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 \((x-\alpha)(x-\alpha^2)(x-\alpha^3)\) (Unclas)

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 \(\{\beta_1, \beta_2, \ldots, \beta_m\}\) 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 \(\beta_1, \beta_2, \ldots, \beta_m\) 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 \((c_1, c_2, \ldots, c_m)\) 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 \(\{\beta_1, \beta_2, \ldots, \beta_m\}\) 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 \(\{\beta_1, \beta_2, \ldots, \beta_m\}\) 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 $R_{S_k}$ 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 $R_{S_k,e}$ 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 $ERS_{k}$ 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 $ERS_{n+1-k}$. 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 $RS_{n-1}$ with $1 \leq i \leq 2$, $RS_{n-1,e}$ with $2 \leq i \leq 3$ and $ERS_{n-1}$ with $1 \leq i \leq 2$ 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 $\text{GF}(2^m)$ 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 $\text{GF}(2^m)$. 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 $\text{GF}(2^m)$

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 $\{\beta_1, \beta_2, \cdots, \beta_m\}$ for $\text{GF}(2^m)$. Let $\{\delta_1, \delta_2, \cdots, \delta_m\}$ be the complementary (or dual) basis of $\{\beta_1, \beta_2, \cdots, \beta_m\}$, i.e.,

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

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

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 \( CD(b) \) denote the binary \((nm,(n-k)m)\) linear code obtained from \( CD \) 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:** \( CD(b) \) 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 \( CD \) respectively. Then

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

Let

\[
a_i = \sum_{j=1}^{m} a_{ij} \delta_j , \tag{2}
\]

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

It follows from (1) to (3) that

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

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

\[
\sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{h=1}^{m} a_{ij} b_{ih} \text{Tr}(\delta_j \delta_h) = 0 . \tag{5}
\]

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

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

Equation (6) implies that \( CD(b) \) is the dual code of \( C(b) \).

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

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

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

\[
\bar{\nu}_j = (\text{Tr}(\delta_j v_1), \text{Tr}(\delta_j v_2), \ldots, \text{Tr}(\delta_j v_n)), \quad (8)
\]

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

\[
|\bar{\nu}|_2 = \sum_{j=1}^m |\bar{\nu}_j|_2. \quad (9)
\]

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 \( \text{Cy}(s) \). Let \( m(s) \) denote the number of integers in \( \text{Cy}(s) \). For a subset \( I \) of \( \{0,1,2, \ldots, n-1\} \), \( \bar{I} \) denotes the set union of those cosets which have a nonempty intersection with \( I \), and \( \text{Rc}(I) \) denotes the set of the representatives of cyclotomic cosets in \( \bar{I} \).

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

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

and let \( \mathcal{C}_b(I) \) 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 \( a_i \in \text{GF}(2^m) \), let \( v[f(X)] \) and \( ev[f(X)] \) be defined by

\[
v[f(X)] = (f(1), f(\gamma), f(\gamma^2), \ldots, f(\gamma^{n-1})) \quad (10)
\]

and

\[
ev[f(X)] = (f(0), f(1), f(\gamma), \ldots, f(\gamma^{n-1})) \quad (11)
\]

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

$$P(1) = \{ \sum_{i \in I} a_i x^i \mid a_i \in \text{GF}(2^m) \text{ for } i \in I \}. \tag{12}$$

As is well-known\[5\],

$$C(I) = \{ v[f(x)] \mid f \in P(I) \}. \tag{13}$$

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

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

and

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

As is also known \[5\],

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

where

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

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

$$f(X) = \sum_{i \in \text{Rc}(I)} \sum_{q \in \text{Q}(i, I)} a_{i,q} x_{i,2^q} \tag{17}$$

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

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

\[ \text{Tr}(\delta_j f(X)) = \sum_{i \in \text{Ro}(I)} \text{Tr}_m(i)(b_j X^i) , \]  

(18)

where

\[ b_j = \text{Tr}_m(i) \left( \sum_{q \in Q(1,I)} \delta_j^{2^m(i)-q} a^q_{12^q} \right) , \quad i \in \text{Ro}(I) , \]  

(19)

where for a divisor \( h \) of \( m \)

\[ \text{Tr}(h)(X) = X + X^{2^h} + X^{2^{2h}} + \cdots + X^{2^{m-h}} . \]  

(20)

Note that

\[ b_j \in \text{GF}(2^m(1)) . \]  

(21)

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

\[ \tilde{v}_j = v[ \sum_{i \in \text{Ro}(I)} \text{Tr}_m(i)(b_j X^i) ] . \]  

(22)

For \( i \in \text{Ro}(I) \), let \( \tilde{C}_i \) be defined by

\[ \tilde{C}_i = \{ (b_1,b_2, \ldots, b_m) | b_j = \text{Tr}_m(i)(\sum_{q \in Q(1,I)} \delta_j^{2^m(i)-q} a^q_{12^q} ) , \]  

\[ 1 \leq j \leq m, a^q \in \text{GF}(2^m) \} . \]  

(23)

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

\[ D = \begin{bmatrix}
\delta_1 & \delta_1^2 & \delta_1^{2^2} & \cdots & \delta_1^{2^{m-1}} \\
\delta_2 & \delta_2^2 & \delta_2^{2^2} & \cdots & \delta_2^{2^{m-1}} \\
\delta_m & \delta_m^2 & \delta_m^{2^2} & \cdots & \delta_m^{2^{m-1}}
\end{bmatrix} \]  

(24)
If $\text{Tr}(m(i)) \left( \sum_{q \in Q(i, I)} a'_q \delta^m_{m(i)-q} \right) = 0$ for $1 \leq j \leq m$, then

$$a'_q = 0, \text{ for } q \in Q(i, I).$$  \hspace{1cm} (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 $i \in I$,

$$mw[C(i)(b)] \geq \min \{ mw[\tilde{C}_i] mw[C_b(I)], mw[C\{-i\}(b)] \},$$  \hspace{1cm} (26)

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

**Proof:** If follows from (19) and (25) that $b_j = 0$ 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 $\{\bar{v}_1, \bar{v}_2, \ldots, \bar{v}_m\}$ where $\bar{v}_j$ 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

$$Q(i, I) = \{ q | m-q \equiv h+j (\text{mod } m), 0 \leq q < m \text{ and } 0 \leq j < s \}.$$  \hspace{1cm} 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 $GF(2^m)$.

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

$$F(X) = \sum_{q \in Q(i, I)} c_q X^{2^m-q}.$$  \hspace{1cm} F(X) = \sum_{q \in Q(i, I)} c_q X^{2^m-q}.

Then,

$$F(X)^{2^m-h} = \sum_{j=0}^{s-1} c_{m-h-j} X^{2^j}, \quad \sum_{j=0}^{s-1} c_{m-h-j} X^{2^j}.$$
where the suffix of a coefficient is taken modulo \( m \). Since \( F(X)^{2^{m-1}} \) is a linearized polynomial of degree \( 2^{s-1} \) or less [5], the zeros of \( F(X) \) in \( \text{GF}(2^m) \) 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 \( c_j \) that \( \text{mw}[\tilde{c}_j] = m-s+1 \).

Since \( \#Q(1,I) = s, \tilde{c}_1 \) 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 \( C(I) \) is RS\(_4\), \( Q(3, I) = \{0\} \), and \( Q(1, I') = \{0, 1, 2\} \) where \( I' = I - \{3\} \). It is known [6, 7] that

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

and

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

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

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

for even \( m \) such that \( m/2 \) is even,

\[
\geq (m-2)(2^{m-1} - 2^{m/2}),
\]

for even \( m \) such that \( m/2 \) is odd.

\( \Delta \Delta \)

**4. Binary Weight Enumerator for ERSh**

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 $0 \le h < n-1$, $v[f(a^hX)]$ 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

$$\text{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 \text{ if and only if } a_3 \neq 0. \text{ The cyclic permutations on the second to the last symbols induce a permutation group on the codewords of } ERS_4, \text{ which divides } ERS_4-ERS_3 \text{ into disjoint sets of transitivity. Each set consists of } (2^m-1)/v \text{ 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

$$v = 1,$$  \hspace{1cm} (32)

and otherwise,

$$v = 3.$$  \hspace{1cm} (33)

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

$$\text{Tr}(\delta_j a_0+\delta_j a_1 X+\delta_j a_2 X^2+\delta_j a^h X^3)$$

$$= \text{Tr}(\delta_j a_0+[(\delta_j a_1+(\delta_j a_2)^{2^m-1}]X+\delta_j a^h X^3).$$  \hspace{1cm} (34)
On the weight of \( \text{ev}[\text{Tr}(b_0 + b_1 X + b_3 X^3)] \) where \( b_0, b_1 \) and \( b_3 \) are in \( \text{GF}(2^m) \),

the following theorem holds \([6,7]\).

**Theorem 3:**

1. For odd \( m \) and \( 0 \leq i < n \),

\[
\text{ev}[\text{Tr}(b_0 + a^i b_1 X + a^{3i} X^3)]_2 = 2^{m-1}, \quad \text{if } \text{Tr}(b_1) = 0 , \quad (35)
\]

\[
= 2^{m-1} \pm 2^{(m-1)/2} , \quad \text{if } \text{Tr}(b_1) = 1 . \quad (36)
\]

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

\[
\text{ev}[\text{Tr}(b_0 + a^i b_1 X + a^{3i} X^3)]_2 = 2^{m-1} \pm 2^{m/2} , \quad \text{if } \text{Tr}(2)(b_1) = 0 , \quad (37)
\]

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

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

\[
\text{ev}[\text{Tr}(b_0 + b_1 X + a^{3i} X^3)]_2 = 2^{m-1} \pm 2^{m/2-1} . \quad (39)
\]

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

\[
\text{ev}[\text{Tr}(b_0 + b_1 X + b_3 X^3)]_2 + \text{ev}[\text{Tr}(b_0' + b_1 X + b_3 X^3)]_2 = 2^m . \quad (40)
\]

For \( 0 \leq i \leq m2^m \), let \( N_1^{(k)} \) denote the number of codewords of weight \( i \) in \( \text{ERS}_k \). For deriving the weight enumerator for \( \text{ERS}_4 - \text{ERS}_3 \), there are two cases to be considered.
4.1 Case I: \( m \) is odd.

Suppose that \( m \) is odd. Then, \( v = 1 \). For \( 1 \leq j \leq m \), let \( \delta_j \) be represented as

\[
\delta_j = a^u_j.
\]  

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

\[
3u \equiv 1 \pmod{(2^m-1)}.
\]

Then

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

Let \( ev[a_0+a_1x+a_2x^2+x^3] \), 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

\[
\bar{v}_j = ev[\text{Tr}(\delta_ja_0+\delta_2a_1x+\delta_2a_2x^2+\delta_3x^3)] \quad \text{for} \quad 1 \leq j \leq m.
\]

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

\[
\text{Tr}(\delta_ja_0+\delta_2a_1x+\delta_2a_2x^2+\delta_3x^3)
\]

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

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 \( \text{Tr}(\alpha^{3u_j}a_1) = \text{Tr}(\alpha^{u_j}a_2) \), then

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

and otherwise,

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

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

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

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

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

Then we have that

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

Suppose that \( \{\delta_1^u, \delta_2^u, \ldots, \delta_m^u\} \) 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 \( \{\delta_1^u, \delta_2^u, \ldots, \delta_m^u\} \) is linearly independent. Since \( \delta_j = a_j^3 \) and \( \delta_j^u = a_j^{3u_j} \), \( \{a_1^{u_1}, a_2^{u_2}, \ldots, a_m^{u_m}\} \) is linearly independent for \( 1 \leq i \leq 3 \). Therefore, we have that

$$\{ (\text{Tr}(a_1^{u_1}a_2), \text{Tr}(a_1^{u_2}a_2), \ldots, \text{Tr}(a_1^{u_m}a_2)) \mid a_2 \in GF(2^m) \}$$

$$= \{ (\text{Tr}(a_1^{u_1}a_1), \text{Tr}(a_1^{u_2}a_1), \ldots, \text{Tr}(a_1^{u_m}a_1)) \mid a_1 \in GF(2^m) \}$$

$$= \{ (\text{Tr}(a_1^{u_1})a_1, \text{Tr}(a_1^{u_2})a_1, \ldots, \text{Tr}(a_1^{u_m})a_1)) \mid a_0 = GF(2^m) \}$$

= 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 \( \vec{v} \) such that \( S_+(\vec{v}) = s_+ \) and \( S_-(\vec{v}) = s_- \) is given by

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

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

$$N_4^{(4)}_{m2^{m-1} \pm j2^{(m-1)/2}} = N_4^{(3)}_{m2^{m-1} \pm j2^{(m-1)/2}}.$$
\[ = (2^{m-1}) \left( \frac{(m-j)/2}{i=0} \right)_{j=1}^{m-j-1} 2^{m-j-2}, \quad (49) \]

\[ N_1^{(4)} = N_1^{(3)}, \quad \text{for other } i, \quad (50) \]

where sign ± 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

\[ \delta_j = a^{3u_j+w_j}, \quad (51) \]

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 \( a^e \), 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

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

By (34), we have that

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

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
\[
\bar{v}_j = \text{ev}[\text{Tr}(\alpha^{3u_j} a_0 + \alpha^j [\alpha^{2u_j} a_1 + (\alpha^{2u_j} a_2)^{2^{m-2}}]x + a^{3u_j x^3})],
\]
for $h = 0$, \hspace{1cm} (55)
\[
\bar{v}_j = \text{ev}[\text{Tr}(\alpha^{3u_j+2} a_0 + \alpha^{j+1} [\alpha^{2u_j} a_1 + (\alpha^{2u_j} a_2)^{2^{m-2}}]x + a^{3(u_j+1) x^3})],
\]
for $h = 1$, \hspace{1cm} (56)
\[
\bar{v}_j = \text{ev}[\text{Tr}(\alpha^{3u_j+1} a_0 + \alpha^{j+1} [\alpha^{2u_j} a_1 + (\alpha^{2u_j} a_2)^{2^{m-2}}]x + a^{3(u_j+1) x^3})],
\]
for $h = 2$. \hspace{1cm} (57)

Since $\text{Tr}(2)(x^{2^{m-2}}) = \text{Tr}(2)(x)$ for even $m$ and $x$ in $\text{GF}(2^m)$, it follows from (2) of Theorem 3 and (55) to (57) that if either $j \in J_1$ and $\text{Tr}(2)(\alpha^{2u_j} a_2)$, or $j \in J_2$ and $\text{Tr}(2)(\alpha^{2u_j} a_1) = \text{Tr}(2)(\alpha^{2u_j} a_2)$, or $j \in J_2$ and $\text{Tr}(2)(\alpha^{2u_j} a_1) = \text{Tr}(2)(\alpha^{2u_j} a_2)$, then
\[
|\bar{v}_j|_2 = 2^{m-1} + 2^{m/2}, \hspace{1.5cm} (58)
\]
and otherwise,
\[
|\bar{v}_j|_2 = 2^{m-1}. \hspace{1.5cm} (59)
\]

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

For $0 \leq h \leq 2$, let \{ $u_j$ \mid $j \in J_h$ \} be represented by \{ $u_{h1}$, $u_{h2}$, ..., $u_{hj_h}$ \}, where $j_h = \#J_h$. Since \{ $\alpha^2$ \mid $\alpha \in \text{GF}(2^m)$ \} = \{ $\alpha^i$ $\mid$ $\alpha \in \text{GF}(2^m)$ \} = $\text{GF}(2^m)$ for an integer $i$, we have that
\[
\{(\text{Tr}(2)(\alpha^{2u_0} a_1), \text{Tr}(2)(\alpha^{2u_0} a_1), \ldots, \text{Tr}(2)(\alpha^{2u_0} a_1)) \mid a_1 \in \text{GF}(2^m)\}
\]
and
\[
\{(\text{Tr}(2)(\alpha^{2u_0} a_2), \text{Tr}(2)(\alpha^{2u_0} a_2), \ldots, \text{Tr}(2)(\alpha^{2u_0} a_2)) \mid a_2 \in \text{GF}(2^m)\}
\]
the set of all \(j_0\)-tuples over \(GF(2^2)\),

\[
\{(\text{Tr}(2)(a^{2u_1}a_1), \text{Tr}(2)(a^{2u_2}a_2), \ldots, \text{Tr}(2)(a^{2u_{j_0}}a_1)) | a_1 \in GF(2^m)\}
\]

the set of all \(j_1\)-tuples over \(GF(2^2)\),

\[
\{(\text{Tr}(2)(a^{2u_1}a_2), \text{Tr}(2)(a^{2u_2}a_2), \ldots, \text{Tr}(2)(a^{2u_{j_0}}a_2)) | a_2 \in GF(2^m)\}
\]

the set of all \(j_2\)-tuples over \(GF(2^2)\),

\[
\{(\text{Tr}(2)(a^{2u_1}a_2), \text{Tr}(2)(a^{2u_2}a_2), \ldots, \text{Tr}(2)(a^{2u_{j_0}}a_2)) | a_2 \in GF(2^m)\}
\]

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 \(\text{Tr}(2)(a^{2u_0}a_1) = b_j\) 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

\[
\{\text{Tr}(\delta_1a_0), \text{Tr}(\delta_2a_0), \ldots, \text{Tr}(\delta_ma_0) | a_0 \in GF(2^m)\}
\]

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

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

\[
S_+(\vec{v}) = \# \{ i | |\vec{v}_j|_2 = 2^{m-1} + 2^{m/2}, j \in J_h \},
\]

\[
S_-(\vec{v}) = \# \{ i | |\vec{v}_j|_2 = 2^{m-1} - 2^{m/2}, j \in J_h \},
\]

\[
T_+(\vec{v}) = \# \{ i | |\vec{v}_j|_2 = 2^{m-1} + 2^{m/2-1}, j \in Cj_h \}.
\]

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

\[
\# \{ i | |\vec{v}_j|_2 = 2^{m-1} - 2^{m/2-1}, 1 \leq j \leq m \} = m - J_h - T_+(\vec{v}),
\]
Then it follows from (13), (2) and (3) of Theorem 3 and (64) to (68) that

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

It follows from (4) of Theorem 3 and (54) to (63) that for given nonnegative integers \(s_+, s_-, t_+\) with \(0 \leq s_+ + s_- \leq j_h\) and \(0 \leq t_+ \leq m - j_h\), 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

\[ \binom{j_h}{s_+} \binom{j_h - s_+}{s_-} \binom{m - j_h}{t_+} 2^{(s_+ + s_-)} 24 \binom{j_h - s_+ + s_- + 2m - 4j_h}{m - j_h}. \]

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

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

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

\[ N^{(4)}_{m^2 m-1+j_{2m/2-1}} = \frac{N^{(3)}_{m^{2m-1}+j_{2m/2-1}}}{(2^m - 1)/3} \sum_{h=0}^{2m} \frac{j_h}{s_+} \binom{j_h - s_+}{s_-} \binom{m - j_h}{t_+} 2^{(s_+ + s_-)} 24 \binom{j_h - s_+ + s_- + 2m - 4j_h}{m - j_h}; \]

and

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

### 4.3 Binary Weight Enumerator for ERS_3

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

\[ |\bar{v}_j|_2 = |\text{ev}[a_0]|_2 = 2^m |a_0|_2. \]
where \(|a_0|_2\) denotes the weight of the binary representation of \(a_0\) in \(GF(2^m)\). For \(0 \leq j \leq m\),

\[
N_{j}^{(1)} = \binom{m}{j}, \quad \quad \quad (74)
\]

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

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

\[
\text{Tr} \left( \delta_j a_0 + \delta_j a_1 X + \delta_j a_2 X^2 \right) = \text{Tr} \left( \delta_j a_0 + (\delta_j a_1 + (\delta_j a_2)^{2^{m-1}}) X \right). \quad \quad \quad (76)
\]

For each \(j\) with \(1 \leq j \leq m\), \(\delta_j a_1 + (\delta_j a_2)^{2^{m-1}} = 0\) if and only if \(a_2 = a_1^{-1} \delta_j\).

There are \(m2^{m-1}(2^{m-1})\) combinations of \((a_0, a_1, a_2)\) such that \(a_2 = a_1^{-1} \delta_j\) and \(\text{Tr}(\delta_j a_0) = 0\) (or 1). If \(\delta_j a_1 + (\delta_j a_2)^{2^{m-1}} = 0\) and \(\text{Tr}(\delta_j a_0) = 0\) (or 1), then

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

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

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

Therefore, we have that

\[
N_{(m+1)2^{m-1}}^{(1)} - N_{m2^{m-1}}^{(1)} = 2^{m(2^{m-1})(2^{m+1}-m)}, \quad \quad \quad (79)
\]

\[
N_{m2^{m-1}}^{(3)} - N_{m2^{m-1}}^{(1)} = 2^{m(2^{m-1})(2^{m+1}-m)}, \quad \quad \quad (80)
\]

\[
N_{(m-1)2^{m-1}}^{(3)} - N_{(m-1)2^{m-1}}^{(1)} = 2^{m(2^{m-1})(2^{m+1}-m)}, \quad \quad \quad (81)
\]

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

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


