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 \((x-\alpha^2)(x-\alpha^3)\)
(Faward Univ., Honolulu.)

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 \((nm, mk)\) 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 \( GF(2^m) \), and let \( n = 2^m - 1 \). For \( 1 \leq k < n \), 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 \( RS_{n-1} \) with \( 1 \leq i \leq 2 \), \( RS_{n-2},e \) 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 \( GF(2^m) \) 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 \( GF(2^m) \). In section 4, the binary weight enumerator of \( ERS_n \) is derived for a class of bases including the complementary bases of primitive polynomial bases. By Theorem 1 the binary weight enumerator for \( ERS_{n-3} \) 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 \( \{\beta_1, \beta_2, \ldots, \beta_m\} \) for \( GF(2^m) \). Let \( \{\delta_1, \delta_2, \ldots, \delta_m\} \) be the complementary (or dual) basis of \( \{\beta_1, \beta_2, \ldots, \beta_m\} \), i.e.,

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

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

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 $\{\delta_1, \delta_2, \cdots, \delta_m\}$ of $\{\beta_1, \beta_2, \cdots, \beta_m\}$. Then we have Theorem 1.

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

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

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

Let

$$a_i = \sum_{j=1}^{m} a_{ij} \delta_j ,$$

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

(2)

(3)

It follows from (1) to (3) that

$$\sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} \delta_j \sum_{h=1}^{m} b_{ih} \delta_h = \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{h=1}^{m} a_{ij} b_{ih} \delta_j \delta_h = 0 .$$

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

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

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

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

(6)

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

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

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

(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 \( \{ \delta_1, \delta_2, \ldots, \delta_m \} \), then \( \tilde{v}_j \) is represented as

\[
\tilde{v}_j = (\text{Tr}(\delta_j v_1), \text{Tr}(\delta_j v_2), \ldots, \text{Tr}(\delta_j v_n)) \tag{8}
\]

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

\[
|\tilde{v}|_2 = \sum_{j=1}^{m} |\tilde{v}_j|_2 . \tag{9}
\]

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

Let \( \gamma \) be an element of order \( n \) in \( GF(2^m) \). For a subset \( I \) of \( \{0,1,2, \ldots,n-1\} \), let \( C(I) \) 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

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

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

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

and

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

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

\[
P(I) = \{ \sum_{i \in I} a_i x^i \mid a_i \in \text{GF}(2^m) \text{ for } i \in I \}.
\]

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 \( \bar{v} = v[f(x)] \in C(I) \), the \( \delta_j \) component vector of \( \bar{v} \), denoted \( \bar{v}_j \), is given by

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

and

\[
\bar{v}_j \in C_b(I).
\]

As is also known [5],

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

where

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

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

\[
f(X) = \sum_{i \in R(I)} \sum_{q \in Q(i,I)} a_{iq} x^{i2^q},
\]

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

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

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

(18)

where

\[
b_{j_1} = \text{Tr}(m(i)) \left( \sum_{q \in Q(1,I)} \delta_j^{2^m(i)-q} a_2 a_4 \right), i \in \text{Ro}(I),
\]

(19)

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

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

(20)

Note that

\[
b_{j_1} \in GF(2^{m(i)})
\]

(21)

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

\[
\bar{v}_j = \bar{v}[\sum_{i \in \text{Ro}(I)} \text{Tr}(m(i)) (b_j x^i)].
\]

(22)

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

\[
\bar{c}_i = \{ (b_1, b_2, \ldots, b_m) | b_j = \text{Tr}(m(i)) \left( \sum_{q \in Q(1,I)} \delta_j^{2^m(i)-q} a_q \right),
\]

\[
1 \leq j \leq m, a_q \in GF(2^m) \}
\]

(23)

Note that the following matrix \(D\) over \(GF(2^m)\) 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 \( \text{Tr}(m(i)) \left( \sum_{q \in Q(i, I)} \delta_{2^{m(i)}-q} a'_q \right) = 0 \) for \( 1 \leq j \leq m \), then
\[
a'_q = 0, \quad \text{for } q \in Q(i, I) .
\] (25)

Hence \( \tilde{C}_i \) is a linear \((m, \#Q(i, I) m/m(i))\) code over \( \mathbb{GF}(2^{m(i)}) \), 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 \( (b_{i1}, b_{i2}, \ldots, b_{im}) \) 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
\[
Q(i, I) = \{q|m-q \equiv h+j(mod \ m), \ 0 \leq q < m \text{ and } 0 \leq j < s\} .
\]
Then \( \tilde{C}_i \) is a maximum distance separable \((m,s)\) code over \( \mathbb{GF}(2^m) \).

Proof: Consider a polynomial \( F(X) \) over \( \mathbb{GF}(2^m) \) of the following form:
\[
F(X) = \sum_{q \in Q(i, I)} c_q X^{2^m-q}.
\]
Then,
\[
F(X)^{2^m-h} = \sum_{j=0}^{s-1} c_{m-h-j} X^{2^j}.
\]
where the suffix of a coefficient is taken modulo \( m \). Since \( F(X)^{2m-h} \) is a linearized polynomial of degree \( 2^{m-1} \) 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 \( \tilde{c}_j \) that \( mw[\tilde{c}_1] = m - s + 1 \).

Since \( \#Q(1, I) = s \), \( \tilde{c}_1 \) is a maximum distance separable \((m, s)\) code.

\[ \Delta \Delta \]

**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 \( \text{RS}_{4,4} \), \( Q(3, I) = \{0\} \), and \( Q(1, I') = \{0, 1, 2\} \) where \( I' = I - \{3\} \). It is known \([6, 7]\) that

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

\[
= 2^{m-1} - 2^{m/2-1}, \quad \text{for even } m \text{ such that } m/2 \text{ is even},
\]

\[
= 2^{m-1} - 2^{m/2}, \quad \text{for even } m \text{ such that } m/2 \text{ is odd},
\]

and

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

\[
= 2^{m-1} - 2^{m/2}, \quad \text{for even } m.
\]

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

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

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

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 \( \text{ERS}_4 \)**

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
\[ RS_k = \{ v(f(X)) \mid f(X) \in P(I_{0,k-1}) \} , \]  
(27)
\[ RS_{k,e} = \{ v(f(X)) \mid f(X) \in P(I_{1,k}) \} , \]  
(28)
and
\[ ERS_k = \{ ev(f(X)) \mid f(X) \in P(I_{0,k-1}) \} . \]  
(29)
For \( 0 \leq h < n-1 \), \( v'[a^hX] \) is the vector obtained from \( v'[X] \) by the \( h \) symbol cyclic shift, \( ev'[a^hX] \) is the vector obtained from \( ev'[X] \) by the \( h \) symbol cyclic shift among the second to the last symbols, and
\[ |v'[a^hX]|_2 = |v'[X]|_2 , \]  
(30)
\[ |ev'[a^hX]|_2 = |ev'[X]|_2 . \]  
(31)

For \( f(X) = a_0 + a_1X + a_2X^2 + a_3X^3 \in P(I_{0,3}) \), \( ev'[X] \in ERS_4-ERS_3 \) if and only if \( a_3 = 0 \). 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
\[ v = 1 , \]  
(32)
and otherwise,
\[ v = 3 . \]  
(33)
Let \( ev'[a_0+a_1X+a_2X^2+a^hX^3] \) for \( 0 \leq h < v \) represent each set of \( (2^m-1)/v \) codewords of \( ERS_4-ERS_3 \). Note that
\[ \text{Tr}(\delta_ja_0 + \delta_ja_1X + \delta_ja_2X^2 + \delta_ja^hX^3) \]
\[ = \text{Tr}(\delta_ja_0 + \delta_ja_1 + (\delta_ja_2)^{2^{m-1}})X + \delta_ja^hX^3) . \]  
(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 $0 \leq i < n$,

   \[ |\text{ev}[\text{Tr}(b_0 + a_1 b_1 X + a_3^i X^3)]|_2 \]
   \[ = 2^{m-1} , \text{ if } \text{Tr}(b_1) = 0 , \]  \hfill (35)
   \[ = 2^{m-1} \pm 2^{(m-1)/2} , \text{ if } \text{Tr}(b_1) = 1 . \]  \hfill (36)

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

   \[ |\text{ev}[\text{Tr}(b_0 + a_1 b_1 X + a_3^i X^3)]|_2 \]
   \[ = 2^{m-1} \pm 2^m/2 , \text{ if } \text{Tr}^{(2)}(b_1) = 0 , \]  \hfill (37)
   \[ = 2^{m-1} , \text{ if } \text{Tr}^{(2)}(b_1) = 0 . \]  \hfill (38)

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

   \[ |\text{ev}[\text{Tr}(b_0 + b_1 X + a_3^i h X^3)]|_2 \]
   \[ = 2^{m-1} \pm 2^m/2^{-1} . \]  \hfill (39)

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

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

\[ \Delta \Delta \]

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

\[
\delta_j = \alpha^u_j.
\] (41)

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

\[
3\mu \equiv 1 \mod (2^m - 1).
\] (42)

Then

\[
\delta_j = \alpha^{3\mu u_j}.
\] (43)

Let \( ev[a_0 + a_1 X + a_2 X^2 + X^3] \), denoted \( \bar{v} \), be a representative codeword in \( ERS_4 - ERS_3 \). Then the \( v_j \) component vector of \( \bar{v}, \bar{v}_j \), is defined by

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

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

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

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

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

Then we have that
\[ |v|_2 = m2^{m-1} + (S_+(\bar{v}) - S_-(\bar{v}))2^{(m-1)/2} \quad \text{(47)} \]

Suppose that \{\delta_1, \delta_2, \ldots, \delta_m\} is linearly independent. It follows from (42) that \(\delta\) is relatively prime to \(2^m-1\). If \{\delta_1, \delta_2, \ldots, \delta_m\} is a polynomial basis, then \{\delta_1, \delta_2, \ldots, \delta_m\} is linearly independent. Since \(\delta_j = \alpha^{3u_j}\) and \(\delta_i = \alpha^{u_j}\), \{\alpha^{u_1}, \alpha^{u_2}, \ldots, \alpha^{u_m}\} is linearly independent for \(1 \leq i \leq 3\). Therefore, we have that
\[ \{ (\text{Tr}(\alpha^{u_1}a_2), \text{Tr}(\alpha^{u_2}a_2), \ldots, \text{Tr}(\alpha^{u_m}a_2)) \mid a_2 \in GF(2^m) \} \]
\[ = \{ (\text{Tr}(\alpha^{u_1}a_1), \text{Tr}(\alpha^{u_2}a_1), \ldots, \text{Tr}(\alpha^{u_m}a_1)) \mid a_1 \in GF(2^m) \} \]
\[ = \{ (\text{Tr}(\alpha^{u_1}a_0), \text{Tr}(\alpha^{u_2}a_0), \ldots, \text{Tr}(\alpha^{u_m}a_0)) \mid a_0 \in GF(2^m) \} \]
\[ = \text{the set of all binary } m\text{-tuples.} \quad \text{(48)} \]

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

Since there are \(2^m-1\) choices of \(a_3\) of nonzero \(a_3\), it follows from (47) and (48) that for \(0 \leq j \leq m\),
\[ \binom{m}{s_+}(s_+)^{s_++s_-} \cdot m^{s_+} \cdot 2^{s_-} = \binom{m}{s_+}(s_+)^{s_++s_-} \cdot m^{s_+} \cdot 2^{s_-}. \]
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

\[
\delta_j = \alpha^{3u_j + w_j},
\]

where \( 0 \leq u_j < \frac{(2^m - 1)}{3} \) 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

\[
e \equiv h \pmod{3}, \ 0 \leq h \leq 2.
\]

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

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

By (34), we have that

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

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

\[
J_h = \{ \ j \ | \ w_j + h \equiv 0 \ (\text{mod} \ 3), \ 1 \leq j \leq m \},
\]

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 \( j \in CJ_h \),

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

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

for $h = 0$, (55)

$$= \text{ev}[\text{Tr}(a^3 u_j^{h+2} + u_j^{h+1} [a^2 u_j^{h+1} a_1 + (a^2 u_j^{h+1} a_2)^2x^2]x + a^3(u_j^{h+1}) x^3)],$$

for $h = 1$, (56)

$$= \text{ev}[\text{Tr}(a^3 u_j^{h+1} + u_j^{h+1} [a^2 u_j^{h+1} a_1 + (a^2 u_j^{h+1} a_2)^2x^2]x + a^3(u_j^{h+1}) x^3)],$$

for $h = 2$. (57)

Since $\text{Tr}(2)(x^{2m-2}) = \text{Tr}(2)(x)$ 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 $\text{Tr}(2)(2u_j a_1) = \text{Tr}(2)(2u_j a_2)$, or $j \in J_1$ and $\text{Tr}(2)(2u_j a_1) = \text{Tr}(2)(2u_j a_2)$, or $j \in J_2$ and $\text{Tr}(2)(2u_j a_1) = \text{Tr}(2)(2u_j a_2)$, then

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

and otherwise,

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

Suppose that for $0 \leq h \leq 2$, $\{a^{2u_j} \mid j \in J_h\}$ is linearly independent over $GF(2^2)$. 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 $\{u_{h1}, u_{h2}, \ldots, u_{hh}\}$, where $j_h = \#J_h$. Since $\{a^2 \mid a \in GF(2^m)\} = \{a^i a \mid a \in GF(2^m)\} = GF(2^m)$ for an integer $i$, we have that

$$\{\text{Tr}(2)(a^{2u_{h1}} a_1), \text{Tr}(2)(a^{2u_{h2}} a_1), \ldots, \text{Tr}(2)(a^{2u_{hh}} a_1) \mid a_1 \in GF(2^m)\}$$

$$= \{\text{Tr}(2)(a^{2u_{h1}} a_2), \text{Tr}(2)(a^{2u_{h2}} a_2), \ldots, \text{Tr}(2)(a^{2u_{hh}} a_2) \mid a_2 \in GF(2^m)\}$$
the set of all $j_0$-tuples over $GF(2^2)$,  

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

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

\[(\{\text{Tr}(2)(\alpha^{2u_1}a_1), \text{Tr}(2)(\alpha^{2u_2}a_2), \ldots, \text{Tr}(2)(\alpha^{2u_{j_1}}a_{j_1})\} | a_2 \in GF(2^m)\} = \]

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

\[(\{\text{Tr}(2)(\alpha^{2u_2}a_1), \text{Tr}(2)(\alpha^{2u_2}a_2), \ldots, \text{Tr}(2)(\alpha^{2u_{j_2}}a_{j_2})\} | a_2 \in GF(2^m)\} = \]

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

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

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

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

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

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

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

$$D_{h,j} = \{ (s_+, s_-, t_+) : 0 \leq s_+ \leq j_h, 0 \leq s_- \leq j_h, 0 \leq s_+ + s_- \leq j_h, 0 \leq t_+ \leq m - j_h, 2(s_+ + s_- + t_+) = m + j - j_h \}.$$  \hfill (71)

Since there are $(2^{m-1})/3$ choices of nonzero $a_0$ satisfying (52), it follows from (69), (70) and (71) that for $-2m \leq j \leq 2m$,

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

and

$$N^{(4)}_i = N^{(3)}_i, \text{ for other } i.$$  \hfill (72)

### 4.3 Binary Weight Enumerator for ERS$_3$

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

$$|\bar{v}_j|_2 = |ev[a_0]|_2 = 2^m |a_0|_2,$$  \hfill (73)
where $|a_0|_2$ denotes the weight of the binary representation of $a_0$ in $GF(2^m)$. For $0 \leq j \leq m$,

$$N^{(1)}_{j} = \binom{m}{j}, \quad \text{for other } i.$$  \hspace{1cm} (74)  

$$N^{(1)}_{j} = 0, \quad \text{for other } i.$$  \hspace{1cm} (75)

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

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

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

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

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

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

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

Therefore, we have that

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

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

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

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

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

REFERENCES


