GODDARD/GRANT-

IN-64
CR.
67853
19P.

THE BINARY WEIGHT DISTRIBUTION OF THE EXTENDED $(2^m, 2^m-4)$ CODE OF REED-SOLOMON CODE OVER $GF(2^m)$ WITH GENERATOR POLYNOMIAL $(x-\alpha)(x-\alpha^2)(x-\alpha^3)$

Technical Report

to

NASA
Goddard Space Flight Center
Greenbelt, Maryland

Grant Number NAG 5-407

(NASA-CR-180510) THE BINARY WEIGHT DISTRIBUTION OF THE EXTENDED (2 SUP m, 2 SUP m-4) CODE OF REED-SOLOMON CODE OVER GF(2 SUP m) WITH GENERATOR POLYNOMIAL (x-ALPHA SUP 2) (x-ALPHA SUP 3) (Hawaii Univ., Honolulu.) N87-21625
Unclas
G3/64 43347

Shu Lin
Principal Investigator
Department of Electrical Engineering
Honolulu, Hawaii 96822

May 1, 1987

The Binary Weight Distribution of the Extended $(2^m, 2^m-4)$ Code of Reed-Solomon Code over $GF(2^m)$ with Generator Polynomial $(x-\alpha)(x-\alpha^2)(x-\alpha^3)$*

Tadao Kasami
Osaka University

Shu Lin
Texas A&M University

ABSTRACT: Consider an (n,k) linear code with symbols from $GF(2^m)$. If each code symbol is represented by a binary m-tuple using a certain basis for $GF(2^m)$, we obtain a binary (nm,km) linear code, called a binary image of the original code. In this paper, we present a lower bound on the minimum weight of a binary image of a cyclic code over $GF(2^m)$ and the weight enumerator for a binary image of the extended $(2^m,2^m-4)$ code of Reed-Solomon code over $GF(2^m)$ with generator polynomial $(x-\alpha)(x-\alpha^2)(x-\alpha^3)$ and its dual code, where α is a primitive element in $GF(2^m)$.

1. Introduction

Let $\{\beta_1, \beta_2, \cdots, \beta_m\}$ be a basis of the Galois field $GF(2^m)$. Then each element z in $GF(2^m)$ can be expressed as a linear sum of $\beta_1, \beta_2, \cdots, \beta_m$ as follows:

$$z = c_1\beta_1 + c_2\beta_2 + \cdots + c_m\beta_m,$$

where $c_i \in GF(2)$ for $1 \le i \le m$. Thus z can be represented by the m-tuple $(c_1, c_2, \cdots, c_m)$ over GF(2). Let C be an (n,k) linear block code with symbols from the Galois field $GF(2^m)$. If each code symbol of C is represented by the corresponding m-tuple over the binary field GF(2) using the basis $\{\beta_1, \beta_2, \cdots, \beta_m\}$ for $GF(2^m)$, we obtain a binary (mn, mk) linear block code, called a binary image of C. The weight enumerator of a binary image of C is called a binary weight enumerator of C. In general, a binary weight enumerator depends on the choice of basis. A basis $\{\beta_1, \beta_2, \cdots, \beta_m\}$ is called a polynomial basis, if there is an element $\beta \in GF(2^m)$

such that $\beta_j = \beta^{j-1}$ for $1 \le j \le m$. A polynomial basis will be said to be primitive, if β is primitive.

Let α be a primitive element of $GF(2^m)$, and let $n = 2^m-1$. For $1 \le k < n$, let RS_k denote the (n, k) Reed-Solomon code over $GF(2^m)$ with generator polynomial $(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{n-k})$ [1], let $RS_{k,e}$ denote the (n, k) Reed-Solomon code over $GF(2^m)$ with generator polynomial $(x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{n-k-1})$, and let ERS_k be the extended (n+1, k) code of RS_k. The dual code of RS_k is $RS_{n-k,e}$, and the dual code of ERS_k is ERS_{n+1-k}.

Binary weight enumerators for RS_{n-i} with $1 \le i \le 2$, $RS_{n-i,e}$ with $2 \le i \le 3$ and ERS_{n-i} with $1 \le i \le 2$ were presented in [2], and those for $RS_{2,e}$, the dual code of RS_{n-2}, and RS_3, the dual code of $RS_{n-3,e}$, were derived in [3,4]. These binary weight enumerators are independent of the choice of basis.

In section 2, the binary image of the dual code of a linear code C over $GF(2^m)$ by using the complementary basis of a basis $\{\beta_1, \beta_2, \cdots, \beta_m\}$ is shown to be the dual code of the binary image of C by using basis $\{\beta_1, \beta_2, \cdots, \beta_m\}$. In section 3, a lower bound on the minimum weight of a binary image of a cyclic code over $GF(2^m)$. In section 4, the binary weight enumerator of ERS_4 is derived for a class of bases including the complementary bases of primitive polynomial bases. By Theorem 1 the binary weight enumerator for ERS_{n-3} is obtained. This approach can be readily extended to derive the binary weight enumerator for ERS_5.

2. Binary Images of Linear Block Codes over $GR(2^m)$

Let C be an (n,k) linear code with symbols from $GF(2^m)$. Let $C^{(b)}$ denote the binary (nm,km) linear code obtained from C by representing each code symbol by the corresponding m-tuple over GF(2) using the basis $\{\beta_1, \beta_2, \cdots, \beta_m\}$ for $GF(2^m)$. Let $\{\delta_1, \delta_2, \cdots, \delta_m\}$ be the complementary (or dual) basis of $\{\beta_1, \beta_2, \cdots, \beta_m\}$, i.e.,

$$Tr(\beta_i\delta_j) = 0 , \quad \text{for } i \ne j,$$

$$Tr(\beta_i\delta_i) = 1 ,$$

where Tr(x) denotes the trace of the field element x [5,p.117]. Let C^D be the dual code of C. Let $C^{D(b)}$ denote the binary $(nm,(n-k)m)$ linear code obtained from C^D by representing each code symbol by a binary m-tuple over GF(2) using the complementary basis $\{\delta_1, \delta_2, \cdots, \delta_m\}$ of $\{\beta_1, \beta_2, \cdots, \beta_m\}$. Then we have Theorem 1.

<u>Theorem 1</u>: $C^{D(b)}$ is the dual code of $C^{(b)}$.

<u>Proof</u>: Let $(a_1, a_2, \cdots, a_n)$ and $(b_1, b_2, \cdots, b_n)$ be codewords of C and C^D respectively. Then

$$\sum_{i=1}^{n} a_i b_i = 0 . \tag{1}$$

Let

$$a_i = \sum_{j=1}^{m} a_{ij}\beta_j , \tag{2}$$

$$b_i = \sum_{j=1}^{m} b_{ij}\delta_j . \tag{3}$$

It follows from (1) to (3) that

$$\sum_{i=1}^{n} \left(\sum_{j=1}^{m} a_{ij}\beta_j \right)\left(\sum_{h=1}^{m} b_{ih}\delta_h \right) = \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{h=1}^{m} a_{ij}b_{ih}\beta_j\delta_h = 0 . \tag{4}$$

Taking the trace of both sides of (4), we have

$$\sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{h=1}^{m} a_{ij}b_{ih}\mathrm{Tr}(\beta_j\delta_h) = 0 . \tag{5}$$

Since $\mathrm{Tr}(\beta_j\delta_h) = 0$ for $j \neq h$ and $\mathrm{Tr}(\beta_j\delta_j) = 1$, it follows from (5) that

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij}b_{ij} = 0 . \tag{6}$$

Equation (6) implies that $C^{D(b)}$ is the dual code of $C^{(b)}$. $\Delta\Delta$

For a basis $\{\beta_1, \beta_2, \cdots, \beta_m\}$ for $GF(2^m)$ and an n-tuple $\bar{v} = (v_1, v_2, \cdots, v_n)$ over $GF(2^m)$, let $\bar{v}_j$ be defined as

$$\bar{v}_j = (v_{1j}, v_{2j}, \cdots, v_{nj}), \quad \text{for } 1 \leq j \leq m , \tag{7}$$

where $v_i = \sum_{j=1}^{m} v_{ij}\beta_j$ with $v_{ij} \in GF(2)$ for $1 \leq i \leq n$. If $\{\delta_1, \delta_2, \cdots, \delta_m\}$

is the complementary basis of $\{\beta_1, \beta_2, \cdots, \beta_m\}$, then $\bar{v}_j$ is represented as

$$\bar{v}_j = (Tr(\delta_j v_1), Tr(\delta_j v_2), \cdots, Tr(\delta_j v_n)) , \tag{8}$$

and $\bar{v}_j$ is called the δ_j component vector of $\bar{v}$. The binary weight of $\bar{v}$, denoted $|\bar{v}|_2$, is given by

$$|\bar{v}|_2 = \sum_{j=1}^{m} |\bar{v}_j|_2 . \tag{9}$$

3. Binary Images of Cyclic Codes over $GF(2^m)$

Let n be a positive integer which divides 2^m-1. If s is the smallest number in a cyclotomic coset mod n over $GF(2^m)$, s is called the representative of the coset and the coset is denoted by Cy(s). Let m(s) denote the number of integers in Cy(s). For a subset I of $\{0,1,2, \cdots ,n-1\}$, $\bar{I}$ denotes the set union of those cosets which have a nonempty intersection with I, and Rc(I) denotes the set of the representatives of cyclotomic cosets in $\bar{I}$.

Let γ be an element of order n in $GF(2^m)$. For a subset I of $\{0,1,2, \cdots ,n-1\}$, let C(I) be the cyclic code of length n over $GF(2^m)$ with check polynomial

$$\prod_{i \in I} (x - \gamma^i).$$

and let $C_b(I)$ be the binary cyclic code of length n with check polynomial

$$\prod_{i \in \bar{I}} (x - \gamma^i).$$

For a polynomial $f(X) = \sum_{i=0}^{n-1} a_i X^i$ with $a_i \in GF(2^m)$, let v[f(X)] and ev[f(X)] be defined by

$$v[f(X)] = (f(1), f(\gamma), f(\gamma^2), \cdots , f(\gamma^{n-1})) , \tag{10}$$

and

$$ev[f(X)] = (f(0), f(1), f(\gamma), \cdots , f(\gamma^{n-1})) . \tag{11}$$

It follows from (8) and (9) that

$$| v[f(X)] |_2 = \sum_{j=1}^{m} | v[Tr(\delta_j f(X))] |_2 , \tag{12}$$

$$| ev[f(X)] |_2 = \sum_{j=1}^{m} | ev[Tr(\delta_j f(X))] |_2 . \tag{13}$$

For a subset I of $\{0,1,2, \cdots ,n-1\}$, let P(I) be defined by

$$P(I) = \{ \sum_{i\epsilon I} a_i X^i \mid a_i \epsilon GF(2^m) \text{ for } i\epsilon I\} .$$

As is well-known[5],

$$C(I) = \{v[f(X)] | f\epsilon P(I)\} .$$

It follows from (8),(10) and the definitions of C(I) and $C_b(I)$ that for $\bar{v} = v[f(x)] \; \epsilon \; C(I)$, the δ_j component vector of $\bar{v}$, denoted $\bar{v}_j$, is given by

$$\bar{v}_j = v[Tr(\delta_j f(X))] , \qquad 1 \leq j \leq m , \tag{14}$$

and

$$\bar{v}_j \; \epsilon \; C_b(I) . \tag{15}$$

As is also known [5],

$$C_b(I) = \{v[\sum_{i\epsilon Rc(I)} Tr_{m(i)}(a_i X^i)] | a_i \; \epsilon \; GF(2^{m(i)}) \text{ for } i \; \epsilon \; Rc(I) \} , \tag{16}$$

where

$$Tr_j(X) = X + X^2 + \cdots + X^{2^{j-1}} .$$

Polynomial $f(X) \; \epsilon \; P(I)$ can be expressed as

$$f(X) = \sum_{i\epsilon Rc(I)} \sum_{q\epsilon Q(i,I)} a_{i2^q} X^{i2^q} , \tag{17}$$

where $i2^q$ is taken modulo n and

$$Q(i,I) = \{q \mid p{:}i2^q \equiv p \pmod n),\ p \in I \text{ and } 0 \le q < m(i)\} .$$

It follows from (17) that for $1 \le j \le m$

$$Tr(\delta_j f(X)) = \sum_{i\in Rc(I)} Tr_{m(i)}(b_{ji}X^i) , \tag{18}$$

where

$$b_{ji} = Tr^{(m(i))} \left(\sum_{q\in Q(i,I)} \delta_j^{2^{m(i)-q}} a_{i2^q}^{2^{m(i)-q}} \right) , \ i \in Rc(I) , \tag{19}$$

where for a divisor h of m

$$Tr^{(h)}(X) = X + X^{2^h} + X^{2^{2h}} + \cdots + X^{2^{m-h}} . \tag{20}$$

Note that

$$b_{ji} \in GF(2^{m(i)}) . \tag{21}$$

It follows from (14) and (18) that for $1 \le j \le m$

$$\bar{v}_j = v[\sum_{i\in Rc(I)} Tr_{m(i)} (b_{ji} X^i)] . \tag{22}$$

For $i \in Rc(I)$, let $\bar{C}_i$ be defined by

$$\bar{C}_i \overset{\Delta}{=} \{ (b_1,b_2, \cdots ,b_m) \mid b_j = Tr^{(m(i))}(\sum_{q\in Q(i,I)} \delta_j^{2^{m(i)-q}} a'_q) ,$$

$$1 \le j \le m,\ a'_q \in GF(2^m) \} . \tag{23}$$

Note that the following matrix D over $GF(2^m)$ is invertible [5,p.117] :

$$D \overset{\Delta}{=} \begin{bmatrix} \delta_1 & \delta_1^2 & \delta_1^{2^2} & \cdots & \delta_1^{2^{m-1}} \\ \delta_2 & \delta_2^2 & \delta_2^{2^2} & \cdots & \delta_2^{2^{m-1}} \\ & & & & \\ \delta_m & \delta_m^2 & \delta_m^{2^2} & \cdots & \delta_m^{2^{m-1}} \end{bmatrix} . \tag{24}$$

If $Tr^{(m(i))}\left(\sum_{q\epsilon Q(i,I)} \delta_j^{2^{m(i)-q}} a'_q \right) = 0$ for $1 \le j \le m$, then

$$a'_q = 0, \text{ for } q \in Q(i,I) . \tag{25}$$

Hence $\tilde{C}_i$ is a linear (m, $\#Q(i,I)m/m(i)$) code over $GF(2^{m(i)})$, where $\#M$ denotes the number of elements in set M.

For a code C, let mw[C] denote the minimum weight of C. Then the following theorem holds.

Theorem 2 : For $i \in I$,

$$mw[C(I)^{(b)}] \ge \min \{ mw[\tilde{C}_i]mw[C_b(I)], mw[C(I-\overline{\{i\}})^{(b)}] \}, \tag{26}$$

where $mw[C(I-\overline{\{i\}})^b] = \infty$, if $I \subseteq \overline{\{i\}}$.

Proof: If follows from (19) and (25) that $b_{ji} = 0$ for $1 \le j \le m$ if and only if $a_h = 0$ for $h \in I \cap \overline{\{i\}}$. Suppose that there is an integer $h \in I \cap \overline{\{i\}}$ such that $a_h \neq 0$. Then the weight of $(b_{1i}, b_{2i}, \cdots, b_{mi})$ is at least $mw[\tilde{C}_i]$. Hence there are at least $mw[\tilde{C}_i]$ nonzero codewords of $C_b(I)$ in $\{\bar{v}_1, \bar{v}_2, \cdots, \bar{v}_m\}$ where $\bar{v}_j$ is given by (22). Then this theorem follows from (12). ΔΔ

The following lemma holds for $\tilde{C}_i$.

Lemma 1: Suppose that $m(i) = m$ and there are integers h and s such that $0 \le h < m$, $0 < s \le m$ and

$$Q(i,I) = \{q | m-q \equiv h+j (\text{mod } m), 0 \le q < m \text{ and } 0 \le j < s\}.$$

Then $\tilde{C}_i$ is a maximum distance separable (m,s) code over $GF(2^m)$.

Proof: Consider a polynomial F(X) over $GF(2^m)$ of the following form:

$$F(X) = \sum_{q \in Q(i,I)} c_q X^{2^{m-q}}.$$

Then,

$$F(X)^{2^{m-h}} = \sum_{j=0}^{s-1} c_{m-h-j}^{2^{m-h}} X^{2^j},$$

where the suffix of a coefficient is taken modulo m. Since $F(X)^{2^{m-h}}$ is a linearized polynomial of degree 2^{s-1} or less [5], the zeros of F(X) in $GR(2^m)$ form a subspace of $GF(2^m)$ whose dimension is at most s-1. Hence at most s-1 elements of $\{\delta_1, \delta_2, \cdots, \delta_m\}$ can be roots of F(X). It follows from the definition of $\tilde{C}_j$ that $mw[\tilde{C}_i] = m-s+1$.

Since $\#Q(i,I) = s$, $\tilde{C}_i$ is a maximum distance separable (m,s) code.

ΔΔ

Example 1: For an integer m greater than 2, let $n = 2^m - 1$, and let $I = \{1,2,3,4\}$. Then C(I) is $RS_{4,e}$, $Q(3,I) = \{0\}$, and $Q(1,I') = \{0,1,2\}$ where $I' = I - \overline{\{3\}}$. It is known [6,7] that

$$\begin{aligned} mw[C_b(I')] &= 2^{m-1}, && \text{for odd } m, \\ &= 2^{m-1}-2^{m/2-1}, && \text{for even } m \text{ such that } m/2 \text{ is even}, \\ &= 2^{m-1}-2^{m/2}, && \text{for even } m \text{ such that } m/2 \text{ is odd}, \end{aligned}$$

and

$$\begin{aligned} mw[C_b(I)] &= 2^{m-1}-2^{(m-1)/2}, && \text{for odd } m, \\ &= 2^{m-1}-2^{m/2}, && \text{for even } m. \end{aligned}$$

Since $mw[\tilde{C}_1] = m-2$ and $mw[\tilde{C}_3] = m$ by Lemma 1, it follows from Theorem 2 that

$$\begin{aligned} mw[C(I)^{(b)}] = mw[C(I')^{(b)}] &\geq (m-2)2^{m-1}, \quad \text{for odd } m, \\ &\geq (m-2)(2^{m-1}-2^{m/2-1}), \\ &\qquad \text{for even } m \text{ such that } m/2 \text{ is even}, \\ &\geq (m-2)(2^{m-1}-2^{m/2}), \\ &\qquad \text{for even } m \text{ such that } m/2 \text{ is odd}. \end{aligned}$$

ΔΔ

4. Binary Weight Enumerator for ERS_4

Hereafter we assume that

$$m \geq 3,$$

$$n = 2^m-1.$$

For $0 \leq i < j < n$, let

$$I_{i,j} = \{ i, i-1, \cdots, j\}.$$

Then it is known [5] that

$$RS_k = \{ v(f(X)) \mid f(X) \in P(I_{0,k-1}) \} , \tag{27}$$

$$RS_{k,e} = \{ v(f(X)) \mid f(X) \in P(I_{1,k}) \} , \tag{28}$$

and

$$ERS_k = \{ ev(f(X)) \mid f(X) \in P(I_{0,k-1}) \} . \tag{29}$$

For $0 \le h < n-1$, $v[f(\alpha^h X)]$ is the vector obtained from $v[f(X)]$ by the h symbol cyclic shift, $ev[f(\alpha^h X)]$ is the vector obtained from $ev[f(X)]$ by the h symbol cyclic shift among the second to the last symbols, and

$$|v[f(\alpha^h X)]|_2 = |v[f(X)]|_2 , \tag{30}$$

$$|ev[f(\alpha^h X)]|_2 = |ev[f(X)]|_2 . \tag{31}$$

For $f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 \in P(I_{0,3})$, $ev[f(X)] \in ERS_4 - ERS_3$ if and only if $a_3 \neq 0$. The cyclic permutations on the second to the last symbols induce a permutation group on the codewords of ERS_4, which divides $ERS_4 - ERS_3$ into disjoint set of transitivity. Each set consists of $(2^m-1)/\nu$ codewords, where

$$\nu = (2^m-1, 3) ,$$

where (a,b) denotes the greatest common divisor of integers a and b. If m is odd, then

$$\nu = 1 , \tag{32}$$

and otherwise,

$$\nu = 3 . \tag{33}$$

Let $ev[a_0+a_1X+a_2X^2+\alpha^h X^3]$ for $0 \le h < \nu$ represent each set of $(2^m-1)/\nu$ codewords of $ERS_4 - ERS_3$. Note that

$$\begin{aligned} &Tr(\delta_j a_0+\delta_j a_1 X+\delta_j a_2 X^2+\delta_j \alpha^h X^3) \\ &\qquad = Tr(\delta_j a_0+[\delta_j a_1+(\delta_j a_2)^{2^{m-1}}]X+\delta_j \alpha^h X^3) . \end{aligned} \tag{34}$$

On the weight of $ev[Tr(b_0+b_1X+b_3X^3)]$ where b_0, b_1 and b_3 are in $GF(2^m)$, the following theorem holds [6,7].

Theorem 3:

(1) For odd m and $0 \le i < n$,

$$|ev[Tr(b_0+\alpha^i b_1 X+\alpha^{3i}X^3)]|_2$$

$$= 2^{m-1} \quad , \text{ if } Tr(b_1) = 0 \; , \tag{35}$$

$$= 2^{m-1} \pm 2^{(m-1)/2} \; , \text{ if } Tr(b_1) = 1 \; . \tag{36}$$

(2) For even m and $0 \le i < n$,

$$|ev[Tr(b_0+\alpha^i b_1 X+\alpha^{3i}X^3)]|_2$$

$$= 2^{m-1} \pm 2^{m/2} \; , \text{ if } Tr^{(2)}(b_1) = 0 \; , \tag{37}$$

$$= 2^{m-1} \quad , \text{ if } Tr^{(2)}(b_1) \neq 0 \; , \tag{38}$$

(3) For even m, $0 \le i < n$ and $1 \le h \le 2$,

$$|ev[Tr(b_0+b_1X+\alpha^{3i+h}X^3)]|_2$$

$$= 2^{m-1} \pm 2^{m/2-1} \; . \tag{39}$$

(4) If $Tr(b_0) \neq Tr(b_0')$, then

$$|ev[Tr(b_0+b_1X+b_3X^3)]|_2 + |ev[Tr(b_0'+b_1X+b_3X^3)]|_2$$

$$= 2^m \; . \tag{40}$$

ΔΔ

For $0 \le i \le m2^m$, let $N_i^{(k)}$ denote the number of codewords of weight i in ERS_k. For deriving the weight enumerator for ERS_4-ERS_3, there are two cases to be considered.

4.1 Case I: m is odd.

Suppose that m is odd. Then, $\nu = 1$. For $1 \le j \le m$, let δ_j be represented as

$$\delta_j = \alpha^{u_j} . \tag{41}$$

Since 2^m-1 and 3 are relatively prime, there is an integer μ such that $1 \le \mu < 2^m-1$ and

$$3\mu \equiv 1 \bmod (2^m-1) . \tag{42}$$

Then

$$\delta_j = \alpha^{3\mu u_j} . \tag{43}$$

Let $ev[a_0+a_1X+a_2X^2+X^3]$, denoted $\bar{v}$, be a representative codeword in ERS_4-ERS_3. Then the v_j component vector of $\bar{v}, \bar{v}_j$, is defined by

$$\bar{v}_j = ev[Tr(\delta_j a_0+\delta_j a_1X+\delta_j a_2X^2+\delta_j X^3)] \quad \text{for } 1 \le j \le m .$$

By (34) and (43), we have that

$$Tr(\delta_j a_0+\delta_j a_1X+\delta_j a_2X^2+\delta_j X^3)$$

$$= Tr(\alpha^{3\mu u_j}a_0+\alpha^{\mu u_j}(\alpha^{2\mu u_j}a_1+[\alpha^{\mu u_j}a_2]^{2^{m-1}})X+\alpha^{3\mu u_j}X^3) . \tag{44}$$

Since $Tr(X^2) = Tr(X^{2^{m-1}}) = Tr(X)$ for $X \in GF(2^m)$, it follows from (1) of Theorem 3 and (44) that if $Tr(\alpha^{2\mu u_j}a_1) = Tr(\alpha^{\mu u_j}a_2)$, then

$$|\bar{v}_j|_2 = 2^{m-1} , \tag{45}$$

and otherwise,

$$|\bar{v}_j|_2 = 2^{m-1} \pm 2^{(m-1)/2} . \tag{46}$$

Let $S_+(\bar{v})$ and $S_-(\bar{v})$ be defined as

$$S_+(\bar{v}) = \#\{ i \mid |\bar{v}_j|_2 = 2^{m-1} + 2^{(m-1)/2} , 1 \le j \le m \} ,$$

$$S_-(\bar{v}) = \#\{ i \mid |\bar{v}_j|_2 = 2^{m-1} - 2^{(m-1)/2} , 1 \le j \le m \} ,$$

Then it follows from (45) and (46) that

$$\#\{\ i\ |\ |\bar{v}_j|_2 = 2^{m-1}\ ,\ 1 \le j \le m\ \} = m - S_+(\bar{v}) - S_-(\bar{v})\ .$$

Then we have that

$$|\bar{v}|_2 = m2^{m-1} + (S_+(\bar{v}) - S_-(\bar{v}))2^{(m-1)/2}\ . \tag{47}$$

Suppose that $\{\delta_1^\mu, \delta_2^\mu, \cdots, \delta_m^\mu\}$ is linearly independent. It follows from (42) that μ is relatively prime to 2^m-1. If $\{\ \delta_1, \delta_2, \cdots, \delta_m\}$ is a polynomial basis, then $\{\delta_1^\mu, \delta_2^\mu, \cdots, \delta_m^\mu\}$ is linearly independent. Since $\delta_j = \alpha^{3\mu u_j}$ and $\delta_j^\mu = \alpha^{\mu u_j}$, $\{\alpha^{i\mu u_1}, \alpha^{i\mu u_2}, \cdots, \alpha^{i\mu u_m}\}$ is linearly independent for $1 \le i \le 3$. Therefore, we have that

$$\{\ (Tr(\alpha^{\mu u_1}a_2), Tr(\alpha^{\mu u_2}a_2), \cdots, Tr(\alpha^{\mu u_m}a_2))\ |\ a_2 \in GF(2^m)\ \}$$

$$= \{\ (Tr(\alpha^{2\mu u_1}a_1), Tr(\alpha^{2\mu u_2}a_1), \cdots, Tr(\alpha^{2\mu u_m}a_1))\ |\ a_1 \in GF(2^m)\ \}$$

$$= \{\ (Tr(\alpha^{3\mu u_1}a_0), Tr(\alpha^{3\mu u_2}a_0), \cdots, Tr(\alpha^{3\mu u_m}a_0))\ |\ a_0 \in GF(2^m)\ \}$$

$$= \text{the set of all binary m-tuples.} \tag{48}$$

It follows from (40) and (45) to (48) that for given nonnegative integers s_+ and s_- with $0 \le s_+ + s_- \le m$, the number of choices of (a_0, a_1, a_2) of $\bar{v}$ such that $S_+(\bar{v}) = s_+$ and $S_-(\bar{v}) = s_-$ is given by

$$\binom{m}{s_+}\binom{m-s_+}{s_-}2^{s_++s_-}4^{m-s_+-s_-}\ .$$

Since there are 2^m-1 choices of nonzero a_3, it follows from (47) and (48) that for $0 \le j \le m$,

$$N^{(4)}_{m2^{m-1}\pm j2^{(m-1)/2}} - N^{(3)}_{m2^{m-1}\pm j2^{(m-1)/2}}$$

$$= (2^m-1) \sum_{i=0}^{\lfloor (m-j)/2 \rfloor} \binom{m}{j+i} \binom{m-j-i}{i} 2^{2m-j-2i} , \tag{49}$$

$$N_i^{(4)} = N_i^{(3)} \quad , \quad \text{for other } i , \tag{50}$$

where sign $\pm$ is to be taken in the same order.

4.2 Case II: m is even.

Suppose that m is even. Then, $m \geq 4$ and $\nu = 3$. For $1 \leq j \leq m$, let δ_j be represented as

$$\delta_j = \alpha^{3u_j+w_j}, \tag{51}$$

where $0 \leq u_j < (2^m-1)/3$ and $0 \leq w_j \leq 2$. For $f(x) \in P(I_{0,3}) - P(I_{0,2})$, let the coefficient of X^3 be represented as α^e, and let

$$e \equiv h, \bmod 3, \ 0 \leq h \leq 2. \tag{52}$$

Let $ev[a_0 + a_1X + a_2X^2 + \alpha^hX^3]$, denoted $\bar{v}$, be a representative codeword. Then the δ_j component vector of $\bar{v}$, $\bar{v}_j$, is defined by

$$\bar{v}_j = ev[Tr(\delta_j a_0 + \delta_j a_1 X + \delta_j a_2 X^2 + \delta_j \alpha^h X^3)], \text{ for } 1 \leq j \leq m.$$

By (34), we have that

$$\bar{v}_j = ev[Tr(\alpha^{3u_j+w_j}a_0 + [\alpha^{3u_j+w_j}a_1 + (\alpha^{3u_j+w_j}a_2)^{2^{m-1}}]X + \alpha^{3u_j+w_j+h}X^3)]. \tag{53}$$

For $0 \leq h \leq 2$, let

$$J_h = \{ j \mid w_j+h \equiv 0 \pmod 3), 1 \leq j \leq m\},$$

and

$$CJ_h = \{1,2,\cdots,m\} - J_h.$$

It follows from (3) of Theorem 3 and (53) that for $0 \leq h \leq 2$ and $j \in CJ_h$,

$$|\bar{v}_j|_2 = 2^{m-1} \pm 2^{m/2-1}. \tag{54}$$

For $0 \le h \le 2$ and $j \in J_h$, it follows from (53) that

$$\bar{v}_j = ev[Tr(\alpha^{3u_j}a_0 + \alpha^{u_j}[\alpha^{2u_j}a_1 + (\alpha^{2u_j}a_2^2)^{2^{m-2}}]X + \alpha^{3u_j}X^3)] ,$$

for $h = 0$, (55)

$$= ev[Tr(\alpha^{3u_j+2}a_0 + \alpha^{u_j+1}[\alpha^{2u_j+1}a_1 + (\alpha^{2u_j}a_2^2)^{2^{m-2}}]X + \alpha^{3(u_j+1)}X^3)] ,$$

for $h = 1$, (56)

$$= ev[Tr(\alpha^{3u_j+1}a_0 + \alpha^{u_j+1}[\alpha^{2u_j}a_1 + (\alpha^{2u_j-2}a_2^2)^{2^{m-2}}]X + \alpha^{3(u_j+1)}X^3)] ,$$

for $h = 2$. (57)

Since $Tr^{(2)}(X^{2^{m-2}}) = Tr^{(2)}(X)$ for even m and X in $GF(2^m)$, it follows from (2) of Theorem 3 and (55) to (57) that if either $j \in J_0$ and $Tr^{(2)}(\alpha^{2u_j}a_1) = Tr^{(2)}(\alpha^{2u_j}a_2^2)$, or $j \in J_1$ and $Tr^{(2)}(\alpha^{2u_j+1}a_1) = Tr^{(2)}(\alpha^{2u_j}a_2^2)$, or $j \in J_2$ and $Tr^{(2)}(\alpha^{2u_j}a_1) = Tr^{(2)}(\alpha^{2u_j-2}a_2^2)$, then

$$|\bar{v}_j|_2 = 2^{m-1} \pm 2^{m/2}, \qquad (58)$$

and otherwise,

$$|\bar{v}_j|_2 = 2^{m-1}. \qquad (59)$$

Suppose that for $0 \le h \le 2$, $\{ \alpha^{2u_j} \mid j \in J_h\}$ is linearly independent over $GF(2^2)$. This condition holds for a primitive polynomial basis.

For $0 \le h \le 2$, let $\{ u_j \mid j \in J_h\}$ be represented by $\{u_{h1}, u_{h2}, \cdots, u_{hj_h}\}$, where $j_h = \#J_h$. Since $\{ a^2 \mid a \in GF(2^m)\} = \{ \alpha^i a \mid a \in GF(2^m) \} = GF(2^m)$ for an integer i, we have that

$$\{(Tr^{(2)}(\alpha^{2u_{01}}a_1), Tr^{(2)}(\alpha^{2u_{02}}a_1), \cdots, Tr^{(2)}(\alpha^{2u_{0j_0}}a_1)) \mid a_1 \in GF(2^m)\}$$

$$=\{(Tr^{(2)}(\alpha^{2u_{01}}a_2^2), Tr^{(2)}(\alpha^{2u_{02}}a_2^2), \cdots, Tr^{(2)}(\alpha^{2u_{0j_0}}a_2^2)) \mid a_2 \in GF(2^m)\}$$

$=$ the set of all j_0-tuples over $GF(2^2)$, (60)

$$\{(Tr^{(2)}(\alpha^{2u_{11}+1}a_1), Tr^{(2)}(\alpha^{2u_{12}+1}a_1), \cdots, Tr^{(2)}(\alpha^{2u_{1j_1}+1}a_1)) \mid a_1 \in GF(2^m)\}$$

$$= \{(Tr^{(2)}(\alpha^{2u_{11}}a_2^2),\ Tr^{(2)}(\alpha^{2u_{12}}a_2^2),\ \cdots,\ Tr^{(2)}(\alpha^{2u_{1j_1}}a_2^2)) \mid a_2 \in GF(2^m)\}$$

$=$ the set of all j_1-tuples over $GF(2^2)$, (61)

$$\{(Tr^{(2)}(\alpha^{2u_{21}}a_1),\ Tr^{(2)}(\alpha^{2u_{22}}a_1),\ \cdots,\ Tr^{(2)}(\alpha^{2u_{2j_2}}a_1)) \mid a_1 \in GF(2^m)\}$$

$$= \{(Tr^{(2)}(\alpha^{2u_{21}-2}a_2^2), Tr^{(2)}(\alpha^{2u_{22}-2}a_2^2), \cdots, Tr^{(2)}(\alpha^{2u_{2j_2}-2}a_2^2)) \mid a_2 \in GF(2^m)\}$$

$=$ the set of all j_2-tuples over $GF(2^2)$. (62)

For any given j_0-tuple $(b_1, b_2, \cdots, b_{j_0})$ over $GF(2^2)$, the number of a_1 in $GF(2^m)$ such that $Tr^{(2)}(\alpha^{2u_{0j}}a_1) = b_j$ for $1 \le j \le j_0$ is 2^{m-2j_0}. For other sets in (60) to (62), similar results hold. Since $\{\delta_1, \delta_2, \cdots, \delta_m\}$ is linearly independent, we have that

$$\{Tr(\delta_1 a_0),\ Tr(\delta_2 a_0),\ \cdots,\ Tr(\delta_m a_0) \mid a_0 \in GF(2^m)\}$$

$=$ the set of all binary m-tuples. (63)

Let $S_+(\bar{v})$, $S_-(\bar{v})$ and $T_+(\bar{v})$ be defined as

$$S_+(\bar{v}) = \#\{\ i \mid |\bar{v}_j|_2 = 2^{m-1} + 2^{m/2},\ j \in J_h\}, \tag{64}$$

$$S_-(\bar{v}) = \#\{\ i \mid |\bar{v}_j|_2 = 2^{m-1} - 2^{m/2},\ j \in J_h\}, \tag{65}$$

$$T_+(\bar{v}) = \#\{\ i \mid |\bar{v}_j|_2 = 2^{m-1} + 2^{m/2-1},\ j \in CJ_h\}. \tag{66}$$

Then it follows from (54) and (59) that

$$\#\{\ i \mid |\bar{v}_j|_2 = 2^{m-1} - 2^{m/2-1},\ 1 \le j \le m\} = m - j_h - T_+(\bar{v})\ , \tag{67}$$

$$\# \{ i \mid |\bar{v}_j|_2 = 2^{m-1}, 1 \le j \le m \} = j_h - S_+(\bar{v}) - S_-(\bar{v}) . \tag{68}$$

Then it follows from (13), (2) and (3) of Theorem 3 and (64) to (68) that

$$|\bar{v}_j|_2 = m2^{m-1} + (2S_+(\bar{v}) - 2S_-(\bar{v}) + 2T_+(\bar{v}) - m + j_h)2^{m/2-1}. \tag{69}$$

It follows from (4) of Theorem 3 and (54) to (63) that for given nonnegative integers s_+, s_- and t_+ with $0 \le s_+ + s_- \le j_h$ and $0 \le t_+ \le m - j_h$, the number of choices of (a_0,a_1,a_2) of $\bar{v}$ such that $s_+ = S_+(\bar{v})$, $s_- = S_-(\bar{v})$ and $t_+ = T_+(\bar{v})$ is given by

$$\binom{j_h}{s_+}\binom{j_h-s_+}{s_-}\binom{m-j_h}{t_+}2^{2(s_++s_-)}24^{j_h-s_+-s_-}2^{2m-4j_h}. \tag{70}$$

For $0 \le h \le 2$ and integer j with $-2m \le j \le 2m$, let $D_{h,j}$ be defined by

$$D_{h,j} = \{ (s_+,s_-,t_+) \mid 0 \le s_+ \le j_h, 0 \le s_- \le j_h, 0 \le s_+ + s_- \le j_h,$$
$$0 \le t_+ \le m - j_h,\ 2(s_+ - s_- + t_+) = m + j - j_h\} . \tag{71}$$

Since there are $(2^m-1)/3$ choices of nonzero α^e satisfying (52), it follows from (69), (70) and (71) that for $-2m \le j \le 2m$,

$$N^{(4)}_{m2^{m-1}+j2^{m/2-1}} - N^{(3)}_{m2^{m-1}+j2^{m/2-1}}$$
$$= (2^m-1)/3 \sum_{h=0}^{2} \sum_{(s_+,s_-,t_+)\in D_{h,j}} \binom{j_h}{s_+}\binom{j_h-s_+}{s_-}\binom{m-j_h}{t_+}24^{j_h-s_+-s_-}4^{m+s_++s_--2j_h},$$

and

$$N_i^{(4)} = N_i^{(3)} , \text{ for other } i. \tag{72}$$

<u>4.3 Binary Weight Enumerator for ERS_3</u>

Let $\bar{v} = ev[a_0+a_1X+a_2X^2]$, and $\bar{v}_j = ev[\delta_j a_0 + \delta_j a_1 X + \delta_j a_2 X^2]$. If $a_1 = a_2 = 0$, then

$$|\bar{v}|_2 = |ev[a_0]|_2 = 2^m|a_0|_2, \tag{73}$$

where $|a_0|_2$ denotes the weight of the binary representation of a_0 in $GF(2^m)$. For $0 \le j \le m$,

$$N^{(1)}_{j2^m} = \binom{m}{j} , \tag{74}$$

$$N^{(1)}_i = 0 , \quad \text{for other } i. \tag{75}$$

Suppose that either $a_1 \neq 0$ or $a_2 \neq 0$. There are $2^m(2^{2m}-1)$ combinations of such (a_0, a_1, a_2). Note that

$$\mathrm{Tr}(\delta_j a_0+\delta_j a_1 X+\delta_j a_2 X^2)$$

$$= \mathrm{Tr}(\delta_j a_0 + [\delta_j a_1 + (\delta_j a_2)^{2^{m-1}}]X) . \tag{76}$$

For each j with $1 \le j \le m$, $\delta_j a_1+(\delta_j a_2)^{2^{m-1}} = 0$ if and only if $a_2 = a_1^2\delta_j$. There are $m2^{m-1}(2^m-1)$ combinations of (a_0, a_1, a_2) such that $a_2 = a_1^2\delta_j$ and $\mathrm{Tr}(\delta_j a_0) = 0$ (or 1). If $\delta_j a_1 + (\delta_j a_2)^{2^{m-1}} = 0$ and $\mathrm{Tr}(\delta_j a_0) = 0$ (or 1), then

$$|v_j|_2 = |ev[\mathrm{Tr}(\delta_j a_0)]|_2 = 0 \quad (\text{or } 2^m) . \tag{77}$$

If $\delta_j a_1 + (\delta_j a_2)^{2^{m-1}} \neq 0$, then

$$|v_j|_2 = |ev[\mathrm{Tr}(\delta_j a_0+[\delta_j a_1+(\delta_j a_2)^{2^{m-1}}]X)]|_2 = 2^{m-1} . \tag{78}$$

Therefore, we have that

$$N^{(3)}_{(m+1)2^{m-1}} - N^{(1)}_{(m+1)2^{m-1}} = m2^{m-1}(2^m-1) , \tag{79}$$

$$N^{(3)}_{m2^{m-1}} - N^{(1)}_{m2^{m-1}} = 2^m(2^m-1)(2^m+1-m) , \tag{80}$$

$$N^{(3)}_{(m-1)2^{m-1}} - N^{(1)}_{(m-1)2^{m-1}} = m2^{m-1}(2^m-1) , \tag{81}$$

$$N^{(3)}_i = N^{(1)}_i , \quad \text{for other } i . \tag{82}$$

Note that the binary weight enumerator for ERS_3 is independent of the choice of basis.

REFERENCES

1. S. Lin and D. J. Costello, Jr., Error Control Coding: Fundamentals and Applications, Prentice-Hall, New Jersey, 1983.

2. T. Kasami and S. Lin, "On the binary weight distribution of some Reed-Solomon Codes," Proc. of the 7th Symposium on Information Theory and its Applications, Kinugawa, Japan, pp. 49-54, November, 1984.

3. K. Imamura, W. Yoshida and N. Nakamura, "The binary weight distribution of $(n = 2^m-1,\ k = 2)$ Reed-Solomon code whose generator polynomial is $g(X) = (X^n-1)/(X-\alpha^{-1})(X-\alpha^{-2})$," Papers of Inst. Elec. Commun. Eng. Japan, IT86-9, pp. 11-15, May, 1986.

4. K. Tokiwa and M. Kasahara, "Binary Wright Distribution of $(n=2^m-1, k=3)$ RS Code with Generator Polynomial $(x^n-1)/(x-1)(x-\alpha^{-1})(x-\alpha^{-2})$", Proc. of the 9th Symposium on Information Theory and its Applications, Akakura, Japan, pp.143-146, October 1986.

5. F. J. MacWilliams and N. J. A. Sloane, Theory of Error-Correcting Codes, North Holland, Amsterdam, 1977.

6. T. Kasami, "Weight Distribution Formula for Some Class of Cyclic Codes," Report of Coordinated Science Laboratory, Univ. of Illinois, Urbana, Illinois, 1966.

7. T. Kasami, S. Lin and W. W. Peterson, "Some results on cyclic codes which are invariant under the Affine group and their applications," Information and Control, Vol.11, pp. 475-496, November, 1967.