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 \((2^m, 2^m-4)\) CODE OF REED-SOLOMON CODE OVER GF\(2^m\) WITH GENERATOR POLYNOMIAL \((x-\alpha)(x-\alpha^2)(x-\alpha^3)\)

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 \((x-a)(x-a^2)(x-a^3)\)

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 \((x-a)(x-a^2)(x-a^3)\) and its dual code, where \(a\) 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 \(1 \leq i \leq m\). 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 $1 \leq j \leq m$. A polynomial basis will be said to be primitive, if $\beta$ is primitive.

Let $\alpha$ be a primitive element of $\text{GF}(2^m)$, and let $n = 2^m - 1$. For $1 \leq k < n$, let $\text{RS}_k$ denote the $(n, k)$ Reed-Solomon code over $\text{GF}(2^m)$ with generator polynomial $(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{n-k})$ [1], let $\text{RS}_{k,e}$ denote the $(n, k)$ Reed-Solomon code over $\text{GF}(2^m)$ with generator polynomial $(x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{n-k-1})$, and let $\text{ERS}_k$ be the extended $(n+1, k)$ code of $\text{RS}_k$. The dual code of $\text{RS}_k$ is $\text{RS}_{n-k,e}$, and the dual code of $\text{ERS}_k$ is $\text{ERS}_{n+1-k}$.

Binary weight enumerators for $\text{RS}_{n-1}$ with $1 \leq i \leq 2$, $\text{RS}_{n-1,e}$ with $2 \leq i \leq 3$ and $\text{ERS}_{n-1}$ with $1 \leq i \leq 2$ were presented in [2], and those for $\text{RS}_2,e$, the dual code of $\text{RS}_{n-2}$, and $\text{RS}_3$, the dual code of $\text{RS}_{n-3,e}$, 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 $\text{GF}(2^m)$ by using the complementary basis of a basis $\{\beta_1, \beta_2, \ldots, \beta_m\}$ is shown to be the dual code of the binary image of $C$ by using basis $\{\beta_1, \beta_2, \ldots, \beta_m\}$. In section 3, a lower bound on the minimum weight of a binary image of a cyclic code over $\text{GF}(2^m)$. In section 4, the binary weight enumerator of $\text{ERS}_n$ is derived for a class of bases including the complementary bases of primitive polynomial bases. By Theorem 1 the binary weight enumerator for $\text{ERS}_{n-3}$ is obtained. This approach can be readily extended to derive the binary weight enumerator for $\text{ERS}_5$.

2. Binary Images of Linear Block Codes over $\text{GF}(2^m)$

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

$$\text{Tr}(\beta_1\delta_j) = 0, \quad \text{for } i \neq j,$$

$$\text{Tr}(\beta_i\delta_i) = 1,$$

where $\text{Tr}(x)$ 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 $\{\delta_1, \delta_2, \ldots, \delta_m\}$ of $\{\beta_1, \beta_2, \ldots, \beta_m\}$. Then we have Theorem 1.

**Theorem 1:** $C_D(b)$ is the dual code of $C(b)$.

**Proof:** Let $(a_1, a_2, \ldots, a_n)$ and $(b_1, b_2, \ldots, b_n)$ be codewords of $C$ and $C^D$ respectively. Then

$$\sum_{i=1}^{n} a_i b_i = 0. \quad (1)$$

Let

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

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

It follows from (1) to (3) that

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

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

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

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

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

Equation (6) implies that $C_D(b)$ is the dual code of $C(b)$. \[\Delta\Delta\]

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

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

where $v_1 = \sum_{j=1}^{m} v_{1j}\beta_j$ with $v_{ij} \in GF(2)$ for $1 \leq i \leq n$. If $\{\delta_1, \delta_2, \ldots, \delta_m\}$
is the complementary basis of \( \{ \delta_1, \delta_2, \ldots, \delta_m \} \), then \( \bar{v}_j \) is represented as

\[
\bar{v}_j = (\text{Tr}(\delta_j v_1), \text{Tr}(\delta_j v_2), \ldots, \text{Tr}(\delta_j v_n)) , 
\]

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

\[
|\bar{v}|_2 = \sum_{j=1}^{m} |\bar{v}_j|_2 .
\]

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 \( \{0,1,2, \ldots ,n-1\} \), \( I \) 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 \( I \).

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

\[
\prod_{i \in I} (x - Y^i).
\]

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

\[
\prod_{i \in I} (x - Y^i).
\]

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

\[
v[f(X)] = (f(1), f(Y), f(Y^2), \ldots , f(Y^{n-1})) ,
\]

and

\[
ev[f(X)] = (f(0), f(1), f(Y), \ldots , f(Y^{n-1})) .
\]

It follows from (8) and (9) that
For a subset $I$ of $\{0, 1, 2, \cdots, n-1\}$, let $P(I)$ be defined by

$$P(I) = \{ \sum_{i \in I} a_i x^i \mid a_i \in \mathbb{F}_{2^m} \text{ for } i \in I \}.$$  

As is well-known[5],

$$C(I) = \{v[f(x)] \mid f \in P(I)\}.$$  

It follows from (8), (10) and the definitions of $C(I)$ and $C_b(I)$ that for $\vec{v} = v[f(x)] \in C(I)$, the $i$-th component vector of $\vec{v}$, denoted $\vec{v}_i$, is given by

$$\vec{v}_i = v[\text{Tr}(\delta_j f(x))], \quad 1 \leq j \leq m,$$

and

$$\vec{v}_i \in C_b(I).$$

As is also known [5],

$$C_b(I) = \{v[\sum_{i \in \text{Rc}(I)} \text{Tr}_m(1)(a_i x^i)] \mid a_i \in \mathbb{F}(2^m(1)) \text{ for } i \in \text{Rc}(I)\}, \quad (16)$$

where

$$\text{Tr}_j(x) = x + x^2 + \cdots + x^{2^{j-1}}.$$  

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

$$f(X) = \sum_{i \in \text{Rc}(I)} \sum_{q \in \mathbb{Q}(i, I)} a_{i2^q} x^{i2^q}, \quad (17)$$

where $i2^q$ is taken modulo $n$ and
Q(1, I) = \{ q | p:12q \equiv p \pmod{n}, p \in I \text{ and } 0 \leq q < m(1) \}.

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

$$Tr(\delta_j f(X)) = \sum_{i \in R_c(I)} Tr_{m(1)}(b_j x^i),$$  \hspace{1cm} (18)

where

$$b_j = Tr_{m(1)}( \sum_{q \in Q(1, I)} \delta_j^{m(1)-q} a_2^{m(1)-q} ), \quad i \in R_c(I), \quad (19)$$

where for a divisor $h$ of $m$

$$Tr(h)(X) = x + x^{2h} + x^{2h} + \cdots + x^{2m-h}.$$ \hspace{1cm} (20)

Note that

$$b_j \in GF(2^{m(1)}).$$ \hspace{1cm} (21)

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

$$\bar{v}_j = v[ \sum_{i \in R_c(I)} Tr_{m(1)}(b_j x^i) ].$$ \hspace{1cm} (22)

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

$$\bar{C}_i = \{ (b_1, b_2, \cdots, b_m) \mid b_j = Tr_{m(1)}( \sum_{q \in Q(1, I)} \delta_j^{m(1)-q} a_q ) , \quad 1 \leq j \leq m, \quad a_q \in GF(2^m) \}.$$ \hspace{1cm} (23)

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

$$D = \begin{bmatrix}
\delta_1 & \delta_1^{m-1} & \delta_1^{m-2} & \cdots & \delta_1^2 & \delta_1 \\
\delta_2 & \delta_2^{m-1} & \delta_2^{m-2} & \cdots & \delta_2^2 & \delta_2 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
\delta_m & \delta_m^{m-1} & \delta_m^{m-2} & \cdots & \delta_m^2 & \delta_m
\end{bmatrix}.$$ \hspace{1cm} (24)
If $\text{Tr}(m(i)) \left( \sum_{q \in Q(i,I)} 2^{m(i)-q} \delta^j a'_q \right) = 0$ for $1 \leq j \leq m$, then

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

(25)

Hence $\tilde{C}_i$ is a linear $(m, \#Q(i,I)m/m(i))$ code over $\text{GF}(2^{m(i)})$, 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 $i \in I$,

$$mw[C(I)^{(b)}] \geq \min \{ mw[\tilde{C}_i], mw[C_{b}(I)], mw[C(I-\{i\})^{(b)}] \},$$

(26)

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

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

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

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

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

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

**Proof**: Consider a polynomial $F(X)$ over $\text{GF}(2^m)$ of the following form:

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

Then,

$$F(X)^{2^{m-h}} = \sum_{j=0}^{s-1} c_{2^m-h-j} X^{2^j}.$$
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 \( \text{GR}(2^m) \) form a subspace of \( \text{GF}(2^m) \) whose dimension is at most \( s-1 \). Hence at most \( s-1 \) elements of \( \{\delta_1, \delta_2, \ldots, \delta_m\} \) can be roots of \( F(X) \). It follows from the definition of \( \tilde{C}_j \) that \( \text{mw}[\tilde{C}_j] = m-s+1 \).

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

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

\[
\text{mw}[C_6(I')] = 2^{m-1}, \text{ for odd } m, \\
= 2^{m-1} - 2^{m/2-1}, \text{ for even } m \text{ such that } m/2 \text{ is even,} \\
= 2^{m-1} - 2^{m/2}, \text{ for even } m \text{ such that } m/2 \text{ is odd,}
\]

and

\[
\text{mw}[C_6(I)] = 2^{m-1} - 2^{(m-1)/2}, \text{ for odd } m, \\
= 2^{m-1} - 2^m/2, \text{ for even } m.
\]

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

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

4. Binary Weight Enumerator for \( \text{ERS}_4 \)

Hereafter we assume that

\( m \geq 3, \)

\( n = 2^m - 1. \)

For \( 0 \leq i < j < n \), let

\( I_{i,j} = \{i, i+1, \ldots, j\}. \)

Then it is known [5] that
For $0 \leq h < n-1$, $v(f(a^hX))$ is the vector obtained from $v(f(X))$ by the $h$ symbol cyclic shift, $ev(f(a^hX))$ is the vector obtained from $ev(f(X))$ by the $h$ symbol cyclic shift among the second to the last symbols, and

\[ |v(f(a^hX))|_2 = |v(f(X))|_2, \quad (30) \]

\[ |ev(f(a^hX))|_2 = |ev(f(X))|_2. \quad (31) \]

For $f(X) = a_0 + a_1 X + a_2 X^2 + a_3 X^3 \in P(I_0, 3)$, $ev(f(X)) \in ERS_4 - ERS_3$ 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 $(2^m - 1)/v$ codewords, where

\[ v = (2^{m-1}, 3), \]

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

\[ v = 1, \quad (32) \]

and otherwise,

\[ v = 3. \quad (33) \]

Let $ev[a_0 + a_1 X + a_2 X^2 + a_3 X^3]$ for $0 \leq h < v$ represent each set of $(2^m - 1)/v$ codewords of $ERS_4 - ERS_3$. Note that

\[
\text{Tr}(\delta j a_0 + \delta j a_1 X + \delta j a_2 X^2 + \delta j a_3 X^3) \\
= \text{Tr}(\delta j a_0 + [\delta j a_1 + (\delta j a_2)2^{m-1}]X + \delta j a_3 X^3) \quad (34)
\]
On the weight of $ev[\text{Tr}(b_0+b_1X+b_3X^3)]$ 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 $0 \leq i < n$,

$$|ev[\text{Tr}(b_0+a^ib_1X+a^{3i}X^3)]|_2$$

$$= 2^{m-1} + 2^{(m-1)/2}, \text{ if } \text{Tr}(b_1) = 1.$$  \hspace{1cm} (35)

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

$$|ev[\text{Tr}(b_0+a^ib_1X+a^{3i}X^3)]|_2$$

$$= 2^{m-1} \pm 2^{m/2}, \text{ if } \text{Tr}^{(2)}(b_1) = 0.$$  \hspace{1cm} (36)

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

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

$$= 2^{m-1} \pm 2^{m/2-1}.$$  \hspace{1cm} (37)

(4) If $\text{Tr}(b_0) = \text{Tr}(b_0')$, then

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

$$= 2^m.$$  \hspace{1cm} (38)

For $0 \leq i \leq m2^m$, let $N_1^{(k)}$ 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 \( 1 \leq j \leq m \), let \( \delta_j \) be represented as

\[
\delta_j = a^{uj}.
\]

(41)

Since \( 2^m - 1 \) and 3 are relatively prime, there is an integer \( \mu \) such that \( 1 \leq \mu < 2^m - 1 \) and

\[
3\mu \equiv 1 \pmod{2^m - 1}.
\]

(42)

Then

\[
\delta_j = a^{3\mu u_j}.
\]

(43)

Let \( ev[a_0 + a_1 X + a_2 X^2 + X^3] \), denoted \( \bar{v} \), be a representative codeword in \( \text{ERS}_4 - \text{ERS}_3 \). Then the \( v_j \) component vector of \( \bar{v}, \bar{v}_j \), is defined by

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

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

\[
\text{Tr}(\delta_j a_0 + \delta_j a_1 X + \delta_j a_2 X^2 + \delta_j X^3)
\]

\[
= \text{Tr}(a^{3\mu u_j} a_0 + a^{3\mu u_j} a_1 X + [a^{3\mu u_j} a_2] 2^{m-1} X + a^{3\mu u_j} X^3).
\]

(44)

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

\[
|\bar{v}_j|_2 = 2^{m-1},
\]

(45)

and otherwise,

\[
|\bar{v}_j|_2 = 2^{m-1} \pm 2^{(m-1)/2}.
\]

(46)

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

\[
S_+(\bar{v}) = \# \left\{ 1 \mid |\bar{v}_j|_2 = 2^{m-1} + 2^{(m-1)/2}, 1 \leq j \leq m \right\},
\]

\[
S_- (\bar{v}) = \# \left\{ 1 \mid |\bar{v}_j|_2 = 2^{m-1} - 2^{(m-1)/2}, 1 \leq j \leq m \right\}.
\]
Then it follows from (45) and (46) that

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

Then we have that

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

Suppose that \(\{\delta_1^{\mu_1}, \delta_2^{\mu_2}, \ldots, \delta_m^{\mu_m}\}\) is linearly independent. It follows from (42) that \(u\) is relatively prime to \(2^{m-1}\). If \(\{\delta_1, \delta_2, \ldots, \delta_m\}\) is a polynomial basis, then \(\{\delta_1^{\mu_1}, \delta_2^{\mu_2}, \ldots, \delta_m^{\mu_m}\}\) is linearly independent. Since \(\delta_j = \alpha^{\mu_j}\) and \(\delta_j = \alpha^{\mu_j}\), \(\{\alpha^{1\mu_1}, \alpha^{1\mu_2}, \ldots, \alpha^{1\mu_m}\}\) is linearly independent for \(1 \leq j \leq 3\). Therefore, we have that

\[
\{(\text{Tr}(\alpha^{\mu_1}a_2), \text{Tr}(\alpha^{\mu_2}a_2), \ldots, \text{Tr}(\alpha^{\mu_m}a_2)) \mid a_2 \in GF(2^m)\}
\]

\[
= \{(\text{Tr}(\alpha^{1\mu_1}a_1), \text{Tr}(\alpha^{1\mu_2}a_1), \ldots, \text{Tr}(\alpha^{1\mu_m}a_1)) \mid a_1 \in GF(2^m)\}
\]

\[
= \{(\text{Tr}(\alpha^{3\mu_1}a_0), \text{Tr}(\alpha^{3\mu_2}a_0), \ldots, \text{Tr}(\alpha^{3\mu_m}a_0)) \mid a_0 \in GF(2^m)\}
\]

is the set of all binary \(m\)-tuples. \quad (48)

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

\[
\binom{m}{s_+}(\binom{m-s_+}{s_-})2^{s_++s_-} = 2^{m-s_+-s_-}.
\]

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

\[
N(4)_{m2^{m-1}+j2^{(m-1)/2}} - N(3)_{m2^{m-1}+j2^{(m-1)/2}}
\]
\[ = (2^{m-1}) \left\{ \sum_{j=1}^{(m-1)/2} \binom{m}{j} (j+1)(m-1)_2 2^{m-j-1} \right\}, \quad (49) \]

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

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 \( v = 3 \). For \( 1 \leq j \leq m \), let \( \delta_j \) be represented as

\[ \delta_j = \alpha \cdot 3u_j + w_j, \quad (51) \]

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 \( \alpha^e \), and let

\[ e \equiv h \mod 3, \quad 0 \leq h \leq 2. \quad (52) \]

Let \( \text{ev}[a_0 + a_1 x + a_2 x^2 + a^h x^3] \), denoted \( \tilde{v} \), be a representative codeword. Then the \( \delta_j \) component vector of \( \tilde{v} \), \( \tilde{v}_j \), is defined by

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

By (34), we have that

\[ \tilde{v}_j = \text{ev}[\text{Tr}(\alpha^{3u_j + w_j} a_0 + [\alpha^{3u_j + w_j} a_1 + (\alpha^{3u_j + w_j} a_2) 2^{m-1}] x + \alpha^{3u_j + w_j + h} x^3)]. \quad (53) \]

For \( 0 \leq h \leq 2 \), let

\[ J_h = \{ j \mid w_j + h \equiv 0 \mod 3, \quad 1 \leq j \leq m \}, \]

and

\[ CJ_h = \{1, 2, \ldots, m\} - J_h. \]

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

\[ |\tilde{v}_j|_2 = 2^{m-1} \pm 2^{m/2-1}. \quad (54) \]
For $0 \leq h \leq 2$ and $j \in J_h$, it follows from (53) that

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

for $h = 0,$ (55)

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

for $h = 1,$ (56)

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

for $h = 2.$ (57)

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

$$|\overline{v}_j|_2 = 2^{m-1} + 2^{m/2},$$

and otherwise,

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

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

For $0 \leq h \leq 2$, let $\{ u_j | j \in J_h \}$ be represented by $\{ u_{h1}, u_{h2}, \ldots, u_{hJ_h} \}$, where $J_h = \#J_h$. Since $\{ \alpha^i a | a \in \text{GF}(2^m) \} = \text{GF}(2^m)$ for an integer $i$, we have that

$$\{ (\text{Tr}(2)(\alpha^{2u_{h1}} a_1), \text{Tr}(2)(\alpha^{2u_{h2}} a_1), \ldots, \text{Tr}(2)(\alpha^{2u_{hJ_h}} a_1)) | a_1 \in \text{GF}(2^m) \}$$

$$= \{ (\text{Tr}(2)(\alpha^{2u_{h1}} a_2), \text{Tr}(2)(\alpha^{2u_{h2}} a_2), \ldots, \text{Tr}(2)(\alpha^{2u_{hJ_h}} a_2)) | a_2 \in \text{GF}(2^m) \}$$

-14-
- the set of all $j_0$-tuples over $GF(2^2)$,  
\[
\{(\text{Tr}(2)(\alpha^{2u_1+1}a_1), \text{Tr}(2)(\alpha^{2u_2+1}a_1), \ldots, \text{Tr}(2)(\alpha^{2u_j+1}a_1)) \mid a_1 \in GF(2^m)\}
\]
- the set of all $j_1$-tuples over $GF(2^2)$,  
\[
\{(\text{Tr}(2)(\alpha^{2u_1+2}a_1), \text{Tr}(2)(\alpha^{2u_2+2}a_1), \ldots, \text{Tr}(2)(\alpha^{2u_j+2}a_1)) \mid a_2 \in GF(2^m)\}
\]
- the set of all $j_2$-tuples over $GF(2^2)$,  
\[
\{(\text{Tr}(2)(\alpha^{2u_1+2}a_2), \text{Tr}(2)(\alpha^{2u_2+2}a_2), \ldots, \text{Tr}(2)(\alpha^{2u_j+2}a_2)) \mid a_2 \in GF(2^m)\}
\]

For any given $j_0$-tuple $(b_1, b_2, \ldots, b_{j_0})$ over $GF(2^2)$, the number of $a_1$ in $GF(2^m)$ such that $\text{Tr}(2)(\alpha^{2u_0}a_1) = b_j$ for $1 \leq j \leq j_0$ is $2^{m-2j_0}$. For other sets in (60) to (62), similar results hold. Since $\{\delta_1, \delta_2, \ldots, \delta_m\}$ is linearly independent, we have that
\[
\{\text{Tr}(\delta_1a_0), \text{Tr}(\delta_2a_0), \ldots, \text{Tr}(\delta_ma_0) \mid a_0 \in GF(2^m)\}
\]
- the set of all binary $m$-tuples.

Let $S_+(\vec{v}), S_-(\vec{v})$ and $T_+(\vec{v})$ be defined as
\[
S_+(\vec{v}) = \# \{ i \mid |\vec{v}_j|_2 = 2^{m-1} + 2^{m/2}, j \in J_h \}, \quad (64)
\]
\[
S_-(\vec{v}) = \# \{ i \mid |\vec{v}_j|_2 = 2^{m-1} - 2^{m/2}, j \in J_h \}, \quad (65)
\]
\[
T_+(\vec{v}) = \# \{ i \mid |\vec{v}_j|_2 = 2^{m-1} + 2^{m/2-1}, j \in C J_h \}. \quad (66)
\]

Then it follows from (54) and (59) that
\[
\# \{ i \mid |\vec{v}_j|_2 = 2^{m-1} - 2^{m/2-1}, 1 \leq j \leq m \} = m - J_h - T_+(\vec{v}), \quad (67)
\]
It follows from (4) of Theorem 3 and (54) to (63) that for given nonnegative integers \(a_+, a, t+\) with \(0 \leq a_+ \leq a \leq t+ \leq m - j_h\), 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

\[
(j_h) \binom{a_+}{s_+} \binom{a_+}{s_-} (t+) \binom{a_+}{s_+ + s_-} 2^{a_++a_1+a_2} 24^{j_h-a_+ - a_2} 2^{a_2 - 2m - 4j_h}.
\]

For \(0 \leq h \leq 2\) and integer \(j\) with \(-2m \leq j \leq 2m\), let \(D_{h,j}\) be defined by

\[
D_{h,j} = \{ (s_+, s_-, t+) | 0 \leq s_+ \leq j_h, 0 \leq s_- \leq j_h, 0 \leq s_+ + s_- \leq j_h, 0 \leq t+ \leq m - j_h, 2(s_+ - s_- + t+) = m + j - j_h \}.
\]

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

\[
N_i^{(4)} = \frac{N_i^{(3)}}{m_2^{2m-1} + j_2^2} - \frac{N_i^{(3)}}{m_2^{2m-1} + j_2^2} + \frac{2}{(2^m - 1)/3} \sum_{h=0}^{j_h} \binom{j_h}{s_+} \binom{j_h}{s_-} \binom{a_+}{s_+ + s_-} 2^{a_1 + a_2} 2^{a_2 - 2m - 4j_h},
\]

and

\[
N_i^{(4)} = N_i^{(3)}, \text{ for other } i.
\]

4.3 Binary Weight Enumerator for ERS\(_3\)

Let \(\bar{v} = ev[a_0 + a_1 x + a_2 x^2]\), and \(\bar{v}_j = ev[\delta_0 a_0 + \delta_1 a_1 x + \delta_2 a_2 x^2]\). If \(a_1 = a_2 = 0\), then

\[
|\bar{v}|_2 = |ev[a_0]|_2 = 2^m|a_0|_2.
\]

-16-
where \(|a_0|_2\) denotes the weight of the binary representation of \(a_0\) in \(GF(2^m)\). For \(0 \leq j \leq m,\)

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

\[
N^{(1)}_1 = 0, \quad \text{for other } i. \tag{75}
\]

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

\[
\text{Tr}(\delta_j a_0 + \delta_j a_1 X + \delta_j a_2 X^2)
\]

\[
= \text{Tr}(\delta_j a_0 + [\delta_j a_1 + (\delta_j a_2)^2]X) \cdot \tag{76}
\]

For each \(j\) with \(1 \leq j \leq m, \delta_j a_1 + (\delta_j a_2)^2 = 0\) 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 \(\text{Tr}(\delta_j a_0) = 0\) (or 1). If \(\delta_j a_1 + (\delta_j a_2)^2 = 0\) and \(\text{Tr}(\delta_j a_0) = 0\) (or 1), then

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

If \(\delta_j a_1 + (\delta_j a_2)^2 = 0\), then

\[
|v_j|_2 = \left| \text{ev}[\text{Tr}(\delta_j a_0 + [\delta_j a_1 + (\delta_j a_2)^2]X)] \right|_2 = 2^{m-1} \quad \tag{78}
\]

Therefore, we have that

\[
N^{(3)}_{(m+1)2^{m-1} - N^{(1)}_{(m+1)2^{m-1}} = m2^{m-1}(2^m-1)} \quad \tag{79}
\]

\[
N^{(3)}_{m2^{m-1} - N^{(1)}_{m2^{m-1}} = 2^m(2^{m-1})(2^{m+1}-m)} \quad \tag{80}
\]

\[
N^{(3)}_{(m-1)2^{m-1} - N^{(1)}_{(m-1)2^{m-1}} = m2^{m-1}(2^m-1)} \quad \tag{81}
\]

\[
N^{(3)}_1 = N^{(1)}_1, \quad \text{for other } i. \quad \tag{82}
\]

Note that the binary weight enumerator for \(ERS_3\) is independent of the
REFERENCES


