INFORMATION AND CONTROL 18, 369–394 (1971)

The Weight Enumerators for Several Classes of Subcodes of the 2nd Order Binary Reed-Muller Codes*

T. Kasami

Department of Information Engineering, Osaka University, Toyonaka, Osaka Japan

In this paper explicit formulas for the weight enumerators for several classes of subcodes of the 2nd-order binary Reed–Muller codes are derived. A large set of the codes are shown to have the same weight enumerators. The classes of codes studied in this paper contain the (0, 2)th-order Euclidean Geometry codes and the codes studied by Berlekamp as subclasses.

Introduction

Recently, a theorem was proved by Berlekamp (1970) which asserts that all sufficiently low weight codewords in certain supercodes of the $(m-3)$rd-order Reed–Muller code must also be in the $(m-3)$rd-order Reed–Muller code. Theorem 1 is a simple generalization of Berlekamp theorem, Theorem 2 is a generalization of Berlekamp–Sloane theorem (1969), and Theorem A1 is an extension of the results by Berlekamp and Sloane (1970). These new results, in conjunction with previously known results, enable us to derive formulas for the weight enumerators for several classes of subcodes of the 2nd-order Reed–Muller codes. Theorems 3 and 4 show that a large set of the codes have the same weight enumerators. The classes of codes studied here contain the (0, 2)th-order Euclidean Geometry codes and the codes studied by Berlekamp (1970) as subclasses.

1. Definitions and Theorems on Weight Restriction

Let α be an element of order n in $GF(q^m)$, where q is a power of a prime p. Cyclic codes of length n over $GF(q)$ will be considered.

Let $v(X) = c_1X^{u_1} + c_2X^{u_2} + \cdots + c_tX^{u_t}$, where $0 \leqslant u_1 < u_2 < \cdots < u_t < n$, $c_i \neq 0$ and $c_i \in GF(q)$ with $1 \leqslant i \leqslant t$.

* The research reported in this paper was supported in part by NASA grant NGL-12-004-046.

Let[1] $R = \{e \mid v(\alpha^e) = 0\}$ and

$$f(X) = \prod_{i=1}^{t} (X - \alpha^{u_i}).$$

Lemma 1. *Let $\bar{R}$ be the subspace spanned by $\{X^e \mid e \in R\}$ of the residue classes modulo $f(X)$ over $GF(q^m)$. Then, for any $e \notin R$,*

$$X^e \notin \bar{R}.$$

Proof. Suppose that

$$X^e \equiv \sum_{j \in R} b_j X^j \bmod f(X),$$

where $b_j \in GF(q^m)$. Then, for $1 \leqslant i \leqslant t$,

$$\alpha^{eu_i} = \sum_{j \in R} b_j \alpha^{ju_i}.$$

Hence,

$$v(\alpha^e) = \sum_{i=1}^{t} c_i \alpha^{eu_i} = \sum_{i=1}^{t} \sum_{j \in R} c_i b_j \alpha^{ju_i} = \sum_{j \in R} b_j v(\alpha^j) = 0.$$

That is, $e \in R$.

Lemma 2. *Let a and A be positive integers, and let*

$$0 \leqslant w_1 < w_2 < \cdots < w_s < n.$$

Then, (1) *there are $b_1, \ldots, b_s$ in $GF(q^m)$ such that*

$$X^A \equiv \sum_{i=1}^{s} b_i X^{Ap^{ai}} \bmod f_0(X)$$

$$\left(\text{or } X^A \equiv b_1 + \sum_{i=2}^{s} b_i X^{Ap^{a(i-1)}} \bmod f_0(X)\right),$$

and (2) *there are $b_1, \ldots, b_s$ in $GF(q^m)$ such that*

$$X^{Ap^{as}} \equiv \sum_{i=1}^{s} b_i X^{Ap^{a(i-1)}} \bmod f_0(X)$$

$$\left(\text{or } X^{Ap^{a(s-1)}} \equiv b_1 + \sum_{i=2}^{s} b_i X^{Ap^{a(i-2)}} \bmod f_0(X)\right),$$

where $f_0(X) = (X - \alpha^{w_1}) \cdots (X - \alpha^{u_s})$.

[1] Exponents are to be taken as modulo n.

Proof. $X^A, X^{Ap^a}, \dots, X^{Ap^{as}}$ cannot be linearly independent in the residue classes modulo $f_0(X)$. Hence, there exist $b_l', \dots, b_s'$ in $GF(q^m)$ such that

$$\sum_{i=l}^{s} b_i' X^{Ap^{ai}} \equiv 0 \bmod f_0(X),$$

where $b_l' \neq 0$ and $0 \leqslant l < s$. Let j be the smallest nonnegative integer such that $p^{al+j} - 1$ is divisible by n. Then, $\alpha^{w_i A p^{al+j}} = \alpha^{w_i A}$ for $1 \leqslant i \leqslant s$. Hence,

$$X^{Ap^{al+j}} \equiv X^A \bmod f_0(X).$$

Thus,

$$\left(\sum_{i=l}^{s} b_i' X^{Ap^{ai}}\right)^{p^j} = b_l'^{p^j} X^A + \sum_{i=1}^{s-l} b_{i+l}'^{p^j} X^{Ap^{ai}} \equiv 0 \bmod f_0(X).$$

Since $b'^{p^i} \neq 0$, the first case holds. Similarly, the other three cases can be proved.

Let A_{ij} with $0 \leqslant i \leqslant l$ and $0 \leqslant j \leqslant t_i$ be nonnegative integers such that either

$$A_{ij} = A_i p^{a_i j} \quad \text{with} \quad A_i > 0 \quad \text{and} \quad a_i > 0 \quad \text{for} \quad 0 \leqslant j \leqslant t_i ,$$

or

$$A_{i0} = 0,$$
$$A_{ij} = A_i p^{a_i(j-1)} \quad \text{with} \quad A_i > 0 \quad \text{and} \quad a_i > 0 \quad \text{for} \quad 0 < j \leqslant t_i .$$

If $A_{00} \neq 0$, then let $\bar{j}_0 = 0$ and, otherwise, let $\bar{j}_0 = 1$.

THEOREM 1. *Suppose that* $A_0 + \sum_{i=1}^{l} A_{it} \notin R$ *and that except for* $j_0 = \bar{j}_0$, $j_1 = t_1, \dots, j_l = t_l$,

$$\sum_{i=0}^{l} A_{ij_i} \in R \qquad \text{with} \qquad 0 \leqslant j_i \leqslant t_i .$$

Then,

$$t > \sum_{i=0}^{l} t_i .$$

Proof. Assume that $t \leqslant \sum_{i=0}^{l} t_i$. Then, by Lemma 2 there exist b_{ij}'s in $GF(q^m)$ such that

$$X^{A_0} \equiv \sum_{j=0}^{t_0} b_{0j} X^{A_{0j}} \bmod (X - \alpha^{u_{01}}) \cdots (X - \alpha^{u_{0t_0}})$$

$$X^{A_{it_i}} \equiv \sum_{j=0}^{t_i-1} b_{ij} X^{A_{ij}} \bmod (X - \alpha^{u_{i1}}) \cdots (X - \alpha^{u_{it_i}}) \qquad \text{for} \qquad 1 \leqslant i \leqslant l,$$

where $b_{0\bar{j}_0} = 0$ and $\{u_{ij} \mid 0 \leqslant i \leqslant l,\ 1 \leqslant j \leqslant t_i\} = \{u_i \mid 1 \leqslant i \leqslant t\}$. Hence,

$$\left(X^{A_0} - \sum_{j=0}^{t_0} b_{0j} X^{A_{0j}}\right) \prod_{i=1}^{l} \left(X^{A_{it_i}} - \sum_{j=0}^{t_i-1} b_{ij} X^{A_{ij}}\right) \equiv 0 \bmod f(X).$$

Thus, residue class $X^{A_0 + \sum_{i=1}^{l} A_{it_i}}$ is a linear sum of residue classes $X^{\sum_{i=0}^{l} A_{ij_i}}$ with $0 \leqslant j_0 \leqslant t_0$, $0 \leqslant j_1 \leqslant t_1, \ldots, 0 \leqslant j_l \leqslant t_l$ except for $j_0 = \bar{j}_0$, $j_1 = t_1, \ldots, j_l = t_l$. From Lemma 1 it follows that

$$A_0 + \sum_{i=1}^{l} A_{it_i} \in R.$$

This is a contradiction. Consequently, $t > \sum_{i=0}^{l} t_i$.

Remark 1. Let $t_0 = 0$, $t_i = 1$, $A_{00} = 1$, $A_{i0} = 0$, and $A_{i1} = 1$ for $1 \leqslant i \leqslant l$. Then, we have the BCH bound.

Remark 2. Let C be a binary cyclic code of length $2^m - 1$ whose generator polynomial is $g(X)$, and let α be a primitive element of $GF(2^m)$. Suppose that $g(X)$'s roots include α^e for all e in the set

$$1 + 2^{b+a},\ 1 + 2^{b+2a}, \ldots,\ 1 + 2^{b+ua},$$

where a is a positive integer relatively prime to m, b is a nonnegative integer, and u is a positive integer less than m.

(1) If $v \in C$ is a code-word of weight $\leqslant u$, then v is also a code-word in the $(m - 3)$rd-order cyclic Reed–Muller code of length $2^m - 1$.

(2) If $g(\alpha) = 0$, u is even (or odd) and $v \in C$ is a code-word of weight $\leqslant u + 2$ (or $u + 1$), then v is also a code-word in the $(m - 3)$rd-order cyclic Reed–Muller code of length $2^m - 1$.

The proof is similar to the one of Corollary 1. Remark 2 is a strengthened form of Berlekamp's Theorem (Berlekamp, 1970). In (2) of Remark 2, let either $a = 1$, $b = m - t + 1$, $u = 2t - 1$ or $a = 1$, $b = s$, $u = 2t - 1$.

Then, we have Berlekamp's Theorem. His assumption that C is invariant under the translational group is removed. For even u, this remark gives a stronger result.

Let (a, b) denote the greatest common divisor of integers a and b. Let[2]

$$u_1(m, j) = \left\lfloor \frac{m}{2(m, j)} \right\rfloor + 1,$$

and if $m/(m, j)$ is odd, let

$$u_2(m, j) = u_1(m, j)$$

and if $m/(m, j)$ is even, let

$$u_2(m, j) = \left\lceil \frac{m}{4(m, j)} \right\rceil.$$

For $1 \leqslant j \leqslant m/2$ and $1 \leqslant u \leqslant u_1(m, j)$, let $\mathscr{B}_j^{(u)}$ be the cyclic code of length $2^m - 1$ whose generator polynomial is

$$g(X) = \prod_{i=0}^{u-1} M^{(1+2^{ij})}(X),$$

where $M^{(l)}(X)$ is the minimal polynomial of α^l and α is a primitive element in $GF(2^m)$. For $1 \leqslant j \leqslant m/2$ and $2 \leqslant u \leqslant u_2(m, j) + 1$, let $\mathscr{D}_j^{(u)}$ be the cyclic code of length $2^m - 1$ whose generator polynomial is

$$g(X) = M^{(1)}(X) \prod_{i=0}^{u-2} M^{(1+2^{j(2i+1)})}(X).$$

For $1 \leqslant j \leqslant m/2$ and $1 \leqslant u \leqslant u_2(m, j)$, let $\mathscr{F}_j^{(u)}$ be the cyclic code of length $2^m - 1$ whose generator polynomial is[3]

$$g(X) = \prod_{i=0}^{u-1} M^{(1+2^{j(2i+1)})}(X).$$

For even m, $1 \leqslant j \leqslant m/2$ and $1 \leqslant u \leqslant \lceil m/(2(m, j)) \rceil$, let $\mathscr{H}_j^{(u)}$ be the cyclic code of length $2^m - 1$ whose generator polynomial is

$$g(X) = M^{(1)}(X) \prod_{i=0}^{u-1} M^{(1+2^{m/2-ij})}(X).$$

[2] $\lfloor a \rfloor$ denotes the greatest integer not greater than a, and $\lceil a \rceil$ denotes the smallest integer not less than a.

[3] In general, $\mathscr{F}_j^{(u)}$ is not invariant under the affine group of permutations.

For even m, $1 \leqslant j \leqslant m/2$ and $1 \leqslant u \leqslant \lceil m/(2(m, j)) \rceil$, let $\mathscr{J}_j^{(u)}$ be the cyclic code of length $2^m - 1$ whose generator polynomial is

$$g(X) = \prod_{i=0}^{u-1} M^{(1+2^{m/2-ij})}(X).$$

Then, the extended code of $\mathscr{B}_1^{(u)}$ is identical with $\mathscr{B}^{(u)}$ in (Berlekamp, 1970), and for odd m (or even m) the extended code of $\mathscr{D}_{(m-1)/2}^{(u)}$ (or $\mathscr{H}_1^{(u)}$) is identical with $\mathscr{D}^{(u)}$ in (Berlekamp, 1970).

The duals of $\mathscr{B}_j^{(u)}$, $\mathscr{D}_j^{(u)}$, $\mathscr{F}_j^{(u)}$, $\mathscr{H}_j^{(u)}$, and $\mathscr{J}_j^{(u)}$ will be denoted by $\mathscr{A}_j^{(u)}$, $\mathscr{C}_j^{(u)}$, $\mathscr{E}_j^{(u)}$, $\mathscr{G}_j^{(u)}$, and $\mathscr{I}_j^{(u)}$, respectively. The duals of the even parts of $\mathscr{B}_j^{(u)}$, $\mathscr{D}_j^{(u)}$, $\mathscr{F}_j^{(u)}$, $\mathscr{H}_j^{(u)}$, and $\mathscr{J}_j^{(u)}$ will be denoted by $\bar{\mathscr{A}}_j^{(u)}$, $\bar{\mathscr{C}}_j^{(u)}$, $\bar{\mathscr{E}}_j^{(u)}$, $\bar{\mathscr{G}}_j^{(u)}$ and $\bar{\mathscr{I}}_j^{(u)}$, respectively.[4] For even m, $A_2^{(m/2+1)}$ is the (0, 2)th-order Euclidean Geometry codes (Weldon (1967), Berlekamp (1968)).

Corollary 1.

(1) *If* $v \in \mathscr{B}_j^{(u)}$ *is a code-word of weight* $\leqslant 2u$, *then* v *is also a code-word in* $\mathscr{B}_{(m,j)}^{(u_1(m,j))}$.

(2) *If* $(m, j) = (m, 2j)$, *and if* $v \in \mathscr{D}_j^{(u)} \cup \mathscr{F}_j^{(u)}$ *is a code-word of weight* $\leqslant 2u$, *then* v *is also a code-word in* $\mathscr{B}_{(m,j)}^{(u_1(m,j))}$.

(3) *If* $(m, j) \neq (m, 2j)$, *and if* $v \in \mathscr{H}_j^{(u)}$ (*or* $\mathscr{J}_j^{(u)}$) *is a code word of weight* $\leqslant 2u$ (*or* $2u - 1$), *then* v *is also a code-word in* $\mathscr{B}_{(m,j)}^{(u_1(m,j))}$.

(4) *If* $(m, j) \neq (m, 2j)$, *and if* $v \in \mathscr{D}_j^{(u)}$ (*or* $\mathscr{F}_j^{(u)}$) *is a codeword of weight* $\leqslant 2u$, *then* v *is also a codeword in* $\mathscr{D}_{(m,j)}^{(u_2(m,j)+1)}$ (*or* $\mathscr{F}_{(m,j)}^{(u_2(m,j))}$).

(5) *If* m *is even and* $(m, j) = (m, 2j)$, *and if* $v \in \mathscr{H}_j^{(u)}$ (*or* $\mathscr{J}_j^{(u)}$) *is a code-word of weight* $\leqslant 2u$ (*or* $2u - 1$) *then* v *is also a codeword in* $\mathscr{D}_{(m,j)/2}^{(u_1(m,j)+1)}$ (*or* $\mathscr{F}_{(m,j)/2}^{(u_1(m,j))}$).

Proof. By definition, $\mathscr{D}_j^{(u)}$ has $\alpha^{1+2^j}, \alpha^{1+2^{3j}}, \ldots, \alpha^{1+2^{(2v-3)j}}$ as roots of the generator polynomial. Hence,

$$\alpha^{2^{m-j}(1+2^j)} = \alpha^{1+2^{m-j}}, \alpha^{2^{m-3j}(1+2^{3j})} = \alpha^{1+2^{m-3j}}, \ldots, \alpha^{2^{m-(2u-3)j}(1+2^{(2u-3)j})} = \alpha^{1+2^{m-(2u-3)j}}$$

are also roots of the generator polynomial. Let $v(X)$ be the polynomial corresponding to code-word v. Suppose that $v(\alpha^{1+2^{j(2i+1)}}) = 0$ for all i with $0 \leqslant i \leqslant m$. It is shown easily that if $(m, j) = (m, 2j)$, then

$$\{j(2i+1) \mid 0 \leqslant i < m\} = \{(m, j)i \mid 0 \leqslant i < m\}$$

[4] The subcode of C consisting of all the even weight codewords will be called the even part of C.

and otherwise, $\{j(2i+1) \mid 0 \leqslant i < m\} = \{(m, j)(2i+1) \mid 0 \leqslant i < m\}$. Hence, if $(m, j) = (m, 2j)$, then $v \in \mathscr{B}_{(m,j)}^{(u_1(m,j))}$ and otherwise, $v \in \mathscr{D}_{(m,j)}^{(u_2(m,j)+1)}$. Suppose that there is an $i_0 \geqslant u - 1$ such that $v(\alpha^{1+2^{j(2i+1)}}) = 0$ for $0 \leqslant i < i_0$, and $v(\alpha^{1+2^{j(2i_0+1)}}) \neq 0$. If the weight of v is even, then let $p = 2$, $l = 1$, $t_0 = 1$, $A_{00} = 0$, $A_{01} = 1$, $t_1 = u + i_0$, $A_{10} = 0$, $A_1 = 2^{m-(2u-3)j}$, and $a_1 = 2j$. Then, Theorem 1 guarantees that the weight of v is greater than $t_0 + t_1 = 1 + i_0 + u \geqslant 2u$. If the weight of v is odd, then let $p = 2$, $l = 1$, $t_0 = 0$, $A_{00} = 1$, $t_1 = u + i_0$, $A_{10} = 0$, $A_1 = 2^{m-(2u-3)j}$ and $a_1 = 2j$. By Theorem 1, the weight of v is greater than $2u - 1$. Thus, (2) of this corollary holds for $\mathscr{D}_j^{(u)}$. Similarly, the other cases can be proved.

$W_q(i)$ will denote the sum of the coefficients of the radix-q form of i. For positive integers t and j, let $K(t, j) = \{i > 0 \mid W_2(i) > t\} \cup \{i \mid W_2(i) = t$ and $i \geqslant 2^{t+2}\} \cup \{i \mid i = 2^{t+2} - 2^h - 2^{h-lj} - 1$, where h and l are positive integers such that $lj < h < t + 2\}$. Let α be a primitive element of $GF(2^m)$.

THEOREM 2. *Let j be a positive integer which divides $m - r + 2$. If $w < 2^{m-r+1} - 2$ with $2 \leqslant r \leqslant m - 2$ and if the roots of the generator polynomial of a binary cyclic code C of length $2^m - 1$ include all α^i for which*

$$1 \leqslant i \leqslant 2w$$

and

$$i \notin K(m - r, j),$$

then the extended code of C contains no code-words of weight w unless $w = 2^{m-r+1} - 2^{lj-1}$ for some l with $1 \leqslant l \leqslant (m - r + 2)/j$. The proof of this theorem is stated in Appendix II.[5]

COROLLARY 2.

(1) *If $v \in \mathscr{G}_j^{(u)} \cup \mathscr{I}_j^{(u)}$, where $m/(m, j)$ is even or $v \in \mathscr{A}_j^{(u)} \cup \mathscr{C}_j^{(u)} \cup \mathscr{E}_j^{(u)}$, then the weight of v is of the form*

$$2^{m-1} + \epsilon 2^{i-1},$$

where $m/2 \leqslant i \leqslant m$, i is divisible by (m, j) and ϵ is either 0, 1, *or* -1.

(2) *If $v \in \mathscr{A}_j^{(u)}$ and $v \neq 0$, then*

$$i \leqslant m/2 + (u - 1)j.$$

(3) *If $v \in \mathscr{C}_j^{(u)}$ and $v \neq 0$, then*

$$i \leqslant m/2 + (2u - 3)j.$$

[5] Casual readers may skip the proof since in this paper this theorem is used only for the case of $r = 2$, which is covered by Lemma A1.

(4) *If* $v \in \mathscr{E}_j^{(u)}$ *and* $v \neq 0$, *then*

$$i \leqslant m/2 + (2u - 1)j.$$

(5) *If* $v \in \mathscr{G}_j^{(u)} \cup \mathscr{I}_j^{(u)}$, $v \neq 0$, *and* $m/(m, j)$ *is even, then*

$$i \leqslant m/2 + (u - 1)j.$$

Proof. (1) Since $\mathscr{A}_j^{(u)}$, $\mathscr{C}_j^{(u)}$, $\mathscr{E}_j^{(u)}$, $\mathscr{G}_j^{(u)}$, and $\mathscr{I}_j^{(u)}$ are subcodes of the second-order cyclic Reed–Muller code, the weight w must be of the form

$$2^{m-1} + \epsilon 2^{i-1},$$

where $m/2 \leqslant i \leqslant m$ and ϵ is either 0, 1 or -1 (Kasami (1967)). If $w < 2^{m-1}$ with $m \geqslant 5$, then $w < 2^{m-1} - 2$. By Theorem 2, i is divisible by mod(m, j). If $m \leqslant 4$ and $w = 2^{m-1} \pm 2$, then i is divisible by (m, j). Assume that $w = 2^{m-1} + 2^{i-1}$, with $i > 2$ and i is not divisible by (m, j). Then, since $\bar{\mathscr{A}}_j^{(u)}$, $\bar{\mathscr{C}}_j^{(u)}$, $\bar{\mathscr{E}}_j^{(u)}$, $\bar{\mathscr{G}}_j^{(u)}$, and $\bar{\mathscr{I}}_j^{(u)}$ contain the all one vector, the extended codes of $\bar{\mathscr{A}}_j^{(u)}$, $\bar{\mathscr{C}}_j^{(u)}$, $\bar{\mathscr{E}}_j^{(u)}$, $\bar{\mathscr{G}}_j^{(u)}$ and $\bar{\mathscr{I}}_j^{(u)}$ contain a code-word of weight $2^{m-1} - 2^{i-1}$. This contradicts Theorem 2. (This part also follows immediately from Lemma A1.)

(2) Since $\mathscr{A}_j^{(u)}$ is a subcode of the dual of the $1 + 2^{(u-1)j-1}$ error correcting BCH code, the Carlitz–Uchiyama bound (Berlekamp (1970)) guarantees that its minimum weight d is bounded by

$$d \geqslant 2^{m-1} - 2^{m/2+(u-1)j-1}.$$

That is, if $v \in \mathscr{A}_j^{(u)}$, then

$$i \leqslant m/2 + (u - 1)j.$$

Similarly, (3) and (4) can be proved.

(5) The BCH bound guarantees that the minimum weight d of $\mathscr{G}_j^{(u)}$ or $\mathscr{I}_j^{(u)}$ is bounded by

$$d \geqslant 2^{m-1} - 2^{m/2+(u-1)j-1}. \tag{1}$$

This implies part (5), if $m/(m, j)$ is even.

For nonprimitive cases, the following corollary holds:

COROLLARY 3. *Let* m *be even, let* $1 \leqslant j_1 \leqslant m/2$, *and let* $j = (m, j_1)$.

(1) *If* $v \in \mathscr{E}_{j_1}^{(u)}$, $v \neq 0$, *and* m/j *is even, then the weight of* v *is of the form*

$$2^{m-1} - (-1)^i \, 2^{m/2+ij-1}, \qquad \textit{with} \qquad 0 \leqslant i \leqslant (2u - 1)\, j_1/j.$$

(2) *If* $v \in \mathscr{I}_{j_1}^{(u)}$, $v \neq 0$ *and* m/j *is odd, then the weight of* v *is of the form*

$$2^{m-1} - (-1)^i \, 2^{m/2+ij/2-1}, \qquad \text{with} \qquad 0 \leqslant i \leqslant (2u-2)\, j_1/j.$$

Proof. (1) $\mathscr{E}_{j_1}^{(u)}$ is a subcode of $\mathscr{E}_j^{(u_2(m,j))}$. Since m/j is even, $2^m - 1$ is divisible by $2^j + 1$. Hence, the order of α^{1+2^j} is $(2^m - 1)/(2^j + 1)$. Since $2^{j(2i+1)} + 1$ is divisible by $2^j + 1$, a codeword of $\mathscr{E}_j^{(u_2(m,j))}$ is derived from a codeword of a code of length $(2^m - 1)/(2^j + 1)$ by repeating $(2^j + 1)$-times. Hence, the weight of a codeword of $\mathscr{E}_j^{(u_2(m,j))}$ is divisible by $2^j + 1$. Thus, by Corollary 2, part 4, the weight w of a nonzero codeword of $\mathscr{E}_{j_1}^{(u)}$ is either

$$w = 2^{m-1} - 2^{i-1},$$

where $m/2 \leqslant i \leqslant m/2 + (2u-1)j_1$ and $(m-i)/j$ is even, or

$$w = 2^{m-1} + 2^{i-1},$$

where $m/2 \leqslant i \leqslant m/2 + (2u-1)j_1$ and $(m-i)/j$ is odd. Since m is divisible by $2j$, w is of the form

$$2^{m-1} - (-1)^i \, 2^{m/2+ij-1}, \qquad \text{with} \qquad 0 \leqslant i \leqslant (2u-1)\, j_1/j.$$

(2) Since m is even and m/j is odd, j must be even. By definition, $\mathscr{I}_j^{(u)}$ is a subcode of $\mathscr{E}_{j/2}^{(u_2(m,j/2))}$. From the proof of part (1), w is of the form

$$w = 2^{m-1} - (-1)^i \, 2^{m/2+ij/2-1},$$

where $0 \leqslant i \leqslant m/j$. By the BCH bound (1) for $\mathscr{I}_j^{(u)}$,

$$0 \leqslant i \leqslant 2(u-1)\, j_1/j.$$

2. Some Theorems on Weight Distribution

In this section, a large subset of the codes defined in Section 2 are shown to have the same weight enumerators.

Let C and C' be q-ary linear codes of the same length n and the same dimension k, and let C_d and C_d' be the duals of C and C', respectively. Let A_w and A_w' denote the number of code-words of weight w in C and C', and let B_w and B_w' denote the number of code-words of weight w in C_d and C_d', respectively.

Lemma 3. *Let* $0 < w_1 < \cdots < w_{2u} < n$. *Suppose that* $A_w = 0$ *for either* $0 < w < w_1$ *or* $w_{2u} < w < n$, *and that* $A_w' = A_w$ *unless either* $0 < w < w_1$,

$w_{2u} < w < n$ or $w = w_i$ with $1 \leqslant i \leqslant 2u$. If $B_w = B_w{}'$ for $0 \leqslant w \leqslant 2u$, then $A_w = A_w{}'$ for all w.

Proof. If $w_1 = 1$ and $w_{2u} = n - 1$, then this lemma follows directly from the Pless Theorem (Pless (1963)). Assume that $w_{2u} < n - 1$. (In case that $w_1 > 1$, almost the same argument holds.) Let $w_{2u+1} = w_{2u} + 1 < n$. By the Pless power-moment identities (Pless (1963), Berlekamp (1968)) for C and C', we have that for $t \geqslant 0$,

$$\sum_{w_1 \leqslant w \leqslant w_{2u+1}} w^t A_w = q^k \sum_{i=0}^{t} B_i F_t^{(i)}(n) - \varDelta_t - n^t A_n , \tag{2}$$

$$\sum_{w_1 \leqslant w \leqslant w_{2u+1}} w^t A_w{}' + \sum_{w=1}^{w_1-1} w^t A_w{}' + \sum_{w > w_{2u+1}}^{n-1} w^t A_w{}'$$
$$= q^k \sum_{i=0}^{t} B_1{}' F_t^{(i)}(n) - \varDelta_t - n^t A_n{}', \tag{3}$$

where $\varDelta_0 = 1$, $\varDelta_t = 0$ for $t \geqslant 1$ and $F_t^{(i)}(n)$ is dependent only on i, t, q, and n. Then, we have that for $0 \leqslant t \leqslant 2u$,

$$\sum_{i=1}^{2u+1} w_i^t (A'_{w_i} - A_{w_i}) + \sum_{w=1}^{w_1-1} w^t A_w{}' + \sum_{w > u'_{2u+1}}^{n-1} w^t A_w{}' = 0.$$

Let $\delta_0, \ldots, \delta_{2u}$ be the elements of the last row of the inverse matrix of

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ w_1 & w_2 & & w_{2u+1} \\ w_1{}^2 & w_2{}^2 & & w_{2u+1}^2 \\ \vdots & \vdots & & \vdots \\ (w_1)^{2u} & \cdot & & (w_{2u+1})^{2u} \end{bmatrix}.$$

Then,

$$\sum_{t=0}^{2u} \delta_t \left[\sum_{i=1}^{2u+1} w_i{}^t (A'_{w_i} - A_{w_i}) + \sum_{w=1}^{w_1-1} w^t A_w{}' + \sum_{w > w_{2u+1}}^{n-1} w^t A_w{}' \right]$$
$$= A'_{w_{2u+1}} + \sum_{w=1}^{w_1-1} A_w{}' \sum_{t=0}^{2u} \delta_t w^t + \sum_{w > w_{2u+1}}^{n-1} A_w{}' \sum_{t=0}^{2u} \delta_t w^t$$
$$= 0.$$

From the known property of van der Monde determinant,

$$\sum_{t=0}^{2u} \delta_t w^t > 0, \qquad \text{for} \qquad w < w_1 \qquad \text{or} \qquad w > w_{2u}.$$

Hence, we have

$$A_w' = 0 \qquad \text{for} \quad 0 < w < w_1 \quad \text{or} \quad w_{2u} < w < n.$$

Thus, by (2) and (3) we have Lemma 3.

Now, we have the following theorem:

THEOREM 3. *Let j be a factor of m such that m/j is odd and $m \neq j$. For any positive integers j_1, j_2, and j_3 such that $(m, j_1) = (m, j_2) = (m, j_3) = j$, $\mathscr{A}_{j_1}^{(u)}, \mathscr{C}_{j_2}^{(u)}$ and $\mathscr{E}_{j_3}^{(u)}$ (or $\mathscr{B}_{j_1}^{(u)}, \mathscr{D}_{j_2}^{(u)}$ and $\mathscr{F}_{j_3}^{(u)}$) have the same weight enumerators as $\mathscr{A}_j^{(u)}$ (or $\mathscr{B}_j^{(u)}$), where $1 \leqslant u \leqslant u_1(m, j)$.*

Proof. Since $\mathscr{A}_{j_1}^{(u)}$, $\mathscr{C}_{j_2}^{(u)}$ and $\mathscr{E}_{j_3}^{(u)}$ are subcodes of $\mathscr{A}_j^{(u_1(m,j))}$, there is no code-word of weight w unless w is of the form

$$w = 2^{m-1} + \epsilon 2^{i-1}, \tag{4}$$

where $\epsilon = 0$ or ± 1, $m/2 \leqslant i \leqslant m$ and i is divisible by j (Corollary 2, part (1)).

By Corollary 2, part (2), there is no code-word of weight w in $\mathscr{A}_j^{(u)}$ unless $w = 0$, 2^{m-1} or some number of the form $w = 2^{m-1} \pm 2^{i-1}$ with $m/2 \leqslant i \leqslant m/2 + (u-1)j$ and $i \equiv 0 \pmod{j}$. Since m is not divisible by $2j$, w is either 0, 2^{m-1} or

$$2^{m-1} \pm 2^{(m-j)/2+ij-1} \qquad \text{with} \quad 1 \leqslant i \leqslant u-1. \tag{5}$$

By the assumption, $(m, j_1) = (m, j_2) = (m, j_3) = j = (m, 2j) = (m, 2j_2) = (m, 2j_3)$. Since $\mathscr{B}_j^{(u)}$, $\mathscr{B}_{j_1}^{(u)}$, $\mathscr{D}_{j_2}^{(u)}$ and $\mathscr{F}_{j_3}^{(u)}$ are supercodes of $\mathscr{B}_j^{(u_1(m,j))}$, Corollary 1, parts (1) and (2) imply that $\mathscr{B}_j^{(u)}$, $\mathscr{B}_{j_1}^{(u)}$, $\mathscr{D}_{j_2}^{(u)}$, and $\mathscr{F}_{j_3}^{(u)}$ have the same number of code-words of weight w for $0 \leqslant w \leqslant 2u$. Consequently, this theorem follows from Lemma 3.

Remark 3. Consider $\mathscr{E}_j^{(2)}$, where $m/(m, j)$ is odd. Then $\alpha^{1+2^{3j}} = \alpha^{(1+2^j)(1-2^j+2^{2j})}$, and α^{1+2^j} and $\alpha^{1+2^{3j}}$ are primitive elements of $GF(2^m)$. Theorem 3 and weight restriction (5) imply that the cross-correlation between two maximal linear shift register sequences with recurrent polynomials $M^{(1)}(X)$ and $M^{(1-2^j+2^{2j})}(X)$ is a three-valued correlation. This was first proved by Welch (1969) by a different approach.

THEOREM 4. *Let* $1 \leqslant j_1 \leqslant m/2$ *and let* $j = (m, j_1)$. *For* $1 \leqslant u \leqslant u_2(m, j)$, $\mathscr{E}_{j_1}^{(u)}$ *and* $\mathscr{E}_j^{(u)}$ (*or* $\mathscr{F}_{j_1}^{(u)}$ *and* $\mathscr{F}_j^{(u)}$) *have the same weight enumerators.*

Proof. If m/j is odd, then this theorem is covered by Theorem 3. Suppose that m/j is even. By Corollary 3, part (1), the weight of a nonzero codeword in $\mathscr{E}_j^{(u)}$ (or $\mathscr{E}_{j_1}^{(u)}$) is of the form,

$$2^{m-1} - (-1)^i \, 2^{m/2+ij-1},$$

where $0 \leqslant i \leqslant 2u - 1$ (or $0 \leqslant i \leqslant (2u - 1) j_1/j$). Corollary 1, part (4) shows that $\mathscr{F}_j^{(u)}$ and $\mathscr{F}_{j_1}^{(u)}$ have the same number of code-words of weight w for $0 \leqslant w \leqslant 2u$. Thus, Theorem 4 follows from Lemma 3.

We use a version of the theorem due to McEliece (1970). Let C be a binary cyclic code of length $n = 2^m - 1$ whose check polynomial's roots are $\{\alpha^i \mid i \in Q\}$. Let $S_0, S_1, \ldots, S_{n-1}$ be elements of $GF(2^m)$ such that

$$S_i = 0, \qquad \text{unless } i \in Q, \tag{6}$$

$$S_{2i} = S_i^2, \tag{7}$$

where suffices are to be taken as modulo n.

THEOREM (McEliece). *Suppose that for all* $\nu < l$ *and for all* $S_0, S_1, \ldots, S_{n-1}$ *satisfying conditions* (6) *and* (7),

$$\sum_{i_1+i_2+\cdots+i_\nu\equiv 0} S_{i_1} S_{i_2} \cdots S_{i_\nu} = 0.$$

Then, the weight of a code-word of C *is divisible by* 2^{l-1}, *and the number of codewords of* C *whose weight is divisible by* 2^l *is equal to the number of n-tuples* $(S_0, \ldots, S_{n-1})$ *which satisfy the following condition besides* (6) *and* (7):

$$\sum_{i_1+i_2+\cdots i_l\equiv 0 (\mathrm{mod}\, n)} S_{i_1} S_{i_2} \cdots S_{i_l} = 0.$$

Let l have the same meaning as in the McEliece Theorem, and let Q' be the set of those i's in Q for which there exist $i_2, \ldots, i_l$ in Q such that

$$i + i_2 + \cdots + i_l \equiv 0 \bmod 2^m - 1.$$

Let C' be a cyclic code of length $2^m - 1$ whose check polynomial's roots are $\{\alpha^i \mid i \in Q'\}$. Then, the following simple corollary holds:

COROLLARY 4. *C and C' have the same ratio of the number of code-words whose weight is divisible by 2^l to the total number of code-words.*

For example, if m is even, then $\mathscr{G}_j^{(u)}$ and $\mathscr{I}_j^{(u)}$ have the same ratio of the number of code-words with weight $2^{m-1} \pm 2^{m/2-1}$ to the total number of code-words.

There are some questions. For j_1 and j_2 such that $(m, j_1) = (m, j_2)$ and $m/(m, j_1)$ is even, do $\mathscr{A}_{j_1}^{(u)}$ and $\mathscr{A}_{j_2}^{(u)}$ (or $\mathscr{G}_{j_1}^{(u)}$ and $\mathscr{G}_{j_2}^{(u)}$, or $\mathscr{I}_{j_1}^{(u)}$ and $\mathscr{I}_{j_2}^{(u)}$) have the same weight distribution? Are the codes stated in Theorems 3 or 4 isomorphic to each other under some permutation of the coordinates?

Very little is known on the weight structure of subcodes of the 3rd or high order Reed–Muller code (or supercodes of the $(m-4)$th or lower order Reed–Muller code). The following remark on the minimum weight code-words is a strengthened version of Theorem 11 in (Kasami–Lin–Peterson (1968a)).

Remark 4. Let C be a p-ary cyclic code of length $p^{ms} - 1$ with generator polynomial $g(X)$, let β be a primitive element of $GF(p^{ms})$ and let $1 \leqslant c < m$. If $g(\beta^i) = 0$ for every i such that

$$0 < i < 2(p^{(m-c)s} - 1),$$
$$W_{p^s}(i) < (m-c)(p^s - 1),$$

then any code-word of minimum weight $p^{(m-c)s} - 1$ is a scalar multiple of the incidence vector[6] of an $(m-c)$-flat through the origin in $EG(m, p^s)$.

This remark is proved by showing that the reciprocal of the locator polynomial of a code-word of weight $p^{(m-c)s} - 1$ is an affine polynomial.

3. WEIGHT ENUMERATORS

In this section, weight enumerator formulas will be derived for $\mathscr{E}_j^{(u)}$ with all possible u and j, for $\mathscr{A}_j^{(u)}$ and $\mathscr{C}_j^{(u)}$ with odd $m/(m, j)$, for $\mathscr{A}_j^{(u)}$ and $\mathscr{G}_j^{(u)}$, where m is divisible by j and m/j is even, and for $\mathscr{I}_j^{(u)}$, where m is divisible by j. By Theorems 3 and 4, we assume without loss of generality that m is divisible by j. Weight enumerator formulas for $\mathscr{A}_1^{(u)}$ and $\mathscr{C}_1^{(u)}$ with odd m and for $\mathscr{A}_1^{(u)}$ and $\mathscr{G}_1^{(u)}$ with even m were derived by Berlekamp (1970). Except for these two cases, the following results are new.

[6] The component corresponding to the origin is deleted.

3.1 *Weight Enumerators for $\mathscr{A}_j^{(u)}$, $\mathscr{C}_j^{(u)}$, and $\mathscr{E}_j^{(u)}$ with Odd m/j*

Let j be a factor of m such that m/j is an odd integer greater than 1. By Theorem 3, $\mathscr{A}_j^{(u)}$, $\mathscr{C}_j^{(u)}$, and $\mathscr{E}_j^{(u)}$ have the same weight enumerators. Formulas for weight enumerators for $\mathscr{A}_j^{(u)}$ with $1 \leqslant u \leqslant u_1(m, j)$ will be derived below. $A_w^{(u)}$ and $B_w^{(u)}$ will denote the number of code-words of weight w in $\bar{\mathscr{A}}_j^{(u)}$ and $\mathscr{B}_j^{(u)}$, respectively. $\mathscr{A}_j^{(u)}$ is the even part of $\bar{\mathscr{A}}_j^{(u)}$. Since $\bar{\mathscr{A}}_j^{(u)}$ is invariant under the affine group of permutations, the following equation due to Prange holds (Berlekamp, 1968):

$$A_{2i-1}^{(u)} = A_{2^m-2i}^{(u)} = 2iA_{2i}^{(u)}/(2^m - 2i). \tag{8}$$

Hence, it is sufficient to find $A_{2i}^{(u)} + A_{2^m-2i}^{(u)}$.[7] For $1 \leqslant i \leqslant u - 1$, let

$$a_i^{(u)} = 2^{-mu}(A^{(u)}_{2^{m-1}-2^{(m-j)/2+ij-1}} + A^{(u)}_{2^{m-1}+2^{(m-j)/2+ij-1}}). \tag{9}$$

(Refer to (5).) By the Pless translated power moment identities with center 2^{m-1} (Pless (1963), Berlekamp (1968)), we have that for $1 \leqslant u < u_1(m, j)$ and $t \geqslant 1$,

$$2^{2mt-mu} + \sum_{i=1}^{u} 2^{(m+2ij-j)t} a_i^{(u)} = \sum_{i=0}^{2t} B_i^{(u)} F_{2t}^{(i)}(2^m - 1), \tag{10}$$

$$2^{2mt-m(u+1)} + \sum_{i=1}^{u} 2^{(m+2ij-j)t} a_i^{(u+1)} = \sum_{i=0}^{2t} B_i^{(u+1)} F_{2t}^{(i)}(2^m - 1). \tag{11}$$

By Corollary 1, $B_i^{(u)} = B_i^{(u+1)}$ for $0 \leqslant i \leqslant 2u$. Hence, for $1 \leqslant t \leqslant u$ we have

$$\sum_{i=1}^{u} 2^{2ijt}(a_i^{(u+1)} - a_i^{(u)}) = 2^{(m+j)t-mu}(1 - 2^{-m}). \tag{12}$$

By solving simultaneous equations above and using the formula for van der Monde determinant, we have

$$\begin{aligned} a_i^{(u+1)} - a_i^{(u)} &= 2^{-mu-(2i-1)j}(2^m - 1) \prod_{t=1}^{i-1} \frac{(2^{m+j} - 2^{2tj})}{(2^{2ij} - 2^{2tj})} \prod_{t=i+1}^{u} \frac{(2^{m+j} - 2^{2tj})}{(2^{2ij} - 2^{2tj})} \\ &= (-1)^{u-i}\, 2^{-mu-(2i-1)j+(u-i+1)(u-i)j}(2^m - 1) \\ &\quad \times \prod_{t=1}^{i-1} \frac{1 - 2^{m+j-2jt}}{1 - 2^{2jt}} \prod_{t=1}^{u-1} \frac{1 - 2^{m-(2i+2t-1)j}}{1 - 2^{2jt}}. \end{aligned}$$

[7] Since $\sum_w A_w^{(u)} = 2^{mu}$, $A_{2^{m-1}}^{(u)}$ is found from other $A_w^{(u)}$'s.

For the convenience of notation, let

$$\begin{bmatrix} l \\ h \end{bmatrix}_j = \prod_{t=1}^{h} \frac{1 - 2^{2j(l+1-t)}}{1 - 2^{2jt}}, \qquad \text{for} \quad h > 0,$$
$$= 1, \qquad \text{for} \quad h = 0,$$

where $2l$ and h are nonnegative integers. Then, for $0 \leqslant h < u_1(m, j) - i$,

$$a_i^{(i+h+1)} - a_i^{(i+h)}.$$
$$= (-1)^h \, 2^{-mi-(2i-1)j-(m-(h+1)j)h} (2^m - 1) \begin{bmatrix} (m-j)/(2j) \\ i-1 \end{bmatrix}_j \begin{bmatrix} (m-j)/(2j) - i \\ h \end{bmatrix}_j . \tag{13}$$

Since $a_i^{(i)} = 0$, we have

$$2^{m(i+1)} a_i^{(i+1)} = 2^{m-(2i-1)j} (2^m - 1) \begin{bmatrix} (m-j)/(2j) \\ i-1 \end{bmatrix}_j . \tag{14}$$

For $j = 1$, this formula was derived by Berlekamp (1970) in a different way. By (13), we have that for $1 \leqslant i \leqslant u_1(m, j)$ and $0 \leqslant h < u_1(m, j) - i$,

$$a_i^{(i+h+1)} = 2^{-mi-(2i-1)j} (2^m - 1) \begin{bmatrix} (m-j)/(2j) \\ i-1 \end{bmatrix}_j$$
$$\times \left(1 + \sum_{t=1}^{h} (-2)^{-mt} 2^{t(t+1)j} \begin{bmatrix} (m-j)/(2j) - i \\ t \end{bmatrix}_j \right). \tag{15}$$

A compact form of the last factor of (15) is unknown except for $u = u_1(m, j)$ (refer to Theorem A1).

3.2 *Weight Enumerators for Nonprimitive Cases*

Let j be a factor of m such that $m/j \equiv 2 \bmod 4$. $E_w^{(u)}$, $F_w^{(u)}$, $I_w^{(u)}$, and $J_w^{(u)}$ will denote the number of code-words of weight w in $\bar{\mathscr{E}}_j^{(u)}$, $\mathscr{F}_j^{(u)}$, $\bar{\mathscr{I}}_{2j}^{(u)}$, and $\mathscr{I}_{2j}^{(u)}$, respectively. Referring to Corollary 3, let

$$a_i^{(u)} = 2^{-k} E^{(u)}_{2^{m-1}-(-1)^i 2^{m/2+ij-1}}$$

for $1 \leqslant u \leqslant \lceil m/(4j) \rceil$ and $0 \leqslant i \leqslant 2u - 1$, where $k = mu$ for $1 \leqslant u < \lceil m/(4j) \rceil$ and $k = m(u - 1/2)$ for $u = \lceil m/(4j) \rceil$, and let

$$b_i^{(u)} = 2^{-m(u-1/2)} I^{(u)}_{2^{m-1}-(-1)^i 2^{m/2+ij-1}}$$

for $1 \leqslant u \leqslant \lceil m/(4j) \rceil$ and $0 \leqslant i \leqslant 2u - 2$. From Corollary 1, parts (4) and (5), it follows that

$$F_w^{(u)} = J_w^{(u)} \qquad \text{for} \quad 0 \leqslant w \leqslant 2u - 1.$$

Use the Pless translated power moment identities with center 2^{m-1}. Then, for $1 \leqslant u < m/(4j)$,

$$\sum_{i=0}^{2u} (-2)^{ijt}(b_i^{(u+1)} - a_i^{(u)}) = 2^{mt/2-m(u+1/2)}(2^{m/2} - 1) \quad \text{for} \quad 0 \leqslant t \leqslant 2u, \tag{16}$$

$$\sum_{i=0}^{2u} (-2)^{ijt}(b_i^{(u+1)} - b_i^{(u)}) = 2^{mt/2-m(u+1/2)}(2^{m} - 1) \quad \text{for} \quad 0 \leqslant t \leqslant 2u-1, \tag{17}$$

where $a_{2u}^{(u)} = b_{2u}^{(u)} = b_{2u-1}^{(u)} = 0$. By solving (16), $b_i^{(u+1)} - a_j^{(u)}$ can be found. Since $a_{2u}^{(u)} = 0$, $b_{2u}^{(u+1)}$ can be found. Substitute this value for $b_{2u}^{(u+1)}$ in (17), and solve (17). By a similar way to the one used in Section 3.1, each $b_i^{(u)}$ can be found. Then, $a_i^{(u)}$ with $1 \leqslant u < m/(4j)$ can be determined. For $u = [m/(4j)]$, $a_i^{(u)} = b_i^{(u)}$ by definition. Thus, formulas for $a_i^{(u)}$ and $b_i^{(u)}$ can be derived.

3.3 *Weight Enumerators for $\mathscr{A}_j^{(u)}$ and $\mathscr{G}_j^{(u)}$ with Even m/j*

Let j be a factor of m such that m/j is even. $A_w^{(u)}$ and $G_w^{(u)}$ will denote the number of code-words of weight w in $\bar{\mathscr{A}}_j^{(u)}$ and $\bar{\mathscr{G}}_j^{(u)}$, respectively. Refer to Corollary 2, parts (2) and (5). For $1 \leqslant u \leqslant m/(2j)$ and $0 \leqslant i \leqslant u$, let

$$a_i^{(u)} = 2^{-mu}(A_{2^{m-1}-2^{m/2+ij-1}}^{(u)} + A_{2^{m-1}+2^{m/2+ij-1}}^{(u)}),$$

$$b_i^{(u)} = 2^{-m(u+1/2)}(G_{2^{m-1}-2^{m/2+ij-1}}^{(u)} + G_{2^{m-1}+2^{m/2+ij-1}}^{(u)}).$$

By definition, $a_i^{(1+m/(2j))} = b_i^{(m/(2j))}$. Let $a_i = a_i^{(1+m/(2j))}$. Then, the following equations are derived by a similar way to the one used for (12):

$$\sum_{i=0}^{u-2} 2^{2ijt}(a_i^{(u)} - a_i^{(u-1)}) = 2^{mt-mu}(2^m - 1) - 2^{2(u-1)jt}a_{u-1}^{(u)}$$
$$\text{for} \quad 2 \leqslant u \leqslant m/(2j) \quad \text{and} \quad 1 \leqslant t < u, \tag{18}$$

$$\sum_{i=0}^{u-1} 2^{2ijt}(b_i^{(u)} - a_i^{(u)}) = 2^{mt-m(u+1/2)}(2^{m/2} - 1)$$
$$\text{for} \quad 1 \leqslant u \leqslant m/(2j) \quad \text{and} \quad 1 \leqslant t \leqslant u, \tag{19}$$

$$\sum_{i=0}^{u-1} 2^{2ijt}(a_i^{(u)} - a_i) = -2^{mt-mu} + \sum_{i=u}^{m/(2j)} 2^{2ijt}a_i$$
$$\text{for} \quad 1 \leqslant u \leqslant m/(2j) \quad \text{and} \quad 1 \leqslant t \leqslant u. \tag{20}$$

We first derive a formula for $a_{u-1}^{(u)}$ from (20) and Theorem A1. Then, a formula for $a_i^{(u)}$ will be derived by using the formula for $a_{u-1}^{(u)}$ and (18). By solving Eq. (20), we have

$$a_i^{(u)} - a_i = (-1)^{u-i}\, 2^{-2ij+m(1-u)+(u-i)(u-i-1)j} \begin{bmatrix} m/(2j) \\ i \end{bmatrix}_j \begin{bmatrix} m/(2j)-1-i \\ u-1-i \end{bmatrix}_j$$

$$+ (-1)^{u-1-i}\, 2^{-2ij+(u-i)(u-i-1)j} \sum_{t=u}^{m/(2j)} 2^{2jt} \begin{bmatrix} t \\ i \end{bmatrix}_j \begin{bmatrix} t-1-i \\ u-1-i \end{bmatrix}_j a_t . \tag{21}$$

For $i = u - 1$,

$$a_i^{(i+1)} = -2^{-(m+2j)i} \begin{bmatrix} m/(2j) \\ i \end{bmatrix}_j + 2^{-2ij} \sum_{t=i+1}^{m/(2j)} 2^{2jt} \begin{bmatrix} t \\ i \end{bmatrix}_j a_t$$

$$= -2^{-(m+2j)i} \begin{bmatrix} m/(2j) \\ i \end{bmatrix}_j + 2^{m-2ij} \sum_{t=0}^{m/(2j)-i-1} 2^{-2jt} \begin{bmatrix} m/(2j)-t \\ i \end{bmatrix}_j a_{m/(2j)-t} .$$

From Theorem A1 in Appendix I,

$$2^{m(m+j)/(2j)} a_{m/(2j)-t} = 2^{t(t+1)j}(-1)^t \begin{bmatrix} m/(2j) \\ t \end{bmatrix}_j \begin{bmatrix} (m-j)/(2j) \\ t \end{bmatrix}_j [t]_j , \tag{22}$$

where $[t]_j = \prod_{i=1}^{t} (1 - 2^{2ij})$ if $t > 0$ and $[0]_j = 1$. Hence,

$$2^{m-2ij} \sum_{t=0}^{m/(2j)-i-1} 2^{-2jt} \begin{bmatrix} m/(2j)-t \\ i \end{bmatrix}_j a_{m/(2j)-t}$$

$$= 2^{m-2ij-m(m+j)/(2j)} \sum_{t=0}^{m/(2j)-i-1} (-1)^t\, 2^{t(t-1)j}$$

$$\times \begin{bmatrix} m/(2j)-t \\ i \end{bmatrix}_j \begin{bmatrix} m/(2j) \\ t \end{bmatrix}_j \begin{bmatrix} (m-j)/(2j) \\ t \end{bmatrix}_j [t]_j .$$

By an identity due to Berlekamp (1970), this equals to

$$2^{-(m+j)i} \begin{bmatrix} m/(2j) \\ i \end{bmatrix}_j .$$

Thus, we have

$$a_i^{(i+1)} = 2^{-(m+2j)i}(2^{ij} - 1) \begin{bmatrix} m/(2j) \\ i \end{bmatrix}_j . \tag{23}$$

For $j = 1$, this formula was derived by Berlekamp (1970). By solving (18),

$$\begin{aligned} & a_i^{(i+h+1)} - a_i^{(i+h)} \\ &\quad = (-1)^h\, 2^{-(m+2j)i-(m-(h+1)j)h} \left(-(2^m - 1) \begin{bmatrix} m/(2j) \\ i \end{bmatrix}_j \right. \\ &\qquad \left. \cdot \begin{bmatrix} m/(2j) - i - 1 \\ h - 1 \end{bmatrix}_j + (2^{(i+h)j} - 1) \begin{bmatrix} i + h \\ i \end{bmatrix}_j \begin{bmatrix} m/(2j) \\ i + h \end{bmatrix}_j \right) \\ &\quad = (-1)^{h_2\ -(m+2j)i-(m-(h+1)j)h} \begin{bmatrix} m/(2j) \\ i \end{bmatrix}_j \begin{bmatrix} m/(2j) - i - 1 \\ h - 1 \end{bmatrix}_j \\ &\qquad \cdot \left(\frac{(2^{m-2ij} - 1)(2^{(i+h)j} - 1)}{2^{2hj} - 1} - (2^m - 1) \right). \end{aligned}$$

Hence, for $1 \leqslant h \leqslant m/(2j) - i$ and $0 \leqslant i < m/(2j)$,

$$\begin{aligned} a_i^{(i+h)} = 2^{-(m+2j)i} \begin{bmatrix} m/(2j) \\ i \end{bmatrix}_j & \left(2^{ij} - 1 + \sum_{t=1}^{h-1} (-1)^t\, 2^{-(m-(t+1)j)t} \right. \\ & \left. \times \begin{bmatrix} m/(2j) - i - 1 \\ t - 1 \end{bmatrix}_j \left(\frac{(2^{m-2ij} - 1)(2^{(i+t)j} - 1)}{(2^{2jt} - 1)} - 2^m + 1 \right) \right). \end{aligned} \tag{24}$$

By (19), we have

$$\begin{aligned} b_i^{(i+h)} - a_i^{(i+h)} &= (-1)^{h+1} 2^{-(m+2j)i+m/2-(m-(h+1)j)h} (2^{m/2} - 1) \begin{bmatrix} m/(2j) \\ i \end{bmatrix}_j \\ &\quad \cdot \begin{bmatrix} m/(2j) - i - 1 \\ h - 1 \end{bmatrix}_j, \\ &\quad \text{for} \quad 1 \leqslant h \leqslant m/(2j) - i \quad \text{and} \quad 0 \leqslant i < m/(2j). \end{aligned} \tag{25}$$

A formula for $b_i^{(i+h)}$ follows from (24) and (25).

3.4 *Weight Enumerators for $\mathscr{I}_j^{(u)}$ with Even m/j*

Suppose that m/j is even. By Corollary 2, part (5), the weight of a codeword in $\mathscr{G}_i^{(u)} \cup \mathscr{I}_i^{(u)}$ is of the form,

$$2^{m-1} + \epsilon 2^{m/2+ij-1},$$

where ϵ is either 0, 1 or -1 and $0 \leqslant i \leqslant u - 1$. Let G_w (or I_w) denote the number of code-words of $\mathscr{G}_j^{(u)}$ (or $\mathscr{I}_j^{(u)}$) of weight w, and for $0 \leqslant i \leqslant u-1$ let

$$a_i = 2^{-mu-m/2}(G_{2^{m-1}+2^{m/2+ij-1}} + G_{2^{m-1}-2^{m/2+ij-1}}),$$
$$a_i' = 2^{-mu-m/2}(G_{2^{m-1}+2^{m/2+ij-1}} - G_{2^{m-1}-2^{m/2+ij-1}}),$$
$$b_i = 2^{-mu+m/2}(I_{2^{m-1}+2^{m/2+ij-1}} + I_{2^{m-1}-2^{m/2+ij-1}}),$$
$$b_i' = 2^{-mu+m/2}(I_{2^{m-1}+2^{m/2+ij-1}} - I_{2^{m-1}-2^{m/2+ij-1}}).$$

By Corollary 1, part (3), the dual codes of $\mathscr{G}_j^{(u)}$ and $\mathscr{I}_j^{(u)}$ have the same number of codewords of weight w for $0 \leqslant w \leqslant 2u-1$. Hence, by subtracting the Pless translated power moment identities with center 2^{m-1} for $\mathscr{I}_j^{(u)}$ from those for $\mathscr{G}_j^{(u)}$, we have that

$$2^{2mt-mu}(2^{-m/2} - 2^{m/2}) + \sum_{i=0}^{u-1} 2^{(m+2ij)t}(a_i - b_i) = 0,$$
$$\text{for} \quad 1 \leqslant t \leqslant u-1,$$
$$-2^{2mt+m-mu}(2^{-m/2} - 2^{m/2}) + \sum_{i=0}^{u-1} 2^{(m/2+ij)(2t+1)}(a_i' - b_i') = 0,$$
$$\text{for} \quad 0 \leqslant t \leqslant u-1.$$

By Corollary 4, we have

$$a_0 = b_0\,.$$

Since the coefficient matrices are nonsingular, $a_i - b_i$ and $a_i' - b_i'$ are determined uniquely by the linear equations above. Since a_i is found in Section 3.3 and a_i' is derived from a_i by using the Prange Symmetry relation, b_i and b_i' can be found.

APPENDIX I: WEIGHT ENUMERATORS FOR $\mathscr{A}_j^{(u_1(m,j))}$

$\mathscr{A}_1^{(u_1(m,1))}$ is the even part of the 2nd-order cyclic Reed–Muller codes, and for even m, $\mathscr{A}_2^{(u_1(m,2))}$ is the (0, 2)th-order Euclidean Geometry codes. Theorem A1 is an extension of the results by Berlekamp and Sloane (1970).

Let j be a factor of m and $j \neq m$. Let $m/j = \bar{m}$. By definition, α^h is a root of the generator polynomial of $\mathscr{B}_j^{(u_1(m,j))}$ if and only if

$$\min_{0 \leqslant l < j} W_{2^j}(j2^l) < 3.$$

This implies that $\mathscr{B}_j^{(u_1(m,j))}$ is a polynomial code, that is, the binary subfield subcode of $(\bar{m}(2^j - 1) - 3)$rd-order generalized Reed–Muller code of length $2^m - 1$ over $GF(2^j)$ (Kasami–Lin–Peterson (1968b)). Therefore, the extended code of $\bar{\mathscr{A}}_j^{(u_1(m,j))}$, denoted by $\mathscr{A}_j$, can be characterized as follows. Let $P_{\bar{m}}$ be the set of polynomials of variables $X_1, \ldots, X_{\bar{m}}$ of degree less than 3 over $GF(2^j)$. For $f(X_1, \ldots, X_{\bar{m}}) \in P_{\bar{m}}$, let $v(f)$ be the binary vector of length 2^m whose first component is $f(0, \ldots, 0)$ and whose i-th component with $1 \leqslant i < 2^m$ is $f(a_{i1}, a_{i2}, \ldots, a_{i\bar{m}})$, where $\beta^{i-1} = \sum_{h=1}^{\bar{m}} a_{ih}\beta^{h-1}$ with $a_{ih} \in GF(2^j)$ and β is a primitive element of $GF((2^j)^{\bar{m}})$. For $f \in P_{\bar{m}}$, $v(f)$ is orthogonal to every code-word of the extended code of $\mathscr{B}_j^{(u_1(m,j))}$, (Kasami–Lin–Peterson (1968b)). Hence $v(\mathrm{Tr}(f))$ is orthogonal to every code-word of the extended code of $\mathscr{B}_j^{(u_1(m,j))}$, where $\mathrm{Tr}(f) = f + f^2 + \cdots + f^{2^j-1}$. That is

$$\mathscr{A}_j \supseteq \{v(\mathrm{Tr}(f)) \mid f \in P_{\bar{m}}\}.$$

Let $\bar{P}_{\bar{m}}$ be the set of those polynomials in $P_{\bar{m}}$ which are of the form

$$c_0 + \sum_i c_i X_i + \sum_{i<h} c_{ih} X_i X_h ,$$

where $c_0 \in GF(2)$, $c_i \in GF(2^j)$ and $c_{ih} \in GF(2^j)$. Since $\mathrm{Tr}(cX^2) = \mathrm{Tr}(c'X)$ with $c = c'^2$ and $\mathrm{Tr}(c) \in GF(2)$ for $c \in GF(2^j)$,

$$\{v(\mathrm{Tr}(f)) \mid f \in P_{\bar{m}}\} = \{v(\mathrm{Tr}(f)) \mid f \in \bar{P}_{\bar{m}}\}.$$

If $f_1 \in \bar{P}_{\bar{m}}$, $f_2 \in \bar{P}_{\bar{m}}$ and $f_1 \neq f_2$, then $\mathrm{Tr}(f_1) \neq \mathrm{Tr}(f_2)$ and, therefore, $v(\mathrm{Tr}(f_1)) \neq v(\mathrm{Tr}(f_2))$. Since the dimension of $\{v(\mathrm{Tr}(f)) \mid f \in \bar{P}_{\bar{m}}\}$ is $1 + \bar{m}(\bar{m} + 1)j/2$, $\mathscr{A}_j = \{v(\mathrm{Tr}(f)) \mid f \in \bar{P}_{\bar{m}}\}$. Let $Y_i = b_{i0} + \sum_{h=1}^{\bar{m}} b_{ih}X_h$ with $1 \leqslant i \leqslant m/j$ and $b_{ih} \in GF(2^j)$ be an invertible affine transformation. For $f \in P_{\bar{m}}$, $g = f(b_{10} + \sum_{h=1}^{\bar{m}} b_{1h}X_h, b_{20} + \sum_{h=1}^{\bar{m}} b_{2h}X_h, \ldots) \in P_{\bar{m}}$ and $v(\mathrm{Tr}(g))$ has the same weight as $v(\mathrm{Tr}(f))$. It follows from Corollary 16.351 (Berlekamp (1968)) that any polynomial in $P_{\bar{m}}$ can be reduced by an invertible affine transformation of its variables and by substituting X_i and $\mathrm{Tr}(c_0)$ for X_i^2 and constant term c_0, respectively, to one of the canonical forms:

$$X_1X_2 + X_3X_4 + \cdots + X_{2i-1}X_{2i}, \qquad 0 \leqslant i \leqslant \bar{m}/2, \qquad \text{(A1)}$$

$$X_1X_2 + X_3X_4 + \cdots + X_{2i-1}X_{2i} + X_{2i+1}, \qquad 0 \leqslant i < \bar{m}/2, \qquad \text{(A2)}$$

$$X_1X_2 + X_3X_4 + \cdots + X_{2i-1}X_{2i} + 1, \qquad 0 \leqslant i \leqslant \bar{m}/2. \qquad \text{(A3)}$$

Let $P_{\bar{m},i}^{(1)}$, $P_{\bar{m},i}^{(2)}$, and $P_{\bar{m},i}^{(3)}$ denote the sets of those polynomials in $\bar{P}_{\bar{m}}$ which can be reduced to the forms (A1), (A2), and (A3), respectively, by an invertible affine transformation of its variables and by substituting X_i for X_i^2 and $\mathrm{Tr}(c_0)$ for a constant term c_0. Then, the following lemma holds:

LEMMA A1. *The weight of*

$$\begin{aligned} v(\mathrm{Tr}(f)) &= 2^{\bar{m}j-1} - 2^{\bar{m}j-ij-1} && \text{for } f \in P^{(1)}_{\bar{m},i} \\ &= 2^{\bar{m}j-1} && \text{for } f \in P^{(2)}_{\bar{m},i} \\ &= 2^{\bar{m}j-1} + 2^{\bar{m}j-ij-1} && \text{for } f \in P^{(3)}_{\bar{m},i}. \end{aligned}$$

Proof. By induction on i, this lemma will be proved. The number of (X_1, X_2) such that $\mathrm{Tr}(X_1X_2) = 1$ (or 0) with $X_1 \in GF(2^j)$ and $X_2 \in GF(2^j)$ is $2^{j-1}(2^j - 1)$ (or $2^{2j-1} + 2^{j-1}$). By the induction hypothesis, the number of $(X_3, X_4, ..., X_{\bar{m}})$ such that $\mathrm{Tr}(X_3X_4 + X_5X_6 + \cdots + X_{2i-1}X_{2i}) = 1$ (or 0) is $2^{\bar{m}j-2j-1} - 2^{\bar{m}j-j-ij-1}$ (or $2^{\bar{m}j-2j-1} + 2^{\bar{m}j-j-ij-1}$). Since

$$\begin{aligned} &\mathrm{Tr}(X_1X_2 + X_3X_4 + \cdots + X_{2i-1}X_{2i}) \\ &\quad = \mathrm{Tr}(X_1X_2) + \mathrm{Tr}(X_3X_4 + \cdots + X_{2i-1}X_{2i}), \end{aligned}$$

the number of $(X_1, ..., X_{\bar{m}})$ such that $\mathrm{Tr}(X_1X_2 + \cdots + X_{2i-1}X_{2i}) = 1$ is

$$\begin{aligned} &(2^{2j-1} - 2^{j-1})(2^{\bar{m}j-2j-1} + 2^{\bar{m}j-j-ij-1}) + (2^{2j-1} + 2^{j-1})(2^{\bar{m}j-2j-1} - 2^{\bar{m}j-j-ij-1}) \\ &\quad = 2^{\bar{m}j-1} - 2^{\bar{m}j-ij-1}. \end{aligned}$$

The other cases can be proved similarly.

Now let

$$f = X_1X_2 + \cdots + X_{2i-1}X_{2i} + c_0 + c_1X_1 + \cdots + c_{\bar{m}}X_{\bar{m}},$$

where $c_0 \in GF(2)$ and $c_h \in GF(2^j)$. Then, $f \in P^{(1)}_{\bar{m},i}$ (or $P^{(3)}_{\bar{m},i}$) if and only if $c_h = 0$ for $2i < h \leqslant \bar{m}$ and $\mathrm{Tr}(c_0 + c_1c_2 + \cdots + c_{2i-1}c_{2i}) = 0$ (or 1),[8] and $f \in P^{(2)}_{\bar{m},i}$, if and only if $c_h \neq 0$ for some h with $2i < h \leqslant \bar{m}$. In case that $f_1 - f_2$ is a polynomial of degree less that 2, then let $f_1 \sim f_2$. Relation "$\sim$" is a congruence relation. For each $f_1 \in P^{(1)}_{\bar{m},i}$, there are $2^{2ij} f_2$'s in $P^{(1)}_{\bar{m},i}$ such that $f_1 \sim f_2$. By relation "$\sim$", $P^{(1)}_{\bar{m},i}$ is partitioned into $|P^{(1)}_{\bar{m},i}| 2^{-2ij}$ blocks, where $|S|$ denotes the number of elements in set S. Let $|P^{(1)}_{\bar{m},i}| = 0$ for $i > 2\bar{m}$. For each $f \in P^{(2)}_{\bar{m},i}$, there is exactly one block whose members have relation "$\sim$" with f. For a representative f of each block, there are $2^{2ij+1}(2^{mj-2ij} - 1)$ polynomials in $P^{(2)}_{\bar{m},i}$ which have relation "$\sim$" with f. Consequently, we have that

$$|P^{(2)}_{\bar{m},i}| = 2(2^{\bar{m}j-2ij} - 1)\,|P^{(1)}_{\bar{m},i}|. \tag{A4}$$

Obviously,

$$|P^{(1)}_{\bar{m},i}| = |P^{(3)}_{\bar{m},i}|. \tag{A5}$$

[8] Use $X_1X_2 + c_1X_1 + c_2X_2 = (X_1 + c_2)(X_2 + c_1) + c_1c_2$.

Let $f \in P^{(1)}_{\bar{m}+1,i}$, and let

$$f = f_0 + X_{\bar{m}+1} f_1 ,$$

where $f_0 \in \bar{P}_{\bar{m}}$ and $f_1 \in \bar{P}_{\bar{m}}$ are independent of $X_{\bar{m}+1}$. If $f = f_0 + X_{\bar{m}+1} f_1$, $f' = f_0' + X_{\bar{m}+1} f_2'$ and $f_0 \neq f_0'$, then $f \neq f'$. We proceed to count the number of polynomials in $P^{(1)}_{\bar{m}+1,i}$. Without loss of generality, let

$$\begin{aligned} f &= f_0 + f_1 X_{\bar{m}+1} \\ &= c_0 + X_1X_2 + X_3X_4 + \cdots + X_{2h-1}X_{2h} + c_1 X_{2h+1} \\ &\quad + (b_0 + b_1X_1 + b_2X_2 + \cdots + b_{\bar{m}}X_{\bar{m}})X_{\bar{m}+1} , \end{aligned}$$

where $c_0 \in GF(2)$, $c_1 \in GF(2)$, $c_0c_1 = 0$, $b_l \in GF(2^j)$, $0 \leqslant h \leqslant \bar{m}/2$, and if $c_1 = 1$, then $2h + 1 \leqslant \bar{m}$. For a fixed $f_0 \in \bar{P}_m$ different choices of b_0, b_1,..., $b_{\bar{m}}$ give different f's in $\bar{P}_{\bar{m}+1}$.

(1) Suppose that $c_1 = 0$. If $b_l \neq 0$ for some l with $2h < l \leqslant \bar{m}$, then $f \in P^{(1)}_{\bar{m}+1,i} \cup P^{(3)}_{\bar{m}+1,i}$ if and only if $h = i - 1$. The number of these cases is

$$2^{(2i-1)j+1}(2^{\bar{m}j-2(i-1)j} - 1) \mid P^{(1)}_{\bar{m},i-1} \mid . \tag{A6}$$

If $b_l = 0$ for every l with $2h < l \leqslant \bar{m}$, then

$$\begin{aligned} &= (X_1 + b_2X_{\bar{m}+1})(X_2 + b_1X_{\bar{m}+1}) \\ &\quad + \cdots + (X_{2h-1} + b_{2h}X_{\bar{m}+1})(X_{2h} + b_{2h-1}X_{\bar{m}+1}) \\ &\quad + (b_1b_2 + \cdots + b_{2h-1}b_{2h})\, X^2_{\bar{m}+1} + b_0X_{\bar{m}+1} + c_0 . \end{aligned}$$

Replace $X^2_{\bar{m}+1}$ by $X_{\bar{m}+1}$. Then, $f \in P^{(1)}_{\bar{m}+1,i} \cup P^{(3)}_{\bar{m}+1,i}$ if and only if $h = i$ and $b_0 + b_1b_2 + \cdots + b_{2i-1}b_{2i} = 0$. The number of these cases is

$$2^{2ij+1} \mid P^{(1)}_{\bar{m},i} \mid . \tag{A7}$$

(2) Suppose that $c_1 = 1$. If $b_l \neq 0$ for some l with $2h + 1 < l \leqslant \bar{m}$, then $f \in P^{(2)}_{\bar{m}+1,h+1}$ and $f \notin P^{(1)}_{\bar{m}+1,i} \cup P^{(3)}_{\bar{m}+1,i}$. If $b_l = 0$ for every l with $2h < l \leqslant \bar{m}$, then $f \in P^{(2)}_{\bar{m}+1,h}$ and $f \notin P^{(1)}_{\bar{m}+1,i} \cup P^{(3)}_{\bar{m}+1,i}$. If $b_l = 0$ for $2h + 1 < l \leqslant \bar{m}$ and $b_{2h+1} \neq 0$, then

$$\begin{aligned} f = {} & (X_1 + b_2X_{\bar{m}+1})(X_2 + b_1X_{\bar{m}+1}) \\ & + \cdots + (X_{2h-1} + b_{2h}X_{\bar{m}+1})(X_{2h} + b_{2h-1}X_{\bar{m}+1}) \\ & + (b_1b_2 + \cdots + b_{2h-1}b_{2h})\, X^2_{\bar{m}+1} + X_{2h+1} + (b_0 + b_{2h+1}X_{2h+1})\, X_{\bar{m}+1} . \end{aligned}$$

Replace $X^2_{\bar{m}+1}$ by $X_{\bar{m}+1}$ and use

$$\begin{aligned} b_{2h+1}X_{2h+1}X_{\bar{m}+1} &+ X_{2h+1} + (b_0 + b_1b_2 + \cdots + b_{2h-1}b_{2h})\, X_{\bar{m}+1} \\ &= (b_{2h+1}X_{2h+1} + b_0 + b_1b_2 + \cdots + b_{2h-1}b_{2h})(X_{\bar{m}+1} + b^{-1}_{2h+1}) \\ &\quad + b^{-1}_{2h+1}(b_0 + b_1b_2 + \cdots + b_{2h-1}b_{2h}). \end{aligned}$$

Then, $f \in P^{(1)}_{\bar{m}+1,i} \cup P^{(3)}_{\bar{m}+1,i}$ if and only if $h = i - 1$. The number of these cases is

$$\begin{aligned} 2^{(2i-1)j}(2^j - 1) &\mid P^{(2)}_{\bar{m},i-1} \mid \\ &= 2^{(2i-1)j+1}(2^j - 1)(2^{\bar{m}j-2(i-1)j} - 1) \mid P^{(1)}_{\bar{m},i-1} \mid. \end{aligned} \tag{A8}$$

By (A5)–(A8),

$$\mid P^{(1)}_{\bar{m}+1,i} \mid = 2^{2ij} \mid P^{(1)}_{\bar{m},i} \mid + 2^{2ij}(2^{\bar{m}j-2(i-1)j} - 1) \mid P^{(1)}_{\bar{m},i-1} \mid. \tag{A9}$$

Now, we have the following theorem:

THEOREM A1. (1) $\mid P^{(1)}_{\bar{m},0} \mid = 1$; (2) *For* $0 < i \leqslant \bar{m}/2$,

$$\mid P^{(1)}_{\bar{m},i} \mid = 2^{i(i+1)j} \prod_{t=0}^{2i-1} (2^{(\bar{m}-t)j} - 1) \Big/ \prod_{t=1}^{i} (2^{2jt} - 1).$$

Proof. Obviously, $\mid P^{(1)}_{\bar{m},0} \mid = 1$. By (A9),

$$\mid P^{(1)}_{2,1} \mid = 2^{2j}(2^j - 1).$$

Thus, Lemma A2 holds for $\bar{m} = 2$. Assume that the lemma holds for $\bar{m} \leqslant l$. Consider the case of $\bar{m} = l + 1$. If $2i \leqslant l$, then it follows from (A9) that

$$\begin{aligned} \mid P^{(1)}_{l+1,i} \mid &= 2^{i(i+1)j} \left(\prod_{t=1}^{2i-1} (2^{(l+1-t)j} - 1) \Big/ \prod_{t=1}^{i} (2^{2jt} - 1) \right) \\ &\quad \times \{2^{2ij}(2^{(l-2i+1)j} - 1) + 2^{2ij} - 1\} \\ &= 2^{i(i+1)j} \left(\prod_{t=0}^{2i-1} (2^{(l+1-t)j} - 1) \Big/ \prod_{t=1}^{i} (2^{2jt} - 1) \right). \end{aligned}$$

If $2i = l + 1$, then from (A9), we have

$$| P^{(1)}_{l+1,i} | = 2^{i(i+1)j} \left(\prod_{t=0}^{2i-3} (2^{(l-t)j} - 1) \Big/ \prod_{t=1}^{i-1} (2^{2jt} - 1) \right) (2^{(l-2i+2)j} - 1)$$

$$= 2^{i(i+1)j} \left(\prod_{t=0}^{2i-1} (2^{(l+1-t)j} - 1) \Big/ \prod_{t=1}^{i} (2^{2jt} - 1) \right).$$

Since

$$| P^{(1)}_{\bar{m},i} | = A^{(u_1(m,j))}_{2^{m-1}-2^{m-ij-1}} + A^{(u_1(m,j))}_{2^{m-1}-2^{m-ij-1}-1} = A^{(u_1(m,j))}_{2^{m-1}-2^{m-ij-1}} + A^{(u_1(m,j))}_{2^{m-1}+2^{m-ij-1}},$$

formula (22) follows from Theorem A1.

APPENDIX II: Proof of Theorem 2

We follow the proof by Berlekamp–Sloane (1969) and use the same notations as those in Berlekamp–Sloane (1969) except for $P^{(n)}$. In this proof, $P^{(n)}$ will denote a power series of the form

$$P^{(n)} = \sum_{k \in K(n,j)} a_k z^k,$$

where j divides $n + 2$. For $P^{(n)}$ in this meaning, Lemma 1 of Berlekamp–Sloane (1969) still holds, which is proved as follows:

If $k_{\pi+1} \leqslant 2^{n+1} - 2^{n-\pi} - 1$ with $0 \leqslant \pi \leqslant n$ is in $K(n, j)$, then $k_{\pi+1}$ is of the form

$$2^{n+2} - 2^h - 2^{h-lj} - 1.$$

Hence, $\pi + 1$ is divisible by j. Suppose that $L \leqslant \sum_{\nu=0}^{\pi+1} 2^\nu \sum_{i=0}^{t_\nu} \Delta_i \leqslant M$. (We use t_ν instead of k_ν in (16) of Berlekamp–Sloane (1969).) In order to prove the new version of Lemma 1, it is sufficient to consider the case in which $\sum_{\nu=0}^{\pi+1} 2^\nu \sum_{i=0}^{t_\nu} \Delta_i$ is $2\pi + 4$. For this case, since $2^{n+2} - \sum_{i=0}^{t_\nu} \Delta_i - 1 \in K(n, j)$ and the weight of $2^\nu \sum_{i=0}^{t_\nu} \Delta_i$ is 2, $2^\nu \sum_{i=0}^{t_\nu} \Delta_i$ is of the form

$$2^{\rho_\nu} + 2^{\tau_\nu},$$

where $0 \leqslant \tau_\nu < \rho_\nu \leqslant n + 2 + \pi$ and $\rho_\nu - \tau_\nu$ is divisible by j. Since the weight of $\sum_{\nu=0}^{\pi+1} 2^\nu \sum_{i=0}^{t_\nu} \Delta_i$ is $2\pi + 4$, ρ_ν and τ_ν with $0 \leqslant \nu \leqslant \pi + 1$ are all different. On the other hand, $\sum_{\nu=0}^{\pi+1} 2^\nu \sum_{i=0}^{t_\nu} \Delta_i$ is of the form

$$2^\rho + 2^\tau + \sum_{i=n+1-\pi}^{n+2+\pi} 2^i,$$

when $0 \leqslant \tau < \rho \leqslant n - \pi$. Then, the set of $2\pi + 4$ distinct numbers $\{\rho_0, ..., \rho_{\pi+1}, \tau_0, ..., \tau_{\pi+1}\}$ is identical with $\{\tau, \rho, n + 1 - \pi, n + 2 - \pi, ..., n + 2 + \pi\}$. Consider polynomial over $GF(2)$,

$$f(X) = \sum_{\nu} (X^{\rho_\nu} + X^{\tau_\nu}) = X^\rho + X^\tau + \sum_{i=n+1-\pi}^{n+1} X^i(X^{\pi+1} + 1).$$

Since $X^{\rho_\nu} + X^{\tau_\nu} = X^{\tau_\nu}(X^{\rho_\nu - \tau_\nu} + 1) \equiv 0 \bmod(X^j + 1, 2)$ and $X^{\pi+1} + 1 \equiv 0 \bmod(X^j + 1, 2)$,

$$X^\rho + X^\tau = X^\tau(X^{\rho-\tau} + 1) \equiv 0 \bmod(X^j + 1, 2).$$

Hence, $\rho - \tau$ is divisible by j. Since $(n - \pi - 1) + 2$ is divisible by j, the modified version of Lemma 1 holds. Now, the proof of this theorem proceeds in the same way as the one by Berlekamp and Sloane, which holds still for $w \leqslant 2^{\mu\tau1} - 4$. By induction, $n_i + 2$ and $\pi_i + 1$ are divisible by j and $\theta_i - 1 \in K(n_1, j)$. It is concluded that

$$w = 2^{m-r+1} - 2^{n_l - \pi_{l+1}} = 2^{m-r+1} - 2^{n_l + 2 - (\pi_{l+1}+1) - 1}.$$

Acknowledgment

The author would like to thank Dr. E. R. Berlekamp and Dr. R. J. McEliece for suggesting a possibility of applications of the McEliece Theorem, and Dr. S. Lin for his helpful discussions.

RECEIVED: July 27, 1970

References

BERLEKAMP, E. R. (1968), "Algebraic Coding Theory," McGraw-Hill, New York.

BERLEKAMP, E. R. (1970), The weight enumerators for certain subcodes of the 2nd order binary Reed–Muller code, *Inform. Control* (to appear).

BERLEKAMP, E. R. AND SLOANE, N. J. A. (1969), Restrictions on weight distribution of Reed–Muller codes, *Inform. Control* **14**, 442–456.

BERLEKAMP, E. R. AND SLOANE, N. J. A. (1970), The weight enumerator of second-order Reed–Muller codes, *IEEE Trans. Inform. Theory* **IT-16**, 745–751.

KASAMI, T. (1967–1969), "Weight Distributions of Bose–Chaudhuri–Hocquenghem Codes," Combinatorial Mathematics and Its Applications, 335–357, edited by R. C. Bose and T. A. Dowling.

KASAMI, T., LIN, S., AND PETERSON, W. W. (1968a), New generalizations of the Reed–Muller codes. I: Primitive codes, *IEEE Trans. Inform. Theory* **IT-14**, 189–198.

KASAMI, T., LIN, S., AND PETERSON, W. W. (1968b), Polynomial codes, *IEEE Trans. Inform. Theory* **IT-14**, 807–814.

McELIECE, R. J. (1970), private communication.

WELCH, L. R. (1969), "Trace Mappings in Finite Fields and Shıft Register Cross-Correlation Properties," Electrical Engineering Department Report, University of Southern California.

WELDON, E. J., JR. (1967–1969), "Euclidean Geometry Codes," Combinatorial Mathematics and Its applications, 337–387, edited by R. C. Bose and T. A. Dowling.

PETERSON, W. W. and WELDON, E. J., JR. (1971), "Error Correcting Codes," Second ed., John Wiley, New York.

PLESS, V. (1963), Power moment identities on weight distributions in error correcting codes, *Inform. Control.* **6**, 147–152.

Printed in Belgium