and R. M. Wilson, "On the minimum distance of cyclic codes," *IEEE Trans. Inform. Theory*, vol. IT-33, pp. 23–40, Mar. 1987.

On a Class of Primitive BCH-Codes

PASCALE CHARPIN

***Abstract*—We introduce a special class of primitive BCH codes, the *minimal BCH* (MB) codes. Let C be an MB code of length $p^{m'r} - 1$ and designed distance d over GF(q), $q = p^r$; then $d = a\sum_{i=0}^{m'} q^i$, where $q - a$ is minimal in a certain sense. We prove that an MB code so defined has as minimum distance its designed distance. Using the Roos bound, we propose a lower bound, sometimes tight, for the minimum distance of the dual of an MB code. We describe the subclass of weakly self-dual extended MB codes and then characterize some weakly self-dual extended BCH codes. Similarly, we prove that the nontrivial extended MB code over GF(4) is the smallest extended BCH code which is not an even code. We point out that extended MB codes are principal ideals of a modular algebra of type $F_{p^r}[F_{p^m}]$.**

I. Introduction

Let p be a prime. A cyclic code of length $n = p^m - 1$ over a field of characteristic p is called *primitive*. We denote by G the Galois field GF(p^m) and by α a primitive nth root of unity in G. In this correspondence, all cyclic codes are assumed to be primitive and to have symbols from K, where K is a subfield of G. We denote by q the order of the finite field K; a BCH code is always a narrow-sense BCH code [8].

A cyclic code C is a principal ideal in the ring $K[Z]/(Z^n - 1)$. If $g(Z)$ is the generator polynomial of C then α^i is a *zero of the code* C if and only if $g(\alpha^i) = 0$. Thus we say that the set

$$\{ i \in [0, n] \mid \alpha^i \text{ is a zero of } C \} \tag{1}$$

is the definition set of C. Recall that the BCH code of length n and designed distance d over $K = \mathrm{GF}(q)$ is the cyclic code with definition set

$$T(q, d) = \bigcup_{i \in [1, d[} Cl_i, Cl_i \text{ is the cyclotomic coset of } q \bmod n \text{ containing } i. \tag{2}$$

Such a code is denoted by $B(q, d)$, $d \in [1, n]$.

In Section II we define a class of BCH codes which we call minimal BCH (MB) codes. This terminology is justified by the fact that an MB code with designed distance d has, in a certain sense, a minimal dimension—see Definition 1 and the proof of Lemma 1. In other words MB codes are primitive BCH codes the dimension of which follows immediately from the p-ary expansion of their designed distance. In Theorem 1 we state another definition of the class of MB codes; formula (7) shows the values of the designed distances of the MB codes and provides an overall description. The following corollaries give precise details about this description. Some MB codes are Reed–Solomon codes; the binary MB codes are the trivial even weight codes and thus the MB codes are only of interest if $K \neq \mathrm{GF}(2)$. Theorem 2 proves that the minimum distance of an MB code is its designed distance.

We then consider together MB codes and extended MB (EMB) codes (Sections III and IV)—extended BCH codes having some algebraic properties that BCH codes cannot have. The extended BCH codes are invariant under the affine group; in such a

Manuscript received April 2, 1988; revised March 15, 1989. This work was partially presented at "3 Jours sur le Codage," Toulon, France, November 1988.

The author is with the Laboratoire d'Informatique Théorique et Programmation, Université Paris VI, 4, place Jussieu, 75252 Paris Cedex 05, France.

IEEE Log Number 8931666.

0018-9448/90/1100-0222$01.00 ©1990 IEEE

context there are interesting relations between the weights of the code (or of its dual) and the weights of the extension (or of its dual). When an extended BCH code is an EMB code, some properties take a simple form; for example, the definition of the dual (see (15)), the weakly self-duality (Theorem 6), and the weight-divisibility over GF(4) (Theorem 8). Using the Roos bound we state a lower bound for the minimum distance of the dual of an MB code; Corollary 5 proves that in some cases this bound is exactly the minimum distance.

We point out that MB codes are interesting BCH codes. We prove that studying EMB codes one obtains some weakly self-dual BCH codes and all even BCH codes over GF(4) (Corollary 8 and Theorem 8). Moreover, an extended BCH code is a principal ideal of the group algebra $K[G]$ if and only if it is an MB code (Theorem 9). Table 1 presents the parameters of the MB codes of length $n < 5000$ for $p \in \{2,3,5,7,11\}$.

II. The Class of Minimal BCH Codes

Let S be the interval $[0, n]$. Each $s \in S$ will be identified with its p-ary expansion (written as an m-tuple):

$$s = (s_0, \cdots, s_{m-1}) \qquad s = \sum_{i=0}^{m-1} s_i p^i \qquad s_i \in [0, p-1].$$

The *p-weight* of s is $\omega_p(s) = \sum_{i=0}^{m-1} s_i$. We denote by $\ll$ the partial order relation over S:

$$k \ll t \leftrightarrow k_i \le t_i, \qquad \text{for all } i \in [0, m-1], \tag{3}$$

and we say that t is an *ascendant* of k.

Definition 1: A code $B(q,d)$ which satisfies

$$\dim C = \prod_{i=0}^{m-1} (p - d_i) \tag{4}$$

is called an MB code.

The following lemma gives an equivalent formula for (4) which will be used for the description of the class of MB codes (for the proof of Theorem 1). In the proof of this lemma, we point out that a given BCH code that satisfies (5) has minimal dimension (in a certain sense); for this reason we say that such a code is a minimal BCH code.

Lemma 1: The code $B(q,d)$ is an MB code if and only if $T(q,d)$ satisfies

$$T(q,d) = S^* \backslash \{ s \in S | d \ll s \} \quad \text{with } S^* = [1, n]. \tag{5}$$

Proof: The cardinality of $T(q,d)$ is the cardinality of the zeros set of the cyclic code $B(q,d)$; thus $\dim B(q,d) = n - |T(q,d)|$. Moreover, $T(q,d)$ does not contain the ascendants of d. Indeed, $s \in T(q,d)$ if and only if there exists a j such that $q^j s < d$. Suppose that s is an ascendant of d; then we have $d \ll s$, $q^j d \ll q^j s$, and finally $q^j d \le q^j s < d$, which contradicts (2). Thus we have proved

$$\dim B(q,d) \ge |\{ s \in S | d \ll s \}|$$
$$- ie \;\; T(q,d) \subset S^* \backslash \{ s \in S | d \ll s \}. \tag{6}$$

If (6) is satisfied with equality, we say that the BCH code $B(q,d)$ has minimal dimension. It is clear that

$$|\{ s \in S | d \ll s \}| = \prod_{i=0}^{m-1} (p - d_i).$$

Hence (6) becomes an equality if and only if $B(q,d)$ satisfies (4). Thus we have proved that a BCH code has minimal dimension (i.e., satisfies (5)) if and only if it is an MB code.

Theorem 1: $q = p^r$ and $m = m'r$. For each $j \in [1, (p-1)r]$, we denote by $d(j)$ the element of S defined by

$$d(j) = a(j) \sum_{i=0}^{m'-1} q^i$$
$$\text{with } a(j) = \max \{ s \in [1, q-1] | \omega_p(s) = j \}. \tag{7}$$

Let $D(q)$ be the set of the $d(j)$. Then $B(q,d)$ is an MB code if and only if $d \in D(q)$.

Proof: Note that $D(q)$ is dependent on m', but the cardinality of $D(q)$ is only dependent on q, thus justifying the notation. We shall specify the value of m' when necessary. First it is clear that each element $d(j)$ of $D(q)$ permits us to define a BCH code with designed distance $d(j)$ over K. Indeed, the definition of $d(j)$ implies that $q^i d(j) = d(j)$, for all i. We now denote by T the definition-set of a code $B(q,d)$; let $\overline{T} = \{ s \in S | d \ll s \}$.

1) Suppose that $d = d(j), d(j) \in D(q)$. We have seen that $T \subset S^* \backslash \overline{T}$. Let $s \in S^* \backslash \overline{T}$; let $(s_0, \cdots, s_{m'-1})$ be the q-ary expansion of s (written as an m'-tuple). Similarly, let $(d_0, \cdots, d_{m'-1})$ be the q-ary expansion of d. Since $s \notin \overline{T}$, there exists an i such that s_i is not an ascendant of $a(j)$. In accordance with (7) we can write a formula giving the p-ary expansion of $a(j)$:

$$a(j) = vp^{r-1-u} + \sum_{k=r-u}^{r-1} (p-1) p^k \tag{8}$$

where u and v are, respectively, the quotient and the remainder of j by $(p-1)$—by convention, if $u = 0$ then $[r-u, r-1] = \varnothing$. Obviously, $a(j) \le s_i$ if and only if $a(j) \ll s_i$. Hence $s_i < a(j)$; therefore, $q^{m'-1-i} s < d(j)$ and then $s \in T$. We have proved that T satisfies (5); thus $B(q,d)$ is a MB code.

2) We suppose now that T satisfies (5). Then $d \ll q^i d$, for all i. However, $\omega_p(q^i d) = \omega_p(d)$ implies that $q^i d = d$—two distinct elements which have the same p-weight cannot be related by $\ll$. Then d has the following form:

$$d = \sum_{i=0}^{m'-1} a q^i, \qquad a \in [1, q-1].$$

Let $j = \omega_p(a)$; suppose that $a \ne a(j) - a(j)$ is defined by (7). Let $s = d(j)$; then $d \le s$ and s is not an ascendant of d. Since $B(q,d)$ is a BCH code, we have $s \notin T$. This contradicts (5). Thus we conclude that $d \in D(q)$.

The cardinality of $D(q)$ is $r(p-1)$: among BCH codes of length n over K there are $r(p-1)$ MB codes. The number of MB codes in a class of BCH codes is then only dependent on the order of K. If the length of the considered codes is $q-1$, we obtain Reed–Solomon codes.

Corollary 1: Among the Reed–Solomon codes of length $p^m - 1$, there are $m(p-1)$ MB codes. The minimum distance of such an MB code takes one of the values:

$$d(j) = \max \{ s \in [1, p^m - 1] | \omega_p(s) = j \},$$
$$j \in [1, m(p-1)].$$

The MB code which has $d(r(p-1))$ as designed distance is a trivial cyclic code: its definition set is the interval $[1, n-1]$. If $q = 2$ then $r(p-1) = 1$; hence we have the following.

Corollary 2: There is only one binary MB code of length $2^m - 1$; this is the cyclic code whose generator polynomial is $\sum_{i=0}^{n-1} Z^i$.

Analyzing (4) with the aid of (7) and (8), we can provide another expression for the dimension of an MB code.

TABLE I
EMB CODES OF LENGTH N ($N = p^m$) OVER GF (q) FOR $N < 5000$ AND $p \in \{2,3,5,7,11\}$[a]

N	q	d	δ	k	N	q	d	δ	k
16	4	10	*4	4	1024	32	924	8	16
64	4	42	5	8	1024	32	990	4	4
64	8	36	*8	16	4096	4	2730	8	64
64	8	54	4	4	4096	8	2340	14	512
256	4	170	6	16	4096	8	3510	6	16
256	16	136	*16	64	4096	16	2184	23	512
256	16	204	8	16	4096	16	3276	11	64
256	16	238	4	4	4096	16	3822	5	8
512	8	292	11	64	4096	64	2080	*64	1024
512	8	438	5	8	4096	64	3120	32	256
1024	4	682	7	32	4096	64	3640	16	64
1024	32	528	*32	256	4096	64	3900	8	16
1024	32	792	16	64	4096	64	4030	4	4
9	3	4	4	4	729	9	546	8	27
27	3	13	5	8	729	9	637	5	8
81	3	40	6	16	729	27	252	36	324
81	9	30	12	36	729	27	504	18	81
81	9	60	6	9	729	27	588	12	36
81	9	70	4	4	729	27	672	6	9
243	3	121	7	32	729	27	700	4	4
729	3	364	8	64	2187	3	1093	9	128
729	9	273	17	216					
25	5	6	8	16	625	25	260	30	225
25	5	12	6	9	625	25	390	20	100
25	5	18	4	4	625	25	520	10	25
125	5	31	11	64	625	25	546	8	16
125	5	62	8	27	625	25	572	6	9
125	5	93	5	8	625	25	598	4	4
625	5	156	14	256	3125	5	781	17	1024
625	5	312	10	81	3125	5	1562	12	243
625	5	468	6	16	3125	5	2343	7	32
625	25	130	40	400					
49	7	8	12	36	2401	7	1600	10	81
49	7	16	10	25	2401	7	2000	6	16
49	7	24	8	16	2401	49	350	84	1764
49	7	32	6	9	2401	49	700	70	1225
49	7	40	4	4	2401	49	1050	56	784
343	7	57	17	216	2401	49	1400	42	441
343	7	114	14	125	2401	49	1750	28	196
343	7	171	11	64	2401	49	2100	14	49
343	7	228	8	27	2401	49	2150	12	36
343	7	285	5	8	2401	49	2200	10	25
2401	7	400	22	1296	2401	49	2250	8	16
2401	7	800	18	625	2401	49	2300	6	9
2401	7	1200	14	256	2401	49	2350	4	4
121	11	12	20	100	1331	11	133	29	1000
121	11	24	18	81	1331	11	266	26	729
121	11	36	16	64	1331	11	399	23	512
121	11	48	14	49	1331	11	532	20	343
121	11	60	12	36	1331	11	665	17	216
121	11	72	10	25	1331	11	798	14	125
121	11	84	8	16	1331	11	931	11	64
121	11	96	6	9	1331	11	1064	8	27
121	11	108	4	4	1331	11	1197	5	8

[a] The extended RS codes and the trivial codes are not given. d is the designed distance of the MB code; k is the dimension of the MB code and of its extension; δ is the bound of the minimum distance of the dual (which is stated in Theorem 5). From Theorem 2, d is the minimum distance of the corresponding MB code (i.e., the minimum distance of the EMB code is $d+1$). The asterisk indicates the minimum distance of the dual (see Corollary 5).

Corollary 3: Let B be an MB code with designed distance $d(j) \in D(q)$. Let u and v be the quotient and the remainder of j by $p-1$, respectively. Then

$$\dim B = \left((p-v)\,p^{r-u-1}\right)^{m'}. \tag{9}$$

Hence the dimension of an MB code (such as B) is a power of p if and only if $p-1$ divides j (i.e., the p-ary expansion of $d(j)$ is composed of 0's or $p-1$'s); for characteristic 2, the dimension of B is always a power of 2.

Let $d = a\sum_{i=0}^{m'-1} q^i$, $a \in [1, q-1]$. Then we can construct a corresponding cyclic code C the definition set of which is given by (5). Let T be the definition set in question. That means

$$T = S^* \backslash \{ s \in S | d \ll s \} \quad \text{with } S^* = [1, n], \tag{10}$$

and C is a code over GF(q).

Conversely, if C is a cyclic code over GF(q) such that its definition set contains $[1, d]$ and satisfies (10), then d must satisfy $q^i d = d$, for all i. Suppose that $q = p$; the definition of $D(q)$ simplifies to

$$d(j) = j \sum_{i=0}^{m-1} p^i, \qquad j \in [1, p-1]. \tag{11}$$

This means that if $K = \mathrm{GF}(p)$ then only MB codes have minimal dimension.

Corollary 4: If $q = p$, then a cyclic code the definition set of which satisfies (10) is a BCH code.

The following theorem points out that the true minimum distance of an MB code is equal to its designed distance.

Theorem 2: $n = q^{m'} - 1$; let $b = (q^{m'} - 1)/(q-1)$. Then a BCH code of length n and designed distance $d = ab$ ($a \in [1, q-1]$) over GF(q) has minimum distance exactly equal to d; therefore, all the MB codes of length n over GF(q) satisfy this property.

Proof: We have

$$b = 1 + q + \cdots + q^{m'-1} \qquad n = b(q-1).$$

Then (in the algebra $K(Z)/(Z^n - 1)$),

$$Z^n - 1 = U(Z)Q(Z)$$

with

$$U(Z) = Z^{q-1} - 1$$

and

$$Q(Z) = 1 + Z^{q-1} + Z^{2(q-1)} + \cdots + Z^{(b-1)(q-1)}.$$

Let

$$I = \{ b, 2b, \cdots, (q-1)b \} \qquad J = [1, n] \backslash I.$$

Then we have

$$U(\alpha^i) = 0 \leftrightarrow i \in I,$$

$$Q(\alpha^i) = 0 \leftrightarrow i \in J.$$

Let for each a, $a \in [1, q-1]$:

$$R_a(Z) = Q(Z) \prod_{k=1}^{a-1} (Z - \alpha^{kb})$$

(with $R_1(Z) = Q(Z)$).

Note that the code $B(q, ab)$ exists for all a, because $qab = ab$ modulo n; $R_a(Z)$ is a polynomial over GF(q) the zeros of which are

$$\alpha^l, \qquad l \in [b, 2b, \cdots, ab[\cup J.$$

Then $R_a(Z) \in B(q, ba)$. However, the weight of the corresponding codeword satisfies

$$w(R_a(Z)) \le w(Q(Z))\, w\left(\prod_{k=1}^{a-1} (Z - \alpha^{kb}) \right) \le ab$$

($w(x)$ is the weight of the codeword x). Hence the minimum distance of $B(q, ab)$ is ab. Therefore, by Theorem 1, the minimum distance of an MB code equals its designed distance.

Example 1: $p = 2$; $q = 8$; $m = 6$. There are three MB codes of length 63 over GF(8). The dimensions are, respectively, 2^4, 2^2, and 1. From Theorem 2 the designed distances

$$d(1) = (0,0,1,0,0,1) = 36$$

$$d(2) = (0,1,1,0,1,1) = 54$$

$$d(3) = (1,1,1,1,1,1) = 63 \text{ (the trivial code)}$$

are the true minimum distances of the corresponding MB codes.

Example 2: $q = p = 5$; $m = 3$. There are four MB codes of length 124 over GF(5). From Corollary 4, they are the only cyclic codes with minimal dimension. The elements of $D(5)$ are

$$d(1) = (1,1,1) \quad d(2) = (2,2,2)$$

$$d(3) = (3,3,3) \quad d(4) = (4,4,4).$$

Each $d(j)$ is the true minimum distance of the corresponding MB code; the dimensions are respectively 4^3, 3^3, 2^3, and 1.

III. Some Properties of MB Codes and Extended MB Codes

We now consider together the cyclic code and its extension; the extension is the usual one: each codeword is extended by adding an overall parity check, numbered ∞. Let C be a cyclic code with definition set T; the extension of C, denoted by C_e, is the K-subspace of K^N, $N = p^m$:

$$\left\{ c = (c_\infty, c_0, \cdots, c_{n-1}) | c_\infty + \sum_{i=0}^{n-1} c_i = 0 \right.$$
$$\left. \text{and } \sum_{i=0}^{n-1} c_i (\alpha^i)^s = 0, \forall s \in T \right\}. \tag{12}$$

We say that $T_e = T \cup \{0\}$ is the definition set of C_e. Recall some properties of extended cyclic codes [1], [3]–[7].

1) $\dim C_e = \dim C$.

2) C_e is invariant under the doubly transitive affine group of permutation of G (is an affine-invariant code) if and only if T_e satisfies

$$s \in T_e \quad \text{and} \quad t \ll s \rightarrow t \in T_e. \tag{13}$$

3) If C_e is affine-invariant, then its minimum distance is $d+1$ if and only if the minimum distance of C is d; hence Theorem 2 also gives the minimum distance of the extended MB codes.

4) The definition set of the dual $\hat{C}_e$ of C_e is equal to the definition set of the dual $\hat{C}$ of C. That is,

$$\hat{T} = \hat{T}_e = \{ s \in S | n - s \notin T_e \}. \tag{14}$$

Nevertheless, $\hat{C}$ and $\hat{C}_e$ are distinct codes. From (12) it is clear that a codeword of $\hat{C}$ is a codeword of $\hat{C}_e$ (with $c_\infty = 0$). Suppose that C_e is affine-invariant; then $\hat{C}_e$ is also affine-invariant. Then each codeword c of $\hat{C}_e$ can be transformed into a codeword $c' \in \hat{C}_e$ such that $c'_\infty = 0$ and $w(c) = w(c')$. Thus we have proved the following.

Lemma 2: If C_e is affine-invariant, then $\hat{C}_e$ and $\hat{C}$ have the same minimum distance.

It is well-known that extended BCH codes are affine-invariant; thus a dual of an extended BCH code is also affine-invariant. Henceforth we consider only extended cyclic codes that are affine-invariant. We denote by $B_e(q,d)$ the extension of the code $B(q,d)$; an extended MB code is called an EMB code. Extending BCH codes one produces weakly self-dual codes or even codes over GF(4) or ideals of a modular algebra; all these properties take a simple form when the considered BCH code is an MB code, as we shall show later.

A. On EMB Codes Duality

Theorem 3: Consider an EMB code $B_e(q,d)$, $d \in D(q)$; the definition set of its dual is the set

$$\hat{T}_c(q,d) = \{ s \in S | s \ll n-d \}. \tag{15}$$

Proof: According to (5) and (14), we have

$$s \in \hat{T}_e(q,d) \leftrightarrow n-s \notin T_e(q,d) \leftrightarrow d \ll n-s \leftrightarrow s \ll n-d,$$

completing the proof.

Let $\hat{D}(q)$ be the set of the $n-d(j)$, $d(j) \in D(q)$; Theorem 3 means that each dual of an EMB code is uniquely defined by one element of $\hat{D}(q)$. In accordance with (7) and (8), we can define the elements of $\hat{D}(q)$ as follows: $\hat{D}(q)$ is the set of the $t(k) \in S$, $k \in [0, r(p-1)]$, such that

$$t(k) = b(k) \sum_{i=0}^{m'-1} q^i$$

$$\text{with } b(k) = \min \{ s \in [1, q-1] | \omega_p(s) = k \}. \tag{16}$$

Using the Roos bound [11], we can give a lower bound for the minimum distance of the dual of an MB code; it follows from Lemma 2 that this bound is available for the dual of the extension of the MB code. Theorem 4 is the theorem of Roos (adapted to our notation). A simpler proof of this theorem has recently been given by Van Lint and Wilson [12]. Corollary 5 presents a class of MB codes for which this bound is the minimum distance of their duals.

Let $M \subset S$; M is called a consecutive set of length k, if there is some a, which is relatively prime with n, such that

$$M = \{ as \pmod n | s \in [1,k] \}. \tag{17}$$

If $M_1 \subset S$ and $M_2 \subset S$, then we can define

$$M_1 + M_2 = \{ s_1 + s_2 \pmod n | s_1 \in M_1, s_2 \in M_2 \}. \tag{18}$$

Theorem 4 (Roos Bound): Let T be the definition set for a cyclic code with minimum distance d_T. Let $M \subset S$ be such that there exists a consecutive set $\overline{M}$ containing M with $|\overline{M}| \le |M| + d_T - 2$. Then the cyclic code with definition set $T+M$ has minimum distance $d \ge |M| + d_T - 1$.

Theorem 5: Let $t \in \hat{D}(q)$, $t = t(k)$, and $b(k)$ be defined by (16). Let $T = \{ s \in S | s \ll t \}$, and let U be the cyclic code of length $q^{m'}-1$ over GF(q), the definition set of which is T. Then the minimum distance δ of U satisfies

$$\delta \ge m' b(k) + 2. \tag{19}$$

In other words, let δ be the minimum distance of the dual of $B(q, n-t)$ (or of $B_e(q, n-t)$); then δ satisfies (19).

Proof: We suppose that t is such that U is not a trivial code. We suppose also that $m' > 1$; indeed if $m' = 1$, the considered codes are Reed–Solomon (RS) codes and $t = b(k)$; in this case the dual of $B_e(q, n-t)$ is $B_e(q, t+1)$ the minimum distance of which is $t+2$ (in (19) δ equals the bound). Let

$$M_i = \{ 0, q^i, 2q^i, \cdots, b(k) q^i \}, \qquad i \in [0, m'-1].$$

The definition of $b(k)$ implies that $s \in [0, b(k)]$ if and only if $s \ll b(k)$. Indeed, the p-ary expansion of $b(k)$ is $(p-1, \cdots, p-1, u, 0, \cdots, 0)$ (replacing $a(j)$ by $q-1-a(j)$ in (8)). This observation and the definition of T imply

$$T = \left\{ \sum_{i=0}^{m'-1} s_i | s_i \in M_i \right\} = \sum_{i=0}^{m'-1} M_i.$$

Since α^{q^i} is a primitive nth root of unity in G, M_i is a consecutive set of length $b(k)+1$. We denote by U_i the cyclic code the definition set of which is $\sum_{l=0}^{i} M_l$; let d_i be the minimum distance of U_i. Since $d_{m'-1} = \delta$ and $U_{m'-1} = U$ we shall prove (19) by induction on $i \in [0, m'-1]$.

Clearly, $d_0 \ge b(k)+2$. By Theorem 4, we have

$$d_i \ge |M_i| + d_{i-1} - 1, \qquad i \in [1, m'-1].$$

Then

$$d_1 \ge (b(k)+1) + (b(k)+2) - 1 = 2b(k) + 2.$$

Suppose now that we have proved (19) for $i-1$. Then

$$d_i \ge (b(k)+1) + d_{i-1} - 1 \ge (b(k)+1) + (ib(k)+2) - 1$$
$$\ge (i+1) b(k) + 2.$$

We obtain (19) for $i = m'-1$. Note that T is the definition set of the dual of the MB code $B(q, n-t)$; from Lemma 2, δ is also the minimum distance of the dual of $B_e(q, n-t)$.

Example 3: $p=2$, $q=4$, $m'=3$. Then

$$D(4) = \{ (0\ 1\ 0\ 1\ 0\ 1), (1\ 1\ 1\ 1\ 1\ 1) \}$$
$$= \{ d(1), d(2) \}$$

$$\hat{D}(4) = \{ (0\ 0\ 0\ 0\ 0\ 0), (1\ 0\ 1\ 0\ 1\ 0) \}$$
$$= \{ t(0), t(1) \}.$$

Consider the dual of $B(4, d(1) = 42)$; with the notation of Theorem 5 we have $t = t(1)$, $b(1) = 1$ and

$$T = \{0,1,4,5,16,17,20,21\} \quad \delta \ge 3+2 = 5.$$

Corollary 5: $m = 2r$ and $q = 2^r$. Let $d = 2^{r-1}(1+q)$. Then the dual of the MB code $B(q,d)$ (or of the EMB code $B_e(q,d)$) has minimum distance q.

Proof: Let $\hat{B}$ be the dual of $B_e(q,d)$, and let $\hat{T}$ be the definition set of $\hat{B}$. Let δ be the minimum distance of $\hat{B}$. We have $m' = 2$ and, by (7) and (16), $d = d(1)$ and $n - d = (2^{r-1} - 1)(1+q) = t(r-1)$. Then $m' b(r-1) + 2 = 2(2^{r-1} - 1) + 2 = q$; from Theorem 5, $\delta \ge q$. Thus the proof of the theorem amounts to finding a codeword of $\hat{B}$ the weight of which is q.

Let $a = q-1$ and $c = (q^{m'}-1)/(q-1)$; then $n = ac$ and

$$Z^n - 1 = (Z^c - 1)(Z^{c(a-1)} + Z^{c(a-2)} + \cdots + 1)$$
$$= (Z^c - 1) h(Z).$$

Since $\hat{T} = \{ s \in S | s \ll (2^{r-1}-1)(1+q) \}$, $s \in \hat{T}$ if and only if $s = s_1 + s_2 q$ with $s_1 \in [0, 2^{r-1}-1]$ and $s_2 \in [0, 2^{r-1}-1]$. Note that $q-1$ divides s if and only if $q-1$ divides $s_1 + s_2$. However, $q = 2^r$, and thus $s_1 + s_2 < q-1$. Hence $q-1$ cannot divide s. However $(\alpha^s)^c = 1$ if and only if $s = 0$ or $q-1$ divides s. From the remark above, such an s cannot be in $\hat{T} \setminus \{0\}$. Thus we have proved that

$$s \in \hat{T} \setminus \{0\} \rightarrow h(\alpha^s) = 0. \tag{20}$$

Let h_e be the codeword obtained by extending $h(Z)$. From (12) and (20) $h_e \in \hat{B}$. Moreover, the weight of h_e is $a+1=q$.

Example 4: $m=8$, $q=2^4$, $d=2^3 17=136$. Hence $m'=2$ and $n=255$. Let B be the BCH code of length 255 and designed distance 136; B has minimum distance 136; the extension B_e of B has minimum distance 137 (from Theorem 2). The dual of B and the dual of B_e have minimum distance 16 (from Corollary 5).

B. Weakly Self-Dual EMB Codes

A linear code which is contained in its dual is called weakly self-dual (WSD). Let U be a cyclic code with definition set T. Let $\hat{T}$ be the definition set of the dual of U. Then U is WSD if and only if $\hat{T} \subset T$. Thus a narrow-sense BCH code cannot be WSD because for such a code zero is in $\hat{T} \setminus T$. However extended BCH codes (and therefore EMB codes) are possible WSD codes, as we shall show. Moreover, we exhibit (in Corollary 7) a part of WSD extended BCH codes. Further, we point out that in some cases all WSD extended BCH codes are described.

Theorem 6: An EMB code with designed distance d is WSD if and only if $d > n/2$.

Proof: Let B be an EMB code, and let R be the definition set of B. From (5) and (15), it is obvious that the condition $\hat{R} \subset R$ is equivalent to $n-d<d$.

Corollary 6: EMB codes over GF(2^r) are WSD.

Proof: $q=2^r$. For a given length n, the designed distance of the largest EMB code is

$$d(1)=2^{r-1}\sum_{i=0}^{m'-1} q^i.$$

(See (7) and (8).) Clearly, $d(1) > n/2$.

Remark: If $m'=1$, then $n=q-1$ and extended BCH codes are extended RS codes. Then the dual of $B_e(q,d)$ is the extended RS code $B_e(q, n-d+1)$. We have $d(1)=2^{r-1}=q/2$, and thus $n-d(1)+1=d(1)$. Hence $B_e(q,d(1))$ is the self-dual extended RS code.

Corollary 7: Let $j \in [1, r(p-1)]$ be defined by: $j=1$ if $p=2$ and $j=\omega_p((q-1)/2)+1$ otherwise; let $\lambda=d(j)$. Let U be the extended BCH code $B_e(q,d)$. Then

1) if $d \le n-\lambda$, then U is not WSD;
2) if $n-\lambda < d \le \lambda$, then U can be WSD;
3) if $d > \lambda$, then U is WSD.

Proof: Let T be the definition set of U. $D(q)$ is defined by (7) in Theorem 1. Note that

$$\lambda = \min\{ d(j) \in D(q) \mid d(j) > (n/2)\}$$

(λ is the designed distance of the largest WSD EMB code). If $p=2$, then $\lambda = d(1)$ (from Corollary 6).

1) Since $\lambda > n/2$, we have $d \le n-\lambda < \lambda$. Thus $n-\lambda \in \hat{T} \setminus T$, and U cannot be WSD.
2) See Example 5.
3) This follows immediately from Theorem 6.

Example 5: In Example 1, we had $\lambda = d(1) = 36$. Thus $n-\lambda = (110110) = 27$. If $d=31$, then U is WSD while $B_e(8,28)$ is not WSD. Indeed $n-28=35=q28 \pmod n$; hence $35 \in \hat{T} \setminus T$.

Suppose that m' and q satisfy

$$\exists j,\ j \in [1, r(p-1)] \text{ such that } d(j)=n/2. \qquad (21)$$

Thus $n-d(j)=d(j)$. Let R be the definition set of the EMB code $B_e(q, d(j))$; the symbols U and T are defined in Corollary 7 and its proof. From the definition of $\hat{R}$ and R (see (5) and (15)) we can say that (21) yields $\hat{R} \setminus R = \{d(j)\}$. Thus if $d > d(j)$, then R is strictly contained in T; therefore, $\hat{T}$ is strictly contained in $\hat{R}$ with $d(j) \notin \hat{T}$; hence $\hat{T} \subset R \subset T$. We have $d > d(j) \leftrightarrow U$ is WSD.

By (7), (21) is satisfied if and only if $a(j)=(q-1)/2$. Hence q cannot be even. Suppose that $p>2$ with $q=p^r$. Let $\beta = \omega_p((q-1)/2)$; then

$$\frac{q-1}{2} = \sum_{i=0}^{r-1} \frac{p-1}{2} p^i \rightarrow \beta = r\frac{p-1}{2}.$$

Clearly, $a(\beta)=(q-1)/2$ if and only if $r=1$. Therefore we have proved the following.

Corollary 8: For $p>2$ and $n=p^m-1$, an extended BCH code of length p^m over GF(p) is WSD if and only if its designed distance d satisfies $d > n/2$ (i.e., if and only if it is strictly contained in the EMB code whose designed distance is $n/2$).

C. Even EMB Codes and Even BCH Codes over GF(4)

In this section $K=$ GF(4). The length of the codes is 2^m with $m=2m'$. A code U with weights divisible by two is called an *even* code. There is only one non-trivial EMB code over GF(4). This is $B=B_e(4, d(1))$ with

$$d(1)=2\sum_{i=0}^{m'-1} 4^i = (0,1,0,1,\cdots,0,1); \qquad (22)$$

then

$$n-d(1)=t(1)=\sum_{i=0}^{m'-1} 4^i = (1,0,1,0,\cdots,1,0). \qquad (23)$$

We shall prove that B is the smallest noneven BCH code. The proof of Theorem 8 uses the following result due to MacWilliams *et al.* [9].

Theorem 7 [9]: Let U be a linear code of length N over K. Let the operation of conjugation be defined as follows. If $x \in K$, then $\bar{x}=x^2$. Let

$$\bar{U} = \left\{ \bar{u} = \left(u_1^2, \cdots, u_N^2\right) \mid u = (u_1, \cdots, u_N),\ u \in U \right\},$$

and let $\hat{U}$ be the dual of U. Then

$$U \text{ is an even code } \leftrightarrow \bar{U} \subset \hat{U}. \qquad (24)$$

Theorem 8: An extended BCH code is an even code over GF(4) if and only if its designed distance d satisfies $d > d(1)$ (i.e., if and only if it is strictly contained in the only nontrivial EMB code).

Proof: Let U be an extended BCH code with designed distance d. Let T be the definition set of U. Let I be the permutation on the elements of the interval $S=[0,n]$:

$$I:\ i \in S \rightarrow 2i \pmod n.$$

Let $s \in S$ and let u be a codeword of an extended cyclic code. Using the notation of (12), we have

$$\left(\sum_{i=0}^{n-1} u_i^2 (\alpha^i)^s\right)^2 = \sum_{i=0}^{n-1} u_i (\alpha^i)^{2s}.$$

This equality proves that α^{2s} is a zero of u if and only if α^s is a zero of $\bar{u}$. On the other hand, $\bar{U} \subset \hat{U}$ means that α^s is a zero of $\bar{u}$, for all $u \in U$ and for all $s \in \hat{T}$. We can say equivalently: $2s$ is in

T for all $s \in \hat{T}$. By (24) we have proved

$$U \text{ is an even code} \leftrightarrow I(\hat{T}) \subset T. \tag{25}$$

Let R be the definition set of B. From (5), (15), and (16), we have

$$I(\hat{R}) = \{ s \in S | s \ll 2t(1) \} \qquad I(\hat{R}) \setminus R = \{ 2t(1) \}$$

because $d(1) = 2t(1)$. Then we can deduce from (25) that B is not even; therefore, if $d \le d(1)$, U cannot be even.

Suppose now that $d > d(1)$. Then U is strictly contained in B, R is strictly contained in T, and $\hat{T}$ is strictly contained in $\hat{R}$. Since $d(1) \in T$, then $I(t(1)) \notin I(\hat{T})$. Thus $I(\hat{T}) \subset R \subset T$ and we have proved that U is an even code.

Remark: Results of Corollary 8 and Theorem 8 involve that Table I shows the even extended BCH codes when $q = 4$ and the WSD extended BCH codes when $q = p$ ($p > 2$), for $N < 5000$. Indeed, Table I gives the designed distance of the smallest BCH code which does not satisfy the property.

IV. EMB Codes as Ideals in a Modular Algebra

Let A be the modular group algebra $K[G]$. An element of A is a polynomial

$$x = \sum_{g \in G} x_g X^g, \qquad x_g \in K.$$

The operations of the algebra A are usual polynomial addition and multiplication: $X^g X^h = X^{g+h}$ and $x_g X^g + y_g X^g = (x_g + y_g) X^g$.

An extended cyclic code is an ideal of A if and only if it is an affine-invariant code. In this context, the EMB codes have interesting properties; using the algebraic tools that we have introduced, one can easily obtain the description of these special ideals. Our aim in this correspondence is not to explain this aspect of EMB codes. Nevertheless, we want to give the principal result with a short proof (the reader can find more details in [3], [5], and [6]).

Theorem 9: An MB code is a BCH code the extension of which is a principal ideal of the algebra A.

Proof: Let U be an extended BCH code with definition set T. Let F be the set of minimal elements of $S \setminus T$; that is,

$$F = \{ s \in S \setminus T | \text{ if } t \ll s, \text{ then } s = t \text{ or } t \in T \}.$$

We say that F is the *border* of U. We have proved that U is a principal ideal of A if and only if F has one and only one element [5]. By definition (see (5)) it is clear that the border of an EMB code is $\{d\}$, where d is its designed distance. Then an EMB code is a principal ideal of A.

Let d be the designed distance of U. Obviously if F has only one element, then $F = \{d\}$; therefore, $S \setminus T$ is the set of the ascendant of d. By Lemma 1, U is an EMB code.

Corollary 9: Let B be an EMB code with designed distance d (the minimum distance of B is $d+1$). Let x be a codeword of B with minimum weight. Then x is a generator of the principal A-ideal B.

Proof: Let P be the radical of the algebra A. Let a be a generator of the principal ideal B. Then the generators of B are the λa, $\lambda \in A \setminus P$. We have proved that the ideals product PB is an extended cyclic code with minimum distance strictly greater than $d+1$ (see [5] and [6]). Then a codeword of B which has weight $d+1$, is a generator of B.

References

[1] E. F. Assmus, H. F. Mattson, and R. J. Turyn, "On the Peterson and all affine-invariance theorem," Air Force Cambridge Res. Labs., Bedford, MA, Rep. AFCRL 67-0365, June 1967.

[2] P. Camion, "Etude de codes binaires abéliens modulaires autoduaux de petites longueurs," *Rev. CETHEDEC*, NS 79-2, pp. 3–24, 1979.

[3] P. Charpin, "The extended Reed–Solomon codes considered as ideals of a modular algebra," *Ann. Discrete Math.*, vol. 17, pp. 171–176, 1983.

[4] ——, "Codes cycliques étendus et idéaux principaux d'une algèbre modulaire," *C.R. Acad. Sci. Paris*, vol. 295, série I, pp. 313–315, Sept. 1982.

[5] ——, "A minimum system of generators for cyclic codes which are invariant under the affine group," in *AAECC3, Lecture Notes in Computer Science*, no. 229. Berlin, Germany: Springer-Verlag, 1986, pp. 34–42.

[6] ——, "Some applications of a classification of affine-invariant codes," *AAECC5, Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, to be published.

[7] T. Kasami, S. Lin, and W. W. Peterson, "Some results on cyclic codes which are invariant under the affine group and their applications," *Inform. Contr.*, vol. 11, pp. 475–496, 1967.

[8] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.

[9] F. J. MacWilliams, A. M. Odlyzko, N. J. A. Sloane, and H. N. Ward, "Self-dual codes over GF(4)," *J. Combinatorial Theory*, series A23, pp. 288–318, 1978.

[10] W. W. Peterson, *Error Correcting Codes*. New York: Wiley, 1961.

[11] C. Roos, "A new lower bound for the minimum distance of a cyclic code," *IEEE Trans. Inform. Theory*, vol. IT-29, no. 3, May 1983.

[12] J. H. Van Lint and R. M. Wilson, "On the minimum distance of cyclic codes," *IEEE Trans. Inform. Theory*, vol. IT-32, no. 1, pp. 23–40, 1986.

[13] J. Wolfmann, "A group algebra construction of doubly even self-dual binary codes," *Discrete Math.*, vol. 65, pp. 81–89, 1987.

On a New Binary [22, 13, 5] Code

ZHI CHEN, PINGZHI FAN, AND FAN JIN

If all codewords in a code C have the same weight, then C is called a constant weight code. Let $A(n, d, w)$ be the maximum number of codewords in any binary code of length n, constant weight w, and minimum distance d.

With the help of a VAX-11 computer, we have found a new binary [22,13,5] quasi-perfect code with generator matrix $G = [I | P^T]$, where

$$P = \begin{bmatrix} 0&0&0&0&0&0&0&1&1&1&1&1&1 \\ 0&0&0&0&1&1&1&0&0&0&0&0&1 \\ 0&0&1&1&0&0&1&0&0&1&1&1&0 \\ 0&1&0&1&0&1&0&0&1&0&1&1&1 \\ 0&1&1&0&1&0&0&1&0&1&0&1&1 \\ 1&0&0&1&0&1&1&0&1&1&0&1&0 \\ 1&0&1&0&1&1&1&1&0&1&1&0&1 \\ 1&1&0&1&1&0&0&1&0&1&1&1&0 \\ 1&1&1&0&0&0&1&1&1&0&1&1&1 \end{bmatrix}.$$

In Table I, we give the weight distributions $[A_0(v), A_1(v), \cdots, A_n(v)]$ of the coset codes $C + v$, for vectors v.

Obviously, our code is not equivalent to Wagner's code [1]. Four lower bounds for constant weight codes can be derived

Manuscript received November 7, 1988; revised March 20, 1989.

The authors are with the Department of Computer Science and Engineering, Southwest Jiaotong University, Emei, Sichuan, PRC.

IEEE Log Number 8931679.