Structural Analysis of Minimum Weight Codewords of the (32, 21, 6) and (64, 45, 8) Extended BCH Codes Using Invariance Property

Jun ASATANI
Faculty of Engineering
Okayama University of Science
1-1 Ridaicho, Okayama Japan

Takuya KOUMOTO
Graduate School of Natural Science and Technology, Okayama University
3-1-1, Tsushimanaka Okayama Japan

Toru FUJIWARA
Graduate School of Information Science and Technology, Osaka University
1-5 Yamadaoka, Suita, Osaka Japan

Tadao KASAMI
Graduate School of Information Science and Technology, Nara Institute of Science and Technology
8916-5 Takayamacho, Ikoma, Nara Japan

(Received November 20, 2007)

Two typical examples, the (32, 21, 6) and (64, 45, 8) extended code of primitive permuted BCH codes, are considered. The sets of minimum weight codewords are analyzed in terms of Boolean polynomial representation. They are classified by using their split weight structure with respect to the left and right half trellis sections, and for each class, the standard form is presented. Based on the results, we can generate a proper list of the minimum weight codewords of the codes.

**keywords:** Boolean polynomial representation, extended BCH codes, minimum weight codewords, binary shift invariance property

1 Introduction

Contrast with Reed-Muller (RM) codes, the structure of the set of minimum weight codewords of extended codes of primitive permuted BCH (EBCH) codes of length $2^m$ for which the nesting relation with RM codes of the same length holds are not known in general. The fact is that its structure is not very simple. We briefly review the difference of structural complexity between RM codes and EBCH codes. The latter have smaller invariant permutation groups than the former. Consider a minimum weight codeword $v$ in a proper bit order. For RM codes, either the left half subword of $v$ is equal to the other or one of the half subwords of $v$ is 0. In contrast, for EBCH codes, the left half subword of $v$ is not equal to the other in most cases.

A stimulus to the present study was given by a letter (private communication) to the following effect from Dr. P. Martin of Univ. of Canterbury, Christchurch, New Zealand just after ISIT’04: She was definitely interested in hearing about our progress on future research using the techniques [1] for BCH codes. From a preliminary study, we conclude that before designing a new decoding scheme whose complexity justify the gain, we need to make a thorough analysis of the set of minimum weight codewords of typical examples of EBCH codes with moderate parameters.

In this paper, two typical examples, the (32, 21, 6) and (64, 45, 8) EBCH codes, are considered. Based on the previous works [2, 3], the sets of minimum weight codewords are analyzed in terms of Boolean polynomial representation. They are classified by using their split weight structure with respect to the left and right half trellis sections, and for each class, the standard form is
Presented. Based on the results, we can generate a proper list of the minimum weight codewords of the EBCH codes.

2 Preliminaries

2.1 Notations

For a positive integer \( m \), let \( V_m \) denote the vector space of all binary \( 2^m \)-tuples and let \( C \) be a binary linear block code of length \( 2^m \). We divide the top section of the code into two sub-sections of length \( 2^{m-1} \). For \( u = (u_1, u_2, \ldots, u_{2^m}) \in V_m \), define \( p_0 u = (u_1, u_2, \ldots, u_{2^m-1}) \) and \( p_1 u = (u_{2^m-1+1}, u_{2^m-1+2}, \ldots, u_{2^m}) \). Define \( p_0 C \triangleq \{p_0 u : u \in C\} \) and \( p_1 C \triangleq \{p_1 u : u \in C\} \). Let \( C_0 \) and \( C_1 \) denote the subcodes of \( C \) which consist of those codewords in \( C \) whose nonzero components are confined to the spans of \( 2^{m-1} \) consecutive positions in the sets \( \{1, 2, \ldots, 2^{m-1}\} \) and \( \{2^{m-1}+1, 2^{m-1}+2, \ldots, 2^m\} \). Clearly, every codeword in \( C_0 \) and \( C_1 \) are of the form, \((u_1, u_2, \ldots, u_{2^m-1}, 0, 0, \ldots, 0) \) and \((0, 0, \ldots, 0, u_{2^m-1+1}, u_{2^m-1+2}, \ldots, u_{2^m}) \). For the subcodes \( C_0 \) and \( C_1 \), denote \( s_0 C \triangleq p_0 C_0 \) and \( s_1 C \triangleq p_1 C_1 \).

Let \( C = C_1 \cup C_2 \) be a linear subcode of \( C \) whose nonzero components are confined to the spans of \( 2^{m-1} \) consecutive positions in the sets \( \{1, 2, \ldots, 2^{m-1}\} \) and \( \{2^{m-1}+1, 2^{m-1}+2, \ldots, 2^m\} \). Clearly, every codeword in \( C_0 \) and \( C_1 \) are of the form, \((u_1, u_2, \ldots, u_{2^m-1}, 0, 0, \ldots, 0) \) and \((0, 0, \ldots, 0, u_{2^m-1+1}, u_{2^m-1+2}, \ldots, u_{2^m}) \). For the subcodes \( C_0 \) and \( C_1 \), denote \( s_0 C \triangleq p_0 C_0 \) and \( s_1 C \triangleq p_1 C_1 \).

Let \( C' \) be a linear subcode of \( C \). Define

\[
T \triangleq C/C',
\]

as the set of all cosets of \( C' \) in \( C \). Abbreviate \( C/(s_0 C \circ s_1 C) \) as \( PT \). Then, there is a one-to-one correspondence between the cosets in \( PT \) and the middle states of the 2-section trellis diagram [4]. We will analyze the structure of minimum weight codeword with respect to \( PT \).

For \( u \in V_m \), define \( w(u) \) as the weight of \( u \), and define \( w_0(u) \triangleq w(p_0 u) \) and \( w_1(u) \triangleq w(p_1 u) \). For \( U \subseteq C \), let \( wp(U) \), \( wp_0(U) \) and \( wp_1(U) \) denote the weight profile of \( U \), \( p_0 U \) and \( p_1 U \), respectively. For \( w \in wp(U) \), define

\[
U(w) \triangleq \{u \in U : w(u) = w\}.
\]

For \( u \in V_m \), define \( u_{\mid 1} \) as the split weight of \( u \), \( \{(w_0(u), w_1(u))\} \). Let \( \{u_{\mid 1}\} \) with \( U \subseteq C \) denote the split weight profile of \( U \). For \( (w_0, w_1) \in \{u_{\mid 1}\} \),

\[
U(w_0, w_1) \triangleq \{u \in U : w_0(u) = w_0, w_1(u) = w_1\}.
\]

For \( T = C/C' \), for example \( C' = s_0 C \circ s_1 C \), define \( g \cdot T \triangleq D \in T \) such that \( g \in D \). For \( w \in wp(C) \) (or \( (w_0, w_1) \subseteq \{u_{\mid 1}\} \)), define

\[
T(w) \triangleq \{D(w) : D \in T\},
\]

or \( T(w_0, w_1) \triangleq \{D(w_0, w_1) : D \in T\} \),

and for \( D \in T \), nonempty \( D(w_0) \) (or \( D(w_0, w_1) \)) is called a block (with weight \( w_0 \) or split weight \( (w_0, w_1) \)) of \( D \). Abbreviate \( pwD \) as \( Dh \) for \( b \in \{0, 1\} \).

Let \( d \) be the minimum distance of the linear code \( C \). For \( w_b \in wp_b(C) \) with \( b \in \{0, 1\} \), if there are \( u \) and \( u' \) in \( Dh(w_b) \), \( w_b \geq d/2 \), since \( \|w_b(u + u')\| \geq d \). From this, the following relation holds [3] for \( D \in T \) and \( (w_0, w_1) \in swp_{\mid 1}(D) \) with \( w_0 + w_1 = d \).

\[
\begin{array}{ll}
(i) & \text{If } 0 \leq w_b < d/2, \text{ then } |Dh(w_b)| = 1. \\
(ii) & \text{If } |Dh(w_b)| \geq 2 \text{ for } b = 0 \text{ and } 1, \text{ then } w_b = d/2.
\end{array}
\]

2.2 Review of Boolean Polynomial Representation for Linear Block Codes [2]

For a positive integer \( m \) and a nonnegative integer \( r \) not greater than \( m \), let \( P_m^r \) denote the set of all Boolean polynomials of degree \( r \) or less with \( m \) variables \( x_1, x_2, \ldots, x_m \). A polynomial in \( P_m^r \) is called an affine polynomial. A set of \( l \) affine polynomials \( \{a_i + \sum_{j=1}^l a_{ij} x_j : a_{ij} \in \{0, 1\} \} \) with \( 1 \leq i \leq l \) and \( 1 \leq j \leq m \) such that the rank of coefficient matrix \( (a_{ij} : 1 \leq i \leq l, 1 \leq j \leq m) \) is \( l \) is called linearly independent. Hereafter, \( \{y_1, \ldots, y_l\} \) and \( \{z_1, \ldots, z_l\} \) denote linearly independent affine polynomials, respectively. For a nonnegative integer \( i \) less than \( 2^m \), let \( (b_1, b_2, \ldots, b_m) \) be the standard binary expression of \( i \) such that \( i = \sum_{j=1}^m b_j 2^{m-j} \). For \( f(x_1, x_2, \ldots, x_m) \in P_m^m \), define the following binary \( m \)-tuple:

\[
b(f) \triangleq (v_1, v_2, \ldots, v_m),
\]

where the \((i + 1)\)th component (or bit) is given by

\[
v_{i+1} \triangleq f(b_1, b_2, \ldots, b_m), \quad 0 \leq i < 2^m.
\]

We say that the \( 2^m \)-tuple \( b(f) \) is in standard bit-order. A binary linear code of length \( 2^m \) can be expressed in terms of Boolean polynomials of \( m \) variables. For example, the \( r \)th order RM code of length \( 2^m \) [5, 6], denoted \( RM_{m,r} \), is defined as \( \{b(f) : f \in P_m^r \} \) [5]. In the following sections, \( f \in P_m^m \) and \( b(f) \in V_m \) are used interchangeably for simplicity.

Let \( a = (a_1, a_2, \ldots, a_m) \) and \( b = (b_1, b_2, \ldots, b_m) \) be two binary \( m \)-tuples. Define the following boolean product of \( a \) and \( b \),

\[
a \cdot b \triangleq (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_m \cdot b_m),
\]

where \( \cdot \) denotes the logic product, i.e. \( a_1 \cdot b_1 = 1 \) if and only if both \( a_1 \) and \( b_1 \) are \( 1 \). For simplicity, we use \( ab \) for \( a \cdot b \). For \( f_a, f_b \in V_m \), \( f_a f_b \) denotes the boolean product of \( b(f_a) \) and \( b(f_b) \).

For a Boolean polynomial \( f \in P_m^m \), let \( f \mid m \) denote the weight of \( b(f) \), that is, \( w(b(f)) = f \mid m \). For \( f_0 \) and \( f_1 \) in \( P_m^m \),

\[
f_0 + f_1 \mid m = f_0 \mid m + f_1 \mid m - 2f_0 f_1 \mid m.
\]
The polynomial \( f \in P^r_m \) (with \( r < m \)) can be expressed as
\[
 f = f_0 + x_m f_1, \quad \text{for} \ f_0 \in P^r_{m-1}, f_1 \in P^{r-1}_{m-1}.
\] (8)

Then,
\[
p_0 f = f_0, \quad \text{and} \quad p_1 f = f_0 + f_1.
\] (9)

From (7), (8) and (9), we have that
\[
w_0(f) = |f|_{0,m-1}, \quad w_1(f) = |f|_{0,m-1} + |f|_{1,m-1} - 2|f_0 f_1|_{m-1}.
\] (10) (11)

### 2.3 Invariance Properties under Binary Shifts for Extended BCH Codes

Given linearly independent affine polynomials \( y_i = \sum_{j=1}^{m} a_{ij} x_j + b_i \) with \( 1 \leq i \leq m \), the replacement of \( x_j \) by affine polynomial \( y_i \) is called the affine transformation. An affine transformation \( y_i = x_i + b_i \) with \( 1 \leq i \leq m \) is called a binary shift. Since an affine transformation is invertible, binary shifts of \( y_i \) with \( 1 \leq i \leq m \) correspond to binary shifts of \( x_j \) uniquely. If \( u \in V_m \) can be transformed to \( v \) by binary shift \( B \), then \( u \) and \( v \) are said to be binary shift equivalent and we write \( v = B(u) \).

RM codes are invariant under the affine transformations and the EBCH codes of length \( 2^m \) are invariant under the binary shifts [7]. If \( C \) is invariant under permutations, \( C(w) \) with \( w \in \text{wp}(C) \) is also invariant under the permutations.

The following nesting relation holds [5]:

The EBCH code of length \( 2^m \) with minimum weight \( 2^{m-r} \supseteq \text{RM}_{m,r} \).

\[
 2^m - r \supseteq \text{RM}_{m,r}.
\] (12)

For a Boolean variable \( x \), we use the notations, \( \bar{x} \triangleq x+1 \) and for \( a \in \{0, 1\} \),
\[
x^a = \begin{cases} \bar{x}, & \text{if } a = 0, \\ x, & \text{if } a = 1. \end{cases}
\]

For \( \{i_1, i_2, \ldots, i_s\} \subseteq \{1, 2, \ldots, m\} \), let \( B_{i_1,i_2,\ldots,i_s} \) be the binary shift such that
\[
x_i \left\{ \begin{array}{ll} \bar{x}_i, & \text{if } i \text{ is in the suces}, \\ x_i, & \text{otherwise}. \end{array} \right.
\] (13)

For \( \{a_1, a_2, \ldots, a_m\} \in \{0, 1, \ast\} \), let \( B_{a_1,a_2,\ldots,a_m} \) be the set of binary shifts such that
\[
x_i \left\{ \begin{array}{ll} x_{a_i}, & \text{if } a_i \in \{0, 1\}, \\ x_i, & \text{or } \bar{x}_i, \text{if } a_i = \ast. \end{array} \right.
\] (14)

For \( B_{a_1,a_2,\ldots,a_m} \), if the number of \( \ast \) in its suces is \( s \), it contains \( 2^s \) binary shifts. If a binary linear code \( C \) of length \( 2^m \) is invariant under \( B_m \), then the following symmetry holds:
\[
p_0 C = p_1 C, \quad \text{and} \quad s_0 C = s_1 C.
\] (15)

Hereafter in this section, let \( i \) be a positive integer less than or equal to \( m \), \( b \in \{0, 1\} \), and \( f \in P^i_m \). \( B_i^{(b)} \) denotes the binary shift of \( x_i \) in right and left half subsections defined by
\[
 B_i^{(b)}(f) = \begin{cases} B_i(p_0 f) \circ p_1 f, & \text{if } b = 0, \\ p_0 f \circ B_i(p_1 f), & \text{if } b = 1. \end{cases}
\] (16)

Define \( \text{deg}_i(f) \) as the degree of \( (f + f_{x_i=0})/x_i \). We have the following lemma:

**Lemma 1:** Let \( C \) be a binary linear code of length \( 2^m \) such that
\[
 \text{RM}_{m,r} \subseteq C \subseteq \text{RM}_{m,r+1}, \quad \text{for } r < m.
\] (17)

(i) For \( f \in D \in C/\text{RM}_{m,r} \), any codeword that is binary shift equivalent to \( f \) is in \( D \).

(ii) For \( f \in D \in \text{PT} \triangleq \{C/(s_0 C \circ s_1 C)\} \), if \( \text{deg}_i(f) < r \), then \( B_i^{(b)}(f) \in D \). If \( \text{deg}_i(f) < r \), then \( B_i(f) \in D \).

(Proof) (i) \( f + B(f) \in \text{RM}_{m,r} \) implies \( B(f) \in D \).

(ii) \( p_0(f + B_i^{(b)}(f)) = p_0 f + B_i(p_0 f) \in \text{RM}_{m,r+1} \), and \( p_0(f + B_i^{(b)}(f)) = 0 \). Since \( s_0 C \supseteq s_0 \text{RM}_{m,r} = \text{RM}_{m-1,r-1} \), \( f + B_i^{(b)}(f) \in s_0 C \circ s_1 C \) implies \( B_i^{(b)}(f) \in D \). The last half is proved similarly.

### 3 Structure Analysis of Minimum Weight Codewords of The (32, 21, 6) and (64, 45, 8) Extended BCH Codes

An \((n, k, d)\) EBCH code is denoted by \( \text{EBCH}(n, k, d) \). In this section, for two typical examples, \( \text{EBCH}(32, 21, 6) \) and \( \text{EBCH}(64, 45, 8) \), the structure of minimum weight codewords is analyzed. For these codes, Lemma 1 and (15) hold.

#### 3.1 EBCH(32, 21, 6)

##### 3.1.1 Structure of the code

In this section, let \( C \) denote \( \text{EBCH}(32, 21, 6) \). From (12),
\[
 \text{RM}_{5,2} \subseteq C \subseteq \text{RM}_{5,3},
\] (18)

where \( \text{RM}_{5,3} \) is the extended Hamming code. Define
\[
 \Gamma_{\text{RM}} \triangleq C/\text{RM}_{5,2}.
\] (19)

Then, \( \dim(\Gamma_{\text{RM}}) = 5 \).

By a generator matrix of \( C \) with a generator matrix of \( \text{RM}_{5,2} \) as a submatrix, we found the following set of
generators which spans a set of coset leaders of \( \Gamma_{RM} \):

\[
\begin{align*}
  g_1 &= (x_1 + x_2) x_3 x_4 + (x_2 x_3 + (x_1 + x_3) x_4) x_5, \\
  g_2 &= (x_1 + x_3) x_2 (x_3 + x_4) + [(x_1 + x_3) x_2 + (x_2 + x_3) x_4] x_5, \\
  g_3 &= (x_1 + x_2) (x_2 + x_3) (x_3 + x_4) + (x_1 x_3 + x_2 x_4) x_5, \\
  g_4 &= x_1 (x_2 + x_4) x_3 + (x_1 + x_2) (x_3 + x_4) x_5, \\
  g_5 &= [(x_1 + x_3) x_2 + (x_1 + x_2) x_4] x_5.
\end{align*}
\]

Now, we consider \( p_0 C \) and \( s_0 C \). Since \( p_0 R M_{5,2} = \text{RM}_{4,2} \) and \( p_0 g_0 \in \text{RM}_{4,2} \),

\[
p_0 C = \left\{ \sum_{i=1}^{4} a_i p_0 g_i : a_i \in \{0, 1\} \right\}
\quad \text{with } 1 \leq i \leq 4 \quad \text{and } \text{RM}_{4,2}.
\]  

It can be shown readily that \( p_0 g_0 \) with \( 1 \leq i \leq 4 \) are linearly independent and therefore,

\[
p_0 g_0 \text{ with } 1 \leq i \leq 4 \text{ spans } \text{RM}_{4,3} \setminus \text{RM}_{4,2}.
\]

Hence, by (15),

\[
p_0 C = \text{RM}_{4,3}, \quad \text{and } \dim(p_0 C) = 15.
\]

Since \( s_0 R M_{5,2} = \text{RM}_{4,1} \), by (15) and (22),

\[
s_0 C = \{0, g_5, x_5 = 1\} + \text{RM}_{4,1},
\]

where \( g_5 x_5 = 1 \triangleq (x_1 + x_3) x_2 + (x_1 + x_2) x_4 \in \text{RM}_{4,2} \). Define

\[
\text{RM}'_{5,2} \triangleq \{0, g_5\} + \text{RM}_{5,2}.
\]

Then, \( C \supset \text{RM}'_{5,2} \) and \( \dim(\text{RM}'_{5,2}) = 17 \). Define

\[
\Gamma_{RM} \triangleq C / \text{RM}'_{5,2}
\]

Then, \( \dim(\Gamma_{RM}) = 4 \). Since \( \text{RM}_{4,1} \cap \text{RM}_{4,1} \subseteq \text{RM}_{5,2} \), from (24), \( \dim(s_0 C) = 6 \) and \( s_0 C \cap s_1 C \subseteq \text{RM}'_{5,2} \). Then,

\[
\dim(\text{RM}'_{5,2} / (s_0 C \cap s_1 C)) = 5.
\]

For \( \mathcal{PT} \triangleq C / (s_0 C \cap s_1 C) \), \( \dim(\mathcal{PT}) = 9 \). From (27), each coset of \( \Gamma_{RM} \) consists of \( 2^5 \) cosets of \( \mathcal{PT} \). A computer analysis of \( \mathcal{PT}(6) \) based on the method presented in [3] results in Table 1, where for blocks \( D_0(w_0) \cap D_1(w_1) \in \mathcal{PT}(w_0, w_1) \) with \( (w_0, w_1) \in \text{swp}_{b_1}(C(6)) \), \( |D_0(w_0)| \) with \( b \in \{0, 1\} \) and \( |\mathcal{PT}(w_0, w_1)| \) for \( w_0 \leq w_1 \) are shown for \( w_0 \leq w_1 \).

By (15), it is sufficient to consider \( C(0, 6) \) and \( C(2, 4) \) in the following sections 3.1.2 and 3.1.3.

### 3.1.2 Structure of \( C(0, 6) \)

Let \( v \in C(0, 6) \). Then \( p_0 b \in p_0 C = \text{RM}_{4,3} \) with \( b \in \{0, 1\} \) from (23). Therefore, the Boolean polynomial corresponding to \( v \) is \( (y_1 y_2 + y_3 y_4) x_5 \). Note that \( g_5 \) is of the form. Consider the binary shifts of \( g_5 \) with respect to \( x_1 + x_3, x_2, x_1 + x_2 \) and \( x_4 \), equivalently \( x_3, x_2, x_1, \) and \( x_4 \). For \( B \in \text{B}_{6,1} \), \( B(g_5) = g_5 + \text{RM}_{5,2} \subseteq C \), \( w_1(B(g_5)) = 6 \), and \( |\{B(g_5) : B \in \text{B}_{6,1}\}| = 16 \). Then, we have from Table 1 that

\[
C(0, 6) = \{B(g_5) : B \in \text{B}_{6,1}\}.
\]  

### 3.1.3 Structure of \( C(2, 4) \)

Since \( p_0 C(2, 4) \subseteq p_0 C = \text{RM}_{4,3} \), \( p_0 C(2, 4) \subseteq \text{RM}_{4,3}(2) \). The number of the minimum weight codewords in \( \text{RM}_{4,3} \) is \( 2^{3(2^5 - 1)} = 120 \). From Table 1,

\[
p_0 C(2, 4) = \text{RM}_{4,3}(2)
\]

Each polynomial of \( \text{RM}_{4,3}(2) \) is a form of the product of three linearly independent affine polynomials. By the binary shifts of three component polynomials, the 120 codewords of \( \text{RM}_{4,3}(2) \) can be partitioned into 15 groups. Each group consists of 8 codewords in the same coset of \( \Gamma_{RM} \) from Lemma 1. Table 2 lists the 15 representative codewords in its first column as \( f_0 \).

For \( f_0 \in \text{RM}_{4,3}(2) \), \( f \in C(2, 4) \) with \( p_0 f = f_0 \) can be expressed as

\[
f = f_0 + x_5 f_1,
\]

where \( p_1 f = f_0 + f_1 \in \text{RM}_{4,3}(4) \). \( f_1 \) is called the right part of \( f_0 \) or \( f \). There are exactly four right parts of \( f_0 \) which belong to \( s_1 C = \{0, g_5\} + \text{RM}_{4,1} \). For each of the representative codewords \( f_0 \), two of the four right parts of \( f_0 \) are also listed in the table. Note that the sum of the two \( f_1 \)'s in each block is \( g_5 \) mod \( \text{RM}_{4,1} \). The remaining two right parts can be obtained from the two \( f_1 \) by applying the binary shift \( B \) in the table. Note that \( B(f_0) = f_0 \).

From (11) and (30), \( w_1(f) = |f_0 + f_1| = |

f_0| + |f_1| - 2 |f_0 f_1| = 4 \), \( |f_1| - 2 |f_0 f_1| = 2 \), \( f_1 \in P_2^f \) and \( f_1 \neq 0 \). \( |f_1| \) is even with \( |f_1| \geq 4 \). Since \( |f_0| = 2 \), \( |f_0 f_1| \leq |f_0| = 2 \). Hence, \( |f_1| = 4 \) or 6. There are two cases for \( f_1 \).

Case I: \( |f_1| = 4 \) and \( |f_0 f_1| = 4 \).

Case II: \( |f_1| = 6 \) and \( |f_0 f_1| = 2 \).

Since \( f_0 \in \text{RM}_{4,3}(2) \), we can express \( f_0 = y_1 y_2 y_3 \). We show standard forms for Cases I and II.

Case I: \( f_1 \) is expressed as \( z_1 z_2 \). At least one of \( z_1 \) and \( z_2 \), say \( z_1 \) is linearly dependent on \( y_1, y_2, y_3 \) and \( z_2 \). If \( z_2 \) is also linearly dependent, then there exists an affine polynomial linearly independent of \( y_1, y_2, y_3 \); which implies \( y_1 y_2 y_3 z_2 = 0 \) or 2. Hence, \( z_2 \) is linearly independent of \( y_1, y_2, y_3 \), and \( |z_1 z_2 y_1 y_2 y_3| = 1 = 1 \). Without loss of
Table 2: $C(2,4)$: $f_0 + x_5 f_1$, $B(f_0 + x_5 f_1)$, $B'(f_0 + x_5 f_1)$ and $B'(B(f_0 + x_5 f_1))$ with $B' \in B$ are codewords.

<table>
<thead>
<tr>
<th>Case</th>
<th>$S$</th>
<th>$f_0 = y_1y_2y_3$</th>
<th>$B$</th>
<th>$f_1$</th>
<th>$B$</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>${1, 3, 4}$</td>
<td>$x_1(x_2 + x_3)x_4$</td>
<td>$S_{1,1}$</td>
<td>$y_3x_3$</td>
<td>$y_1 + y_2(x_3 + x_4)$</td>
</tr>
<tr>
<td></td>
<td>${4}$</td>
<td>$x_1(x_2 + x_3)x_4$</td>
<td>$S_{1,1}$</td>
<td>$y_1(x_2 + x_3)$</td>
<td>$(y_1 + y_2 + y_3)(x_1 + x_2)$</td>
</tr>
<tr>
<td></td>
<td>${1, 2, 3, 4}$</td>
<td>$(x_1 + x_2)(x_2 + x_3)x_3$</td>
<td>$S_{1,1}$</td>
<td>$y_1 + y_2x_1$</td>
<td>$(y_1 + y_2 + y_3)x_2$</td>
</tr>
<tr>
<td></td>
<td>${1, 2}$</td>
<td>$x_1(x_2 + x_3)(x_2 + x_4)$</td>
<td>$S_{1,1}$</td>
<td>$y_2x_2$</td>
<td>$y_3(x_1 + x_2)$</td>
</tr>
<tr>
<td>II</td>
<td>${2, 3}$</td>
<td>$x_1x_3x_4$</td>
<td>$S_{1,1}$</td>
<td>$y_1y_2 + y_3(x_1 + x_2 + x_3)$</td>
<td>$y_2y_3 + (y_1 + y_2)(x_1 + x_2)$</td>
</tr>
<tr>
<td></td>
<td>${1}$</td>
<td>$(x_1 + x_2)x_3x_4$</td>
<td>$S_{1,1}$</td>
<td>$y_1 + y_2y_3 + (y_2 + y_3)x_2$</td>
<td>$y_2y_3 + (y_1 + y_3)x_2$</td>
</tr>
<tr>
<td></td>
<td>${2, 4}$</td>
<td>$(x_1 + x_2)(x_2 + x_3)x_4$</td>
<td>$S_{1,1}$</td>
<td>$y_1 + y_2y_3 + y_3x_1$</td>
<td>$y_2y_3 + y_1x_3$</td>
</tr>
<tr>
<td></td>
<td>${3}$</td>
<td>$(x_1 + x_3)(x_2 + x_4)$</td>
<td>$S_{1,1}$</td>
<td>$y_1y_2 + (y_1 + y_3)x_2$</td>
<td>$y_1y_2 + y_1 + y_2 + y_3x_1$</td>
</tr>
<tr>
<td>I &amp; II</td>
<td>${2, 3, 4}$</td>
<td>$x_1x_2x_3$</td>
<td>$S_{1,1}$</td>
<td>$y_1(x_2 + x_4)$</td>
<td>$y_1y_2 + y_1 + y_2 + y_3x_4$</td>
</tr>
<tr>
<td></td>
<td>${1, 2, 3}$</td>
<td>$x_1x_2x_3x_4$</td>
<td>$S_{1,1}$</td>
<td>$(y_1 + y_2 + y_3)x_1$</td>
<td>$y_1y_2 + y_1(x_1 + x_2)$</td>
</tr>
<tr>
<td></td>
<td>${1, 2, 4}$</td>
<td>$x_1x_2x_3x_4$</td>
<td>$S_{1,1}$</td>
<td>$y_1 + y_2(x_2 + x_3)$</td>
<td>$y_1y_2 + y_1x_3$</td>
</tr>
<tr>
<td></td>
<td>${3, 4}$</td>
<td>$(x_1 + x_3)x_2x_4$</td>
<td>$S_{1,1}$</td>
<td>$y_1(x_1 + x_4)$</td>
<td>$y_1y_2 + (y_1 + y_3)x_3$</td>
</tr>
<tr>
<td></td>
<td>${1, 3}$</td>
<td>$x_1(x_2 + x_3) + x_4$</td>
<td>$S_{1,1}$</td>
<td>$y_1 + y_2(x_2 + x_4)$</td>
<td>$y_1y_2 + (y_1 + y_3)x_3$</td>
</tr>
<tr>
<td></td>
<td>${1, 4}$</td>
<td>$(x_1 + x_4)x_2x_3$</td>
<td>$S_{1,1}$</td>
<td>$y_1 + y_2(x_2 + x_3 + x_4)$</td>
<td>$y_1y_2 + y_2x_4$</td>
</tr>
<tr>
<td></td>
<td>${2}$</td>
<td>$(x_2 + x_3)(x_3 + x_4)$</td>
<td>$S_{1,1}$</td>
<td>$y_2x_4$</td>
<td>$y_1y_2 + (y_1 + y_3)x_4$</td>
</tr>
</tbody>
</table>

For $y_1y_2y_3 \in RM_{4,3}(2)$, suppose that there is a code word $f$ of Case I or II. From (32) or (35) and Lemma 1, $f$ and its binary shift with respect to $y_4$, denoted $B_{y_4}(f)$, are in the same coset (block) of $PT$. Note that $y_4$ with $1 \leq i \leq 3$ are invariant under the shift, and therefore the binary shift $B_{y_4}$ is unique. For Case I (or II), $f$ and $B_{y_4}(f)$ are called a Case I (or II) pair.

Table 2 shows that the number of representative blocks which consist of two Case I type II, two Case II pairs and a combination of Case I and Case II pairs are 4, 4 and 7, respectively. In each block, $f_0$ is a product of three affine polynomials named $y_1, y_2, y_3$, and $f_1$ is expressed in terms of $y_1, y_2, y_3$ and an affine polynomial linearly independent of $y_i$'s. Subexpression $y_1 + y_2$ and $y_1 + y_2 + y_3$ in $f_1$ correspond to row operations in $f_0$. By making such row operations and renaming $y_i$'s, the standard forms (32) and (35) can be derived. The first column shows that the coset in which the block belongs is $\sum_{i \in S} g_i \Gamma_{RM'}$.

### 3.2 EBCH(64, 45, 8)

#### 3.2.1 Structure of the code

In this section, let $C$ denote EBCH(64, 45, 8). From (12),

$$RM_{6,3} \subset C \subset RM_{6,4}. \quad (37)$$

Define

$$\Gamma_{RM} \triangleq C/RM_{6,3}. \quad (38)$$

Then, $\dim(\Gamma_{RM}) = 3$. We found the following set $\{g_1, g_2, g_3\}$ of generators which spans a set of coset leaders
Table 3: The characterization of blocks in $\mathcal{PT}(w_0, w_1)$ with $w_0 \leq w_1$ and $w_0 + w_1 = 8$ for EBCH(64, 45, 8).

| $w_0, w_1$ | $|D_0(w_0)|$ | $|D_1(w_1)|$ | $|\mathcal{PT}(w_0, w_1)|$ | Subcode |
|-------------|-------------|-------------|-----------------|--------|
| 0, 8        | 1           | 620         | 1               | RM$_{6,3}$ |
| 2, 6        | 1           | 32          | 112             |        |
| 4, 4        | 8           | 8           | 155             | RM$_{6,3}$ |
|             | 2           | 2           | 2240            |        |

of $\Gamma_{RM}$:

$$
\begin{align*}
  g_1 &= x_1 x_3 x_4 x_5 \{x_1 x_4 + x_3 x_5\} x_2 x_6, \\
  g_2 &= x_1 x_2 x_4 x_5 \{x_1 x_2 x_3 x_4 x_5\} x_6, \\
  g_3 &= (x_1 + x_2) x_3 x_4 x_5 + (x_2 + x_3) x_4 + x_2 x_5 x_6.
\end{align*}
$$

(39)

The basis of coset leaders was given by an algebraic method in [2].

Note that

$$
\begin{align*}
  p_0 g_1 &= x_1 x_3 x_4 x_5, \\
  p_0 g_2 &= x_1 x_2 x_4 x_5, \\
  p_0 g_3 &= (x_1 + x_2) x_3 x_4 x_5.
\end{align*}
$$

(40)

Since $p_0 g_1, p_0 g_2$ and $p_0 g_3$ are linearly independent polynomials of degree 4, $s_1 C = s_1 RM_{6,3} = RM_{5,2}$ and by (15),

$$
  s_6 C = RM_{5,2}, \text{ for } b \in \{0, 1\}.
$$

(41)

For $\mathcal{PT} \triangleq C / (s_6 C \circ s_1 C) = C / (RM_{5,2} \circ RM_{5,2})$, $\text{dim}(\mathcal{PT}) = 13$. Each coset of $\Gamma_{RM}$ consists of $2^{10}$ cosets of $\mathcal{PT}$. The results by a computer analysis of $\mathcal{PT}(8)$ are summarized in Table 3. For blocks $D_0(w_0) \circ D_1(w_1) \in \mathcal{PT}(w_0, w_1)$ with $(w_0, w_1) \in \text{swp}_0.1(C(8))$, $|D_2(w_3)|$ with $b \in \{0, 1\}$ and $|\mathcal{PT}(w_0, w_1)|$ are shown only for $w_0 \leq w_1$ in Table 3 because of the symmetry (15).

Since $s_6 C = RM_{5,2}$, $p_1 C(0, 8)$ is the set of the minimum weight codewords of $RM_{5,2}$. The algebraic structure of $C(4, 4) \cap RM_{6,3}(4, 4)$ can be directly obtained from that of $RM_{m, r}(2^{m-r-1}, 2^{m-r-1})$ presented in [8, 9]. We analyze the structure of $C(4, 4) \setminus RM_{6,3}(4, 4)$.

As shown in Table 4, there exists an affine transformation with $x_1, x_2, x_3$ from $g_1 RM_{6,3}$ to $\sum_{i \in S} g_i RM_{6,3}$ with $S \subseteq \{1, 2, 3\}$. Since RM codes are invariant under affine transformations, 7 cosets in $\Gamma_{RM} \setminus RM_{6,3}$ have the same split weight structure over uniform 8 or less subsections. Hence, it is sufficient to analyze the structure of codewords in the coset with coset leader $g_1$ of $\Gamma_{RM}(2, 6) \cup \Gamma_{RM}(4, 4)$.

We use the fact that $g_1$ has the following invariant affine transformations:

$$
A_{1, 2} \triangleq x_1 \leftarrow x_4, A_{3, 3, 5} \triangleq x_3 \leftarrow x_5, A_{11, 15, 35} \triangleq \begin{cases} x_1 \leftarrow x_3 \\ x_3 \leftarrow x_5 \\ x_4 \leftarrow x_5, \end{cases}
$$

(42)

where $x_i \leftarrow x_j$ and $x_j \leftarrow x_i$ are abbreviated as $x_i \leftrightarrow x_j$.

Table 4: Affine transformations from $g_1 \cdot RM_{6,3}$ to $\sum_{i \in S} g_i \cdot RM_{6,3}$.

<table>
<thead>
<tr>
<th>$S$</th>
<th>Affine transformation</th>
</tr>
</thead>
<tbody>
<tr>
<td>{2}</td>
<td>$x_1 \leftarrow x_2$</td>
</tr>
<tr>
<td>{3}</td>
<td>$x_1 \leftarrow x_2$</td>
</tr>
<tr>
<td>{1, 2}</td>
<td>$x_2 \leftarrow x_3$</td>
</tr>
<tr>
<td>{1, 3}</td>
<td>$x_3 \leftarrow x_2$</td>
</tr>
<tr>
<td>{2, 3}</td>
<td>$x_1 \leftarrow x_2$</td>
</tr>
<tr>
<td>{1, 2, 3}</td>
<td>$x_2 \leftarrow x_3$</td>
</tr>
</tbody>
</table>

3.2.2 Structure of $C(2, 6)$

From Table 3, there are 16 (=112/7) blocks of $\mathcal{PT}(2, 6)$ in $g_1 \cdot \Gamma_{RM}$. Define

$$
g'_1 \triangleq g_1 + x_2 x_5 x_6 = x_1 x_3 x_4 x_5 + (x_1 x_4 + x_3 x_5) x_2 x_6.
$$

(43)

Then, $g'_1 \in g_1 \cdot \mathcal{PT}(2, 6)$. Therefore, one of the 16 blocks is the subset, $g_1 \cdot \mathcal{PT}(2, 6)$, of $g_1 \cdot \mathcal{PT}$, where

$$
g_1 \cdot \mathcal{PT} = g_1 + (RM_{5,2} \circ RM_{5,2}).
$$

(44)

From Lemma 1-(i), the 16 blocks in $g_1 \cdot \Gamma_{RM}$ can be obtained from the block by applying the binary shifts in $B_{1 \times \ast \ast \ast}^1$.

It follows from Table 3, (43) and (44) that for $f$ in $g_1 \cdot \mathcal{PT}(2, 6)$, $p_0 f = p_0 g_1$, and therefore, $f$ can be expressed as $g_1 + x_6 h$ with $h \in RM_{5,2}$. Define $f_0 \triangleq p_0 f = x_1 x_3 x_4 x_5$ and

$$
f_1 \triangleq (x_1 x_4 + x_3 x_5) x_2 + h.
$$

(45)

Then, $p_1 f = f_0 + f_1$, and $|f_0|_5 = 2$ and $|f_0 + f_1|_5 = 6$.

From (7),

$$
|f_0 + f_1|_5 - |f_0|_5 = |f_1|_5 - 2, |f_0 f_1|_5 = 4.
$$

(46)

where

$$
|f_0 f_1|_5 = |f_1 x_{1 \leftarrow x_3} x_{2 \leftarrow x_5}|_1 = |h_{x_1 \leftarrow x_3} x_{2 \leftarrow x_5}|_1.
$$

(47)

If $h = 0$, then from (45) to (47), $|f_1|_5 = 6$, $|f_0 f_1|_5 = 0$ and $|f_0 + f_1|_5 = 8$, a contradiction. Hence $|f_1|_5 \geq 4$. Based on the monomial basis of RM codes, we prove that $|f_1|_5 \geq 6$. If $|f_1|_5 = 4$, then $f_1$ can be expressed as $y_1 y_2 y_3$, where $y_i = a_0 + \sum_{j=1}^{5} a_j x_j$ with $1 \leq i \leq 3$. Express $y_1 y_2 y_3$ as the sum of monomials. From (45), $f_1$ has two monomials of degree 3, $x_1 x_2 x_4$ and $x_2 x_3 x_5$, only. Without loss of generality, we can assume that $a_1 = 1$, $a_2 = a_3 = 1$ and $a_{14} = a_{35} = 1$. Then, besides $x_1 x_2 x_4$ and $x_2 x_3 x_5$, $y_1 y_2 y_3$ has monomials $x_2 x_3 x_4$ and $x_1 x_2 x_5$, a contradiction. From (46) and $|f_1|_5 \geq 6$, we have $|f_0 f_1|_5 \geq 1$. Hence, there remain the following two cases:

Case I: $|f_1|_5 = 6$ and $|f_0 f_1|_5 = |h_{x_1 \leftarrow x_3} x_{2 \leftarrow x_5}|_1 = 1$.
Case II: $|f_1|_5 = 8$ and $|f_0 f_1|_5 = |h_{x_1=x_3=x_4=x_5=1}| = 2$.

First, consider Case I. As an example, $g'_1$ is Case I. From the second condition, for simplicity, we assume that $h$ is a form of $x_2(\bar{a}_1 x_1 + \bar{a}_2 x_2 + \bar{a}_4 x_4 + \bar{a}_5 x_5 + 1)$. Since $x_{2} = \bar{x} + a$, $x_1 x_4 + x_3x_5 + h/x_2 = (x_{1}^{a_1} x_4 + x_3 x_5^{a_2} + a_3 a_4 + a_3 a_5 + 1)$. Therefore, $f_1 = B(x_1 x_4 + x_3 x_5) + h + x_2(a_1 a_4 + a_3 a_5 + 1)$, where $B$ is a binary shift such that $x_i \leftarrow x_i^{a_i}$ for $i = 1, 3, 4, 5$. From the first condition $|f_1|_5 = 6$ of Case I, $a_1 a_4 + a_3 a_5 = 1$, which implies

$$B \in B_{1+0, 1} \cup B_{1+110} \cup B_{0+1+1} \cup B_{1+101}. \quad (48)$$

The number of the binary shifts in (48) is 12.

Next consider Case II.
(i) From the second condition,

$$h_{x_1=x_3=x_4=x_5=1} = 1. \quad (49)$$

A simple example of $h$ which meets the first condition is $h = x_1 x_4$ or $x_3 x_5$. Define $f'_1 \equiv (x_1 x_4 + x_3 x_5) + h + x_2 x_3 x_5. \quad (50)$

Then, $|f'_1|_5 = 8$, $|f_0 f'_1|_5 = 2$ and $B_2(f'_1) = x_2 x_1 x_4 + x_2 x_3 x_5 = (x_1 x_4 + x_3 x_5) x_2 + x_1 x_2$ is Case II, too.

(ii) Consider the following type of Case II:

$$f_1 = B(f'_1) + h', \quad \text{for } h' \in \text{RM}_{5, 2}, \quad (51)$$

where $B \in B_{1+1+1+1}$ such that $B(f'_1)_{x_1=x_3=x_4=x_5=1} = 0. \quad (52)$

From the second condition,

$$h'_{x_1=x_3=x_4=x_5=1} = 1. \quad (53)$$

That is, $h'$ is independent of $x_2$. For the first condition, note that

$$f_1 |_{x_1 x_2 = 0} = x_1^{a_1} x_4^{a_4} + h', \quad f_1 |_{x_1 x_2 = 1} = x_3^{a_3} x_5^{a_5} + h'. \quad (54)$$

From (52), the first term is zero, and therefore, $|f_1|_{x_2=b}|_4 > 0$. Hence,

$$|f_1|_{x_2=b}|_4 = 4, \quad \text{for } b \in \{0, 1\}, \quad (54)$$

which implies that $h'$ is a single term.

(iii) Let $h' = y_1 y_2$, where $y_1 \in \{x_1, x_4\}$, $y_2 \in \{x_3, x_5\}$. As an example meeting (53) and (54), let $y_1 = x_4$, $y_2 = x_5$ and $B = B_{1+1+1+1}$. Then,

$$f_1 = B_{1+1+1+1}(f'_1) + x_4 x_5 = x_2 x_1 x_4 + x_2 x_3 x_5 + x_4 x_5 = x_2 (x_1 + x_5) x_4 + x_2 (x_3 + x_4) x_5. \quad (55)$$

Then, $|f_1|_5 = 8$ and $|f_0 f_1|_5 = 2$. By invariant transformations over $g_1$, $A_{1, 4}$ and $A_{3, 5}$, and binary shift $B_2$, we have 8 new codewords of $g_1$-$\text{PT}(2, 6)$.

(ii) As another example, let $h' = (x_1 + x_4) x_5$ and $B = B_{1+1+1+1}$. Then,

$$f_1 = x_2 x_1 x_4 + x_2 x_3 x_5 + (x_1 + x_4) x_5 = x_2 (x_1 + x_4) (x_4 + x_5) + x_2 (x_1 + x_4 + x_4) x_5. \quad (56)$$

Then, $|f_1|_5 = 8$ and $|f_0 f_1|_5 = 2$. By transformations $A_{3, 5}$, $A_{1, 4}$ and $B_2$, we have 8 new codewords.

(iii) Let $h' = (x_1 + x_4) (x_3 + x_5)$ and $B = B_{1+1+1+1}$. Then,

$$f_1 = x_2 x_1 x_4 + x_2 x_3 x_5 + (x_1 + x_4) (x_3 + x_5) = x_2 (x_1 + x_4) (x_1 + x_3 + x_5) + x_2 (x_3 + x_5) (x_1 + x_3 + x_4). \quad (57)$$

Then, $|f_1|_5 = 8$ and $|f_0 f_1|_5 = 2$. $f$ and $B_2(f)$ are two new codewords of $g_1$-$\text{PT}(2, 6)$.

Thus, we find all 32 codewords in $g_1$-$\text{PT}(2, 6)$ (see Table 5).

### 3.2.3 Structure of $C(4, 4) \setminus \text{RM}_{0, 6}$

From Table 3, there are 320 (2240/7) blocks of $\text{PT}(4, 4)$ in $g_1$-$\text{RM}_{0, 6}(4, 4)$, and for a block $D$ in $\text{PT}(4, 4)$, $D = p_1 D$ and $[p_1 D] = 2$ with $b \in \{0, 1\}$. For $f \in g_1$-$\text{RM}_{0, 6}$, $f$ can be expressed as $f = g_1 + h$, where $h = h_0 + x_6 h_1$ with $h_0 \in \text{RM}_{5, 3}$ and $h_1 \in \text{RM}_{5, 2}$. Suppose that $f \in g_1$-$\text{RM}_{0, 6}(4, 4)$. Then,

$$w_0(f) = |x_1 x_3 x_4 x_5 + h_0|_5 = 4, \quad (57)$$

$$w_1(f) = |x_1 x_3 x_4 x_5 + (x_1 x_4 + x_3 x_5) x_2 + h_0 + h_1|_5 = 4. \quad (58)$$

From (57), $w_0(f) = 2 + |h_0|_5 - 2|x_1 x_3 x_4 x_5 h_0|_5 = 4$, where $|h_0|_5 \geq 4$ and $0 \leq |x_1 x_3 x_4 x_5 h_0|_5 \leq 2$. There are two cases:

Case I: $|h_0|_5 = 4$ and $|h_0 |_{x_1=x_3=x_4=x_5}|_1 = 1$. Then, $h_0 = y_1 y_2 y_3$. By row operations, only $y_3$ is dependent on $x_2$, and $y_1, y_2, y_3, y_4, y_5, y_6 = 1$ with $i \in \{1, 2\}$. By row operations, $p_0 g_1 = y_1 y_2 y_4 y_5$, and therefore

$$p_0 f = y_1 y_2 (y_4 y_5 + y_6). \quad (59)$$

Case II: $|h_0|_5 = 6$ and $|h_0 |_{x_1=x_3=x_4=x_5}|_1 = 1$. Then, $h_0 = z_1 (z_2 z_3 + z_4 z_5)$, and by row and cross operations, only one of $z_1$ and $z_2$ depends on $x_2$. If $z_2$ does not depend on $x_2$, then $h_0 |_{x_1=x_3=x_4=x_5}|_1$ is 0 or $x_2 + b$, where $|h_0 |_{x_1=x_3=x_4=x_5}|_1 = 0$ or 1, a contradiction. Hence, $z_2$ depends on $x_2$. If and only if $z_1 = z_4 = z_5 = 1$ and $z_1 = 0$ at $x_1 = x_3 = x_4 = x_5 = 1$, $|h_0 |_{x_1=x_3=x_4=x_5}|_1 = 2$. By row operations of $p_0 g_1 = y_1 y_2 y_3 y_4$, $y_1 = z_1, y_2 = z_3, y_3 y_4 = z_4 z_5$ and therefore,

$$p_0 f = y_1 y_2 y_3 y_4 + y_1 (z_2 y_2 + y_3 y_4) = y_1 y_2 (y_4 y_5 + y_6). \quad (60)$$

Next we consider (58). Define

$$h'_0 \equiv (x_1 x_4 + x_3 x_5) x_2 + h_0 + h_1 \in \text{RM}_{5, 3}. \quad (61)$$
Table 5: The 5 representative codewords of $g_1 \cdot P \mathcal{T}(2, 6)$. The 32 codewords shown in 3.2.2 are $f_0 + x_6 f_1$, $f_0 + x_6 B(f_1)$ and $f_0 + x_6 A(f_1)$, where $f_0 = x_1 x_2 x_3 x_5$.

<table>
<thead>
<tr>
<th>Case</th>
<th>$f_1$</th>
<th>Binary shift $B$</th>
<th>Transformation $A$</th>
<th>Group Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>$x_1 x_2 x_4 + x_2 x_5 x_6$</td>
<td>$B_{1+11}, B_{1+10}, B_{10+1}, B_{0+01}$</td>
<td>$--$</td>
<td>12</td>
</tr>
<tr>
<td>II (i)</td>
<td>$x_2 x_1 x_4 + x_2 x_3 x_5$</td>
<td>$B_2$</td>
<td>$--$</td>
<td>2</td>
</tr>
<tr>
<td>II (ii-1)</td>
<td>$x_2 x_1 x_4 + x_2 x_3 x_5 + x_4 x_5$</td>
<td>$B_2$</td>
<td>$A_{1, 4}, A_{3, 5}$</td>
<td>8</td>
</tr>
<tr>
<td>II (ii-2)</td>
<td>$x_2 x_1 x_4 + x_2 x_3 x_5 + (x_1 + x_4) x_5$</td>
<td>$B_2$</td>
<td>$A_{1, 3}, A_{1, 4, 5}$</td>
<td>8</td>
</tr>
<tr>
<td>II (ii-3)</td>
<td>$x_2 x_1 x_4 + x_2 x_3 x_5 + (x_1 + x_4)(x_3 + x_5)$</td>
<td>$B_2$</td>
<td>$--$</td>
<td>2</td>
</tr>
</tbody>
</table>

It follows from (61) that
\[
g_1 + h_0' + x_6 h_1 = B_6(g_1 + h_0 + x_6 h_1) = B_6(f).
\] (62)
Since $h_1 \in \text{RM}_{5, 2}$, $h_0' \neq h_0$, and therefore,
\[
p_0 f \neq p_1 f.
\] (63)
From (57) and (58), $h_0$ and $h_0'$ are either Case I or Case II, respectively. We concentrate on the following case, which is the special case of Case I with $y_3 = x_2$.

Case I: $h_0 = y_1 y_2 x_2$ such that $y_1 y_2 x_2 = x_2 = x_1 = x_4 = x_5 = 1$.

Since $h_0' = x_2(x_1 x_4 + x_3 x_5 + y_1 y_2) + h_1$, $h_0$ is not Case II and if $h_0'$ meets (58), then it is a Case I' and $x_1 x_4 + x_3 x_5 + y_1 y_2$ is reduced to a single term, say, $y_1 y_2 = x_1 x_4 x_3 x_5 (x_1 + x_4 + 1)x_4 \ldots$ The number of those minimum weight codewords of RM\textsubscript{4, 2} which are one at $x_1 = x_2 = x_3 = x_4 = x_5 = 1$ is $\prod_{i=0}^{4}(2^{4-i} - 1)/(2^{2} - 1) = 35$. We have found that for 20 $y_1 y_2$'s among the 35 codewords,
\[
h_0' = (x_1 x_2 + x_3 x_5 + y_1 y_2) x_2 + h_1
\] (64)
are Case I'. Table 6 lists the 10 $y_1 y_2$'s and the related $h_1/x_2$ and $h_0'/x_2$.

Table 6: The representative 10 $h_0/x_2$ and related $h_1/x_2$ and $h_0'/x_2$.

<table>
<thead>
<tr>
<th>$h_0/x_2$</th>
<th>$h_1/x_2$</th>
<th>$h_0'/x_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(x_1 + x_5)x_3$</td>
<td>$x_1 + x_3$</td>
<td>$x_1(x_3 + x_4)$</td>
</tr>
<tr>
<td>$(x_1 + x_3 x_5) x_3$</td>
<td>$x_1 + x_3 + x_4$</td>
<td>$(x_1 + x_4)(x_3 + x_4)$</td>
</tr>
<tr>
<td>$(x_1 + x_3)(x_3 + x_5)$</td>
<td>$x_1 + x_3 + x_4$</td>
<td>$x_1(x_3 + x_4 + x_5)$</td>
</tr>
<tr>
<td>$(x_1 + x_4 + x_5)(x_3 + x_5)$</td>
<td>$x_1 + x_3 + x_4 + x_5$</td>
<td>$(x_1 + x_4)(x_3 + x_4 + x_5)$</td>
</tr>
<tr>
<td>$x_1 x_4$</td>
<td>$0$</td>
<td>$x_3 x_5$</td>
</tr>
<tr>
<td>$(x_1 + x_5)x_4$</td>
<td>$x_3 + x_4$</td>
<td>$x_3(x_4 + x_5)$</td>
</tr>
<tr>
<td>$(x_1 + x_5)x_4$</td>
<td>$x_4 + x_5$</td>
<td>$(x_3 + x_4)x_5$</td>
</tr>
<tr>
<td>$(x_1 + x_3) x_4$</td>
<td>$x_3 + x_4$</td>
<td>$(x_3 + x_4)x_5$</td>
</tr>
<tr>
<td>$(x_1 + x_4 + x_5) x_4$</td>
<td>$x_3 + x_4 + x_5$</td>
<td>$(x_3 + x_5)(x_4 + x_5)$</td>
</tr>
<tr>
<td>$x_1(x_4 + x_5)$</td>
<td>$x_1 + x_5$</td>
<td>$(x_1 + x_3 + x_4)x_5$</td>
</tr>
<tr>
<td>$(x_1 + x_5)(x_4 + x_5)$</td>
<td>$x_1 + x_5$</td>
<td>$(x_1 + x_3 + x_4)x_5$</td>
</tr>
</tbody>
</table>

4 Conclusion

For two EBC codes, EBC(32, 21, 6) and EBC(64, 45, 8), the sets of minimum weight codewords are analyzed in terms of Boolean polynomial representation. We have listed all the representative minimum weight codewords for the codes, and shown the transformations to obtain the remaining minimum weight codewords. Both codes contain an RM code as a large subcode. The minimum distance of EBC(32, 21, 6) is smaller than that of the RM code RM\textsubscript{5, 2}, while that of EBC(64, 45, 8) is equal to the RM code RM\textsubscript{6, 3}.

To obtain the results, binary shift invariance property is utilized. Especially, for a linear code $C$ satisfying (17), we can use the property effectively as shown in Lemma 1.

References


