Memoirs of the Faculty of Engineering, Okayama University, Vol. 42, pp. 1-9, January 2008

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
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 $\boldsymbol{v}$ in a proper bit order. For RM codes, either the left half subword of $\boldsymbol{v}$ is equal to the other or one of the half subwords of $\boldsymbol{v}$ is $\mathbf{0}$. In contrast, for EBCH codes, the left half subword of $\boldsymbol{v}$ 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 $\boldsymbol{u} = (u_1, u_2, \ldots, u_{2^m}) \in V_m$, define $p_0\boldsymbol{u} \triangleq (u_1, u_2, \ldots, u_{2^{m-1}})$ and $p_1\boldsymbol{u} \triangleq (u_{2^{m-1}+1}, u_{2^{m-1}+2}, \ldots, u_{2^m})$. Define $p_0C \triangleq \{p_0\boldsymbol{u} : \boldsymbol{u} \in C\}$ and $p_1C \triangleq \{p_1\boldsymbol{u} : \boldsymbol{u} \in C\}$. 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, define $s_0C \triangleq p_0C_0$ and $s_1C \triangleq p_1C_1$. For two binary 2^{m-1}-tuples $\boldsymbol{a} = (a_1, a_2, \ldots, a_{2^{m-1}})$ and $\boldsymbol{b} = (b_1, b_2, \ldots, b_{2^{m-1}})$, let $\boldsymbol{a} \circ \boldsymbol{b}$ denote the concatenation of $\boldsymbol{a}$ and $\boldsymbol{b}$, $(a_1, a_2, \ldots, a_{2^{m-1}}, b_1, b_2, \ldots, b_{2^{m-1}})$, and for binary linear block codes of length 2^{m-1}, A and B, $A \circ B$ denotes $\{\boldsymbol{a} \circ \boldsymbol{b} : \boldsymbol{a} \in A, \boldsymbol{b} \in B\}$.

Let C' be a linear subcode of C. Define

$$\mathcal{T} \triangleq C/C', \tag{1}$$

as the set of all cosets of C' in C. Abbreviate $C/(s_0C \circ s_1C)$ as $\mathcal{PT}$. Then, there is a one-to-one correspondence between the cosets in $\mathcal{PT}$ and the middle states of the 2-section trellis diagram [4]. We will analyze the structure of minimum weight codeword with respect to $\mathcal{PT}$.

For $\boldsymbol{u} \in V_m$, define $w(\boldsymbol{u})$ as the weight of $\boldsymbol{u}$, and define $w_0(\boldsymbol{u}) \triangleq w(p_0\boldsymbol{u})$ and $w_1(\boldsymbol{u}) \triangleq w(p_1\boldsymbol{u})$. For $U \subseteq C$, let $\mathrm{wp}(U)$, $\mathrm{wp}_0(U)$ and $\mathrm{wp}_1(U)$ denote the weight profile of U, p_0U and p_1U, respectively. For $w \in \mathrm{wp}(U)$, define

$$U(w) \triangleq \{\boldsymbol{u} \in U : w(\boldsymbol{u}) = w\}. \tag{2}$$

For $\boldsymbol{u} \in V_m$, define $w_{0,1}(\boldsymbol{u})$ as the split weight of $\boldsymbol{u}$, $(w_0(\boldsymbol{u}), w_1(\boldsymbol{u}))$. Let $\mathrm{swp}_{0,1}(U)$ with $U \subseteq C$ denote the split weight profile of U. For $(w_0, w_1) \in \mathrm{swp}_{0,1}(U)$,

$$U(w_0, w_1) \triangleq \{\boldsymbol{u} \in U : w_0(\boldsymbol{u}) = w_0, w_1(\boldsymbol{u}) = w_1\}. \tag{3}$$

For $\mathcal{T} = C/C'$, for example $C' = s_0C \circ s_1C$, define g-$\mathcal{T} \triangleq D \in \mathcal{T}$ such that $g \in D$. For $w \in \mathrm{wp}(C)$ (or $(w_0, w_1) \subseteq \mathrm{swp}_{0,1}(C)$), define

$$\mathcal{T}(w) \triangleq \{D(w) : D \in \mathcal{T}\}, \tag{4}$$

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

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

Let d be the minimum distance of the linear code C. For $w_b \in \mathrm{wp}_b(C)$ with $b \in \{0, 1\}$, if there are $\boldsymbol{u}$ and $\boldsymbol{u}'$ in $D_b(w_b)$, $w_b \geq d/2$, since $w_b(\boldsymbol{u} + \boldsymbol{u}') \geq d$. From this, the following relation holds [3] for $D \in \mathcal{T}$ and $(w_0, w_1) \in \mathrm{swp}_{0,1}(D)$ with $w_0 + w_1 = d$.

(i) If $0 \leq w_b < d/2$, then $|D_b(w_b)| = 1$.

(ii) If $|D_b(w_b)| \geq 2$ for $b = 0$ and 1, then $w_b = d/2$.

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 $P_m^1 \setminus P_m^0$ is called an affine polynomial. A set of l affine polynomials $\{a_{i0} + \sum_{j=1}^{m} a_{ij}x_j : a_{ij} \in \{0, 1\}$ 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 $(b_{i1}, b_{i2}, \ldots, b_{im})$ be the standard binary expression of i such that $i = \sum_{j=1}^{m} b_{ij}2^{m-j}$. For $f(x_1, x_2, \ldots, x_m) \in P_m^m$, define the following binary 2^m-tuple:

$$b(f) \triangleq (v_1, v_2, \ldots, v_{2^m}), \tag{5}$$

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

$$v_{i+1} \triangleq f(b_{i1}, b_{i2}, \ldots, b_{im}), \text{ for } 0 \leq i < 2^m. \tag{6}$$

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 rth order RM code of length 2^m [5, 6], denoted $\mathrm{RM}_{m,r}$, 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 $\boldsymbol{a} = (a_1, a_2, \ldots, a_{2^m})$ and $\boldsymbol{b} = (b_1, b_2, \ldots, b_{2^m})$ be two binary 2^m-tuples. Define the following boolean product of $\boldsymbol{a}$ and $\boldsymbol{b}$,

$$\boldsymbol{a} \cdot \boldsymbol{b} \triangleq (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_{2^m} \cdot b_{2^m}),$$

where '$\cdot$' denotes the logic product, i.e. $a_i \cdot b_i = 1$ if and only if both a_i and b_i are '1'. For simplicity, we use $\boldsymbol{ab}$ for $\boldsymbol{a} \cdot \boldsymbol{b}$. For $f_a, f_b \in V_m$, f_af_b denotes the boolean product of $b(f_a)$ and $b(f_b)$.

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

$$|f_0 + f_1|_m = |f_0|_m + |f_1|_m - 2|f_0f_1|_m. \tag{7}$$

The polynomial $f \in P_m^r$ (with $r < m$) can be expressed as

$$f = f_0 + x_m f_1, \qquad \text{for } f_0 \in P_{m-1}^r, f_1 \in P_{m-1}^{r-1}. \tag{8}$$

Then,

$$p_0 f = f_0, \qquad p_1 f = f_0 + f_1. \tag{9}$$

From (7), (8) and (9), we have that

$$w_0(f) = |f_0|_{m-1}, \tag{10}$$
$$w_1(f) = |f_0|_{m-1} + |f_1|_{m-1} - 2|f_0 f_1|_{m-1}. \tag{11}$$

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 $1 \le i \le m$, the replacement of x_i by affine polynomial y_i is called the affine transformation. An affine transformation $y_i = x_i + b_i$ with $1 \le i \le m$ is called a binary shift. Since an affine transformation is invertible, binary shifts of y_i with $1 \le i \le m$ correspond to binary shifts of x_i's uniquely. If $\boldsymbol{u} \in V_m$ can be transformed to $\boldsymbol{v}$ by binary shift B, then $\boldsymbol{u}$ and $\boldsymbol{v}$ are said to be binary shift equivalent and we write $\boldsymbol{v} = B(\boldsymbol{u})$.

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 $2^{m-r} \supseteq \text{RM}_{m,r}$. (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

$$x_i \leftarrow \begin{cases} \bar{x}_i, & \text{if } i \text{ is in the suffices}, \\ x_i, & \text{otherwise}. \end{cases} \tag{13}$$

For $a_1, a_2, \ldots, a_m \in \{0, 1, *\}$, let $\mathcal{B}_{a_1,a_2,\ldots,a_m}$ be the set of binary shifts such that

$$x_i \leftarrow \begin{cases} x_i^{a_i}, & \text{if } a_i \in \{0,1\}, \\ x_i \text{ or } \bar{x}_i, & \text{if } a_i = *. \end{cases} \tag{14}$$

For $\mathcal{B}_{a_1,a_2,\ldots,a_m}$, if the number of $*$ in its suffices 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:

$$p_0 C = p_1 C, \qquad \text{and} \qquad s_0 C = s_1 C. \tag{15}$$

Hereafter in this section, let i be a positive integer less than or equal to m, $b \in \{0,1\}$, and $f \in P_m^m$. $B_i^{(b)}$ denotes the binary shift of x_i in right and left half subsections defined by

$$B_i^{(b)}(f) \triangleq \begin{cases} B_i(p_0 f) \circ p_1 f, & \text{if } b = 0, \\ p_0 f \circ B_i(p_1 f), & \text{if } b = 1. \end{cases} \tag{16}$$

Define $\deg_i(f)$ 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

$$\text{RM}_{m,r} \subseteq C \subset \text{RM}_{m,r+1}, \qquad \text{for } r < m. \tag{17}$$

(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 $f \in D \in \mathcal{PT}\ (= C/(s_0 C \circ s_1 C))$, if $\deg_i(p_b f) < r$, then $B_i^{(b)}(f) \in D$. If $\deg_i(f) < r$, then $B_i(f) \in D$.

(Proof) (i) $f + B(f) \in \text{RM}_{m,r}$ implies $B(f) \in D$.
(ii) $p_b(f + B_i^{(b)}(f)) = p_b f + B_i(p_b f) \in \text{RM}_{m-1,r-1}$, and $p_{\bar{b}}(f + B_i^{(b)}(f)) = 0$. Since $s_b C \supseteq s_b \text{RM}_{m,r} = \text{RM}_{m-1,r-1}$, $f + B_i^{(b)}(f) \in s_0 C \circ s_1 C$ 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 EBCH(n,k,d). In this section, for two typical examples, EBCH(32, 21, 6) and 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 EBCH(32, 21, 6). From (12),

$$\text{RM}_{5,2} \subset C \subset \text{RM}_{5,3}, \tag{18}$$

where $\text{RM}_{5,3}$ is the extended Hamming code. Define

$$\Gamma_{\text{RM}} \triangleq C/\text{RM}_{5,2}. \tag{19}$$

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

Table 1: The characterization of blocks in $\mathcal{PT}(w_0, w_1)$ with $w_0 \le w_1$ and $w_0 + w_1 = 6$ for EBCH(32, 21, 6).

w_0, w_1	$\lvert D_0(w_0)\rvert$	$\lvert D_1(w_1)\rvert$	$\lvert\mathcal{PT}(w_0, w_1)\rvert$
0, 6	1	16	1
2, 4	1	4	120

generators which spans a set of coset leaders of Γ_{RM}:

$$\begin{cases} g_1=(x_1+x_2)x_3x_4+(x_2x_3+(x_1+x_3)x_4)x_5, \\ g_2=(x_1+x_3)x_2(x_3+x_4)+[(x_1+x_3)x_2+(x_2+x_3)x_4]x_5, \\ g_3=(x_1+x_2)(x_2+x_3)(x_3+x_4)+(x_1x_3+x_2x_4)x_5, \\ g_4=x_1(x_2+x_4)x_3+(x_1+x_2)(x_3+x_4)x_5, \\ g_5=[(x_1+x_3)x_2+(x_1+x_2)x_4]x_5. \end{cases} \tag{20}$$

Now, we consider p_bC and s_bC. Since $p_b\mathrm{RM}_{5,2} = \mathrm{RM}_{4,2}$ and $p_bg_5 \in \mathrm{RM}_{4,2}$,

$$p_bC = \{\textstyle\sum_{i=1}^{4} a_ip_bg_i : a_i \in \{0,1\} \text{ with } 1 \le i \le 4\} + \mathrm{RM}_{4,2}. \tag{21}$$

It can be shown readily that p_0g_i with $1 \le i \le 4$ are linearly independent and therefore,

$$p_0g_i \text{ with } 1 \le i \le 4 \text{ spans } \mathrm{RM}_{4,3} \setminus \mathrm{RM}_{4,2}. \tag{22}$$

Hence, by (15),

$$p_bC = \mathrm{RM}_{4,3}, \qquad \text{and} \qquad \dim(p_bC) = 15. \tag{23}$$

Since $s_b\mathrm{RM}_{5,2} = \mathrm{RM}_{4,1}$, by (15) and (22),

$$s_bC = \{\mathbf{0}, g_{5,x_5=1}\} + \mathrm{RM}_{4,1}, \tag{24}$$

where $g_{5,x_5=1} \triangleq (x_1+x_3)x_2+(x_1+x_2)x_4 \in \mathrm{RM}_{4,2}$. Define

$$\mathrm{RM}'_{5,2} \triangleq \{\mathbf{0}, g_5\} + \mathrm{RM}_{5,2}. \tag{25}$$

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

$$\Gamma_{\mathrm{RM}'} \triangleq C/\mathrm{RM}'_{5,2}. \tag{26}$$

Then, $\dim(\Gamma_{\mathrm{RM}'}) = 4$. Since $\mathrm{RM}_{4,1} \circ \mathrm{RM}_{4,1} \subseteq \mathrm{RM}_{5,2}$, from (24), $\dim(s_bC) = 6$ and $s_0C \circ s_1C \subseteq \mathrm{RM}'_{5,2}$. Then,

$$\dim(\mathrm{RM}'_{5,2}/(s_0C \circ s_1C)) = 5. \tag{27}$$

For $\mathcal{PT} \triangleq C/(s_0C \circ s_1C)$, $\dim(\mathcal{PT}) = 9$. From (27), each coset of $\Gamma_{\mathrm{RM}'}$ 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 $D_0(w_0) \circ D_1(w_1) \in \mathcal{PT}(w_0, w_1)$ with $(w_0, w_1) \in \mathrm{swp}_{0,1}(C(6))$, $|D_b(w_b)|$ with $b \in \{0, 1\}$ and $|\mathcal{PT}(w_0, w_1)|$ are shown for $w_0 \le w_1$.

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 $\boldsymbol{v} \in C(0, 6)$. Then $p_b\boldsymbol{v} \in p_bC = \mathrm{RM}_{4,3}$ with $b \in \{0, 1\}$ from (23). Therefore, the Boolean polynomial corresponding to $\boldsymbol{v}$ is $(y_1y_2 + y_3y_4)x_5$ [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 $B \in \mathcal{B}_{****1}$, $B(g_5) \in g_5+\mathrm{RM}_{5,2} \subseteq C$, $w_1(B(g_5)) = 6$, and $|\{B(g_5) : B \in \mathcal{B}_{****1}\}| = 16$. Then, we have from Table 1 that

$$C(0, 6) = \{B(g_5) : B \in \mathcal{B}_{****1}\}. \tag{28}$$

3.1.3 Structure of $C(2, 4)$

Since $p_0C(2, 4) \subseteq p_0C = \mathrm{RM}_{4,3}$, $p_0C(2, 4) \subseteq \mathrm{RM}_{4,3}(2)$. The number of the minimum weight codewords in $\mathrm{RM}_{4,3}$ is $2^3(2^4 - 1) = 120$ [5]. From Table 1,

$$p_0C(2, 4) = \mathrm{RM}_{4,3}(2). \tag{29}$$

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

For $f_0 \in \mathrm{RM}_{4,3}(2)$, $f \in C(2, 4)$ with $p_0f = f_0$ can be expressed as

$$f = f_0 + x_5f_1, \tag{30}$$

where $p_1f = f_0 + f_1 \in \mathrm{RM}_{4,3}(4)$. f_1 is called the right part of f_0 or f. There are exactly four right parts of f_0 which belong to $s_1C = \{\mathbf{0}, g_5\} + \mathrm{RM}_{4,1}$. 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 $\mathrm{RM}_{4,1}$. 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), $w_1(f) = |f_0+f_1|_4 = |f_0|_4+|f_1|_4 - 2|f_0f_1|_4 = 4$, $|f_1|_4 - 2|f_0f_1|_4 = 2$. Since $f_1 \in P_4^2$ and $f_1 \ne 0$, $|f_1|_4$ is even with $|f_1|_4 \ge 4$ [5]. Since $|f_0|_4 = 2$, $|f_0f_1|_4 \le |f_0|_4 = 2$. Hence, $|f_1|_4 = 4$ or 6. There are two cases for f_1.

Case I: $|f_1|_4 = 4$ and $|f_0f_1|_4 = 1$.

Case II: $|f_1|_4 = 6$ and $|f_0f_1|_4 = 2$.

Since $f_0 \in \mathrm{RM}_{4,3}(2)$, we can express $f_0 = y_1y_2y_3$. We show standard forms for Cases I and II.

Case I: f_1 is expressed as z_1z_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 $|y_1y_2y_3z_1z_2|_4 = 0$ or 2. Hence, z_2 is linearly independent of y_1, y_2, y_3, and $|z_1z_{2\,y_1=y_2=y_3=1}|_1 = 1$. 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 $B' \in \mathcal{B}$ are codewords.

Case	S	$f_0 = y_1y_2y_3$	$\mathcal{B}$	f_1		B
I	$\{1,3,4\}$	$x_1(x_2+x_3)x_4$	$\mathcal{B}_{**1*1}$	y_3x_3	$\overline{y_1+y_2}(x_2+x_4)$	$B_{2,3}$
	$\{4\}$	$x_1(x_2+x_4)x_3$	$\mathcal{B}_{***11}$	$y_1(x_2+x_3)$	$(y_1+y_2+y_3)(x_1+x_2)$	$B_{2,4}$
	$\{1,2,3,4\}$	$(x_1+x_2)(x_2+x_4)x_3$	$\mathcal{B}_{*1**1}$	$\overline{y_1+y_2}x_1$	$(y_1+y_2+y_3)x_2$	$B_{1,2,4}$
	$\{1,2\}$	$x_1(x_2+x_3)(x_2+x_4)$	$\mathcal{B}_{*1**1}$	y_2x_2	$y_3(x_1+x_2)$	$B_{2,3,4}$
II	$\{2,3\}$	$x_1x_3x_4$	$\mathcal{B}_{*1**1}$	$y_1y_2+\bar{y}_3(x_1+x_2+x_3)$	$y_2y_3+(y_1+y_2)(x_1+x_2)$	B_2
	$\{1\}$	$(x_1+x_2)x_3x_4$	$\mathcal{B}_{*1**1}$	$\overline{y_1+y_2}y_3+(y_2+y_3)x_2$	$y_2y_3+(y_1+y_3)x_2$	$B_{1,2}$
	$\{2,4\}$	$(x_1+x_2)(x_2+x_3)x_4$	$\mathcal{B}_{*1**1}$	$\overline{y_1+y_2}y_3+\bar{y}_2x_1$	$y_2y_3+\bar{y}_1x_3$	$B_{1,2,3}$
	$\{3\}$	$(x_1+x_2)(x_2+x_3)(x_3+x_4)$	$\mathcal{B}_{*1**1}$	$y_1y_2+(y_1+y_3)x_2$	$y_1y_2+\overline{y_1+y_2+y_3}x_1$	$B_{1,2,3,4}$
I & II	$\{2,3,4\}$	$x_1x_2x_3$	$\mathcal{B}_{***11}$	$y_3(x_2+x_4)$	$y_1y_2+\overline{y_1+y_2+y_3}x_4$	B_4
	$\{1,2,3\}$	$x_2x_3x_4$	$\mathcal{B}_{1***1}$	$(y_1+y_2+y_3)x_1$	$y_1y_3+\bar{y}_2(x_1+x_2)$	B_1
	$\{1,2,4\}$	$x_1x_2x_4$	$\mathcal{B}_{**1*1}$	$\overline{y_1+y_2}(x_2+x_3)$	$\overline{y_1+y_2}y_3+\bar{y}_1x_3$	B_3
	$\{3,4\}$	$(x_1+x_3)x_2x_4$	$\mathcal{B}_{**1*1}$	$y_2(x_1+x_4)$	$y_1y_3+(y_2+y_3)x_3$	$B_{1,3}$
	$\{1,3\}$	$x_1x_2(x_3+x_4)$	$\mathcal{B}_{***11}$	$y_3(x_1+x_2+x_4)$	$y_1y_2+(y_1+y_3)x_3$	$B_{3,4}$
	$\{1,4\}$	$(x_1+x_4)x_2x_3$	$\mathcal{B}_{***11}$	$\overline{y_1+y_2}(x_2+x_3+x_4)$	$y_1y_3+\bar{y}_2\bar{x}_4$	$B_{1,4}$
	$\{2\}$	$x_2(x_1+x_3)(x_3+x_4)$	$\mathcal{B}_{***11}$	y_2x_4	$y_1y_2+(y_1+y_3)x_4$	$B_{1,3,4}$

generality, $z_1 = a_0 + a_1y_1 + a_2y_2 + y_3 + a_4z_2$. Write z_2 as y_4. By row operations of f_0 and f_1, we can assume $a_0 = a_1 = a_2 = a_4 = 0$. Then,

$$f_1 = y_3y_4, \tag{31}$$
$$f = y_1y_2y_3 + x_5y_3y_4, \tag{32}$$
$$p_1f = (y_1y_2 + y_4)y_3. \tag{33}$$

Case II: f_1 can be expressed as $z_1z_2 + z_3z_4$ [5]. Without loss of generality, we assume that y_1, y_2, y_3, z_4 are linearly independent. For convenience, write z_4 as y_4. Then, z_1, z_2, z_3 can be expressed as $z_i = a_{i0} + \sum_{j=1}^{4} a_{ij}y_j$, $1 \le i \le 3$. By row operations of z_1z_2 and z_3y_4, $a_{i4} = 0$ for $i = 1$ and 3. If $a_{24} = 1$, then by cross-row operation $z_2 \leftarrow z_2 + y_4$ and $z_3 \leftarrow z_3 + z_1, a_{24} = 0$. By renaming y_1, y_2, y_3, so that $a_{11} = a_{22} = a_{33} = 1$ and by row operations of z_1z_2 again, $a_{12} = 0$, $a_{21} = 0$. From $|f_0f_1|_4 = 2$,

$$|(z_1z_2 + z_3y_4)_{y_1=y_2=y_3=1}|_1 = |(\overline{a_{10} + a_{13}})(\overline{a_{20} + a_{23}}) + (\overline{a_{30} + a_{31} + a_{32}})y_4|_1 = 2,$$
if and only if
$$(\overline{a_{10} + a_{13}})(\overline{a_{20} + a_{23}}) = 1 \quad \text{and} \quad \overline{a_{30} + a_{31} + a_{32}} = 0.$$

By row operations $y_1y_2y_3$ again, $y_1 \leftarrow y_1 + a_{13}\bar{y}_3$, $y_2 \leftarrow y_2 + a_{23}\bar{y}_3$ and $y_3 \leftarrow a_{31}\bar{y}_1 + a_{32}\bar{y}_2 + y_3$, that is, $z_1 = y_1, z_2 = y_2$, and $z_3 = \bar{y}_3$, we have

$$f_1 = y_1y_2 + \bar{y}_3y_4, \tag{34}$$
$$f = y_1y_2(y_3 + x_5) + x_5\bar{y}_3y_4, \tag{35}$$
$$p_1f = (y_1y_2 + y_4)\bar{y}_3. \tag{36}$$

For $y_1y_2y_3 \in \mathrm{RM}_{4,3}(2)$, suppose that there is a codeword 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 $\mathcal{PT}$. Note that y_i with $1 \le i \le 3$ are invariant under the shift, and therefore the binary shift B_{y_2} 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 pairs, 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 and 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 $\overline{y_i + y_j}$ 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 $\sum_{i \in S} g_i$-$\Gamma_{\mathrm{RM}'}$.

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),

$$\mathrm{RM}_{6,3} \subset C \subset \mathrm{RM}_{6,4}. \tag{37}$$

Define

$$\Gamma_{\mathrm{RM}} \triangleq C/\mathrm{RM}_{6,3}. \tag{38}$$

Then, $\dim(\Gamma_{\mathrm{RM}}) = 3$. 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 $w_0 \le w_1$ and $w_0 + w_1 = 8$ for EBCH(64, 45, 8).

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

of Γ_{RM}:

$$\begin{cases} g_1=x_1x_3x_4x_5+(x_1x_4+x_3x_5)x_2x_6, \\ g_2=x_1x_2x_4x_5+[(x_1+x_2)x_3x_4+x_1x_3x_5]x_6, \\ g_3=(x_1+x_2)x_3x_4x_5+x_1[(x_2+x_3)x_4+x_2x_5]x_6. \end{cases} \quad (39)$$

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

Note that

$$\begin{cases} p_0g_1 = x_1x_3x_4x_5, \\ p_0g_2 = x_1x_2x_4x_5, \\ p_0g_3 = (x_1 + x_2)x_3x_4x_5. \end{cases} \quad (40)$$

Since p_0g_1, p_0g_2 and p_0g_3 are linearly independent polynomials of degree 4, $s_1C = s_1\mathrm{RM}_{6,3} = \mathrm{RM}_{5,2}$ and by (15),

$$s_bC = \mathrm{RM}_{5,2}, \text{ for } b \in \{0, 1\}. \quad (41)$$

For $\mathcal{PT} \triangleq C/(s_0C \circ s_1C) = C/(\mathrm{RM}_{5,2} \circ \mathrm{RM}_{5,2})$, $\dim(\mathcal{PT}) = 13$. Each coset of Γ_{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 $(w_0, w_1) \in \mathrm{swp}_{0,1}(C(8))$, $|D_b(w_b)|$ with $b \in \{0, 1\}$ and $|\mathcal{PT}(w_0, w_1)|$ are shown only for $w_0 \le w_1$ in Table 3 because of the symmetry (15).

Since $s_bC = \mathrm{RM}_{5,2}$, $p_1C(0, 8)$ is the set of the minimum weight codewords of $\mathrm{RM}_{5,2}$. The algebraic structure of $C(4, 4) \cap \mathrm{RM}_{6,3}(4, 4)$ can be directly obtained from that of $\mathrm{RM}_{m,r}(2^{m-r-1}, 2^{m-r-1})$ presented in [8, 9]. We analyze the structure of $C(4, 4) \setminus \mathrm{RM}_{6,3}(4, 4)$.

As shown in Table 4, there exists an affine transformation with x_1, x_2, x_3 from g_1-$\mathrm{RM}_{6,3}$ to $\sum_{i\in S} g_i$-$\mathrm{RM}_{6,3}$ with $S \subseteq \{1, 2, 3\}$. Since RM codes are invariant under affine transformations, 7 cosets in $\Gamma_{\mathrm{RM}} \setminus \mathrm{RM}_{6,3}$ 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 $\Gamma_{\mathrm{RM}}(2, 6) \cup \Gamma_{\mathrm{RM}}(4, 4)$. We use the fact that g_1 has the following invariant affine transformations:

$$A_{1,4} \triangleq x_1 \leftrightarrow x_4, A_{3,5} \triangleq x_3 \leftrightarrow x_5, A_{14,35} \triangleq \begin{cases} x_1 \leftrightarrow x_3 \\ x_4 \leftrightarrow x_5, \end{cases} \quad (42)$$

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-$\mathrm{RM}_{6,3}$ to $\sum_{i\in S} g_i$-$\mathrm{RM}_{6,3}$.

S	Affine transformation		
	$x_1 \leftarrow$	$x_2 \leftarrow$	$x_3 \leftarrow$
$\{2\}$	$x_1 + x_2$	x_3	x_1
$\{3\}$	$x_1 + x_2 + x_3$	x_1	$x_1 + x_2$
$\{1, 2\}$	$x_2 + x_3$	$x_1 + x_2$	$x_1 + x_2 + x_3$
$\{1, 3\}$	x_3	$x_1 + x_3$	x_2
$\{2, 3\}$	$x_1 + x_3$	$x_1 + x_2 + x_3$	$x_2 + x_3$
$\{1, 2, 3\}$	x_2	$x_2 + x_3$	$x_1 + x_3$

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-Γ_{RM}. Define

$$\begin{aligned} g_1' &\triangleq g_1 + x_2x_5x_6 \\ &= x_1x_3x_4x_5 + (x_1x_4 + \bar{x}_3x_5)x_2x_6. \end{aligned} \quad (43)$$

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

$$g_1\text{-}\mathcal{PT} = g_1 + (\mathrm{RM}_{5,2} \circ \mathrm{RM}_{5,2}). \quad (44)$$

From Lemma 1-(i), the 16 blocks in g_1-Γ_{RM} can be obtained from the block by applying the binary shifts in $\mathcal{B}_{*1***1}$.

It follows from Table 3, (43) and (44) that for f in g_1-$\mathcal{PT}(2, 6)$, $p_0f = p_0g_1$, and therefore, f can be expressed as $g_1 + x_6h$ with $h \in \mathrm{RM}_{5,2}$. Define $f_0 \triangleq p_0f = x_1x_3x_4x_5$ and

$$f_1 \triangleq (x_1x_4 + x_3x_5)x_2 + h. \quad (45)$$

Then, $p_1f = f_0 + f_1$, and $|f_0|_5 = 2$, and $|f_0 + f_1|_5 = 6$. From (7),

$$|f_0 + f_1|_5 - |f_0|_5 = |f_1|_5 - 2|f_0f_1|_5 = 4, \quad (46)$$

where

$$|f_0f_1|_5 = |f_{1,x_1=x_3=x_4=x_5=1}|_1 = |h_{x_1=x_3=x_4=x_5=1}|_1. \quad (47)$$

If $h = 0$, then from (45) to (47), $|f_1|_5 = 6$, $|f_0f_1|_5 = 0$ and $|f_0 + f_1|_5 = 8$, a contradiction. Hence $|f_1|_5 \ge 4$. Based on the monomial basis of RM codes, we prove that $|f_1|_5 \ge 6$. If $|f_1|_5 = 4$, then f_1 can be expressed as $y_1y_2y_3$, where $y_i = a_{i0} + \sum_{j=1}^{5} a_{ij}x_j$ with $1 \le i \le 3$. Express $y_1y_2y_3$ as the sum of monomials. From (45), f_1 has two monomials of degree 3, $x_1x_2x_4$ and $x_2x_3x_5$, only. Without loss of generality, we can assume that $a_{12} = 1$, $a_{21} = a_{23} = 1$ and $a_{34} = a_{35} = 1$. Then, besides $x_1x_2x_4$ and $x_2x_3x_5$, $y_1y_2y_3$ has monomials $x_2x_3x_4$ and $x_1x_2x_5$, a contradiction. From (46) and $|f_1|_5 \ge 6$, we have $|f_0f_1|_5 \ge 1$. Hence, there remain the following two cases:

Case I: $|f_1|_5 = 6$ and $|f_0f_1|_5 = |h_{x_1=x_3=x_4=x_5=1}|_1 = 1$.

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

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 $x_2(\bar{a}_1\bar{x}_1+\bar{a}_2\bar{x}_3+\bar{a}_4\bar{x}_4+\bar{a}_5\bar{x}_5+1)$. Since $x^a = \bar{x}+a$, $x_1x_4+x_3x_5+h/x_2 = (x_1^{a_4}x_4^{a_1}+x_3^{a_5}x_5^{a_3}+a_1a_4+a_3a_5+1)$. Therefore, $f_1 = B((x_1x_4+x_3x_5)x_2+h)+x_2(a_1a_4+a_3a_5+1)$, 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, $a_1a_4 + a_3a_5 = 1$, which implies

$$B \in \mathcal{B}_{1*01*} \cup \mathcal{B}_{1*110} \cup \mathcal{B}_{0*1*1} \cup \mathcal{B}_{1*101}. \tag{48}$$

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

Next consider Case II.

(i) From the second condition,

$$h_{x_1=x_3=x_4=x_5=1} = 1. \tag{49}$$

A simple example of h which meets the first condition is $h = x_1x_4$ or x_3x_5. Define

$$f_1' \triangleq (x_1x_4 + x_3x_5)x_2 + x_3x_5 = x_2x_1x_4 + \bar{x}_2x_3x_5. \tag{50}$$

Then, $|f_1'|_5 = 8$, $|f_0f_1'|_5 = 2$ and $B_2(f_1') = \bar{x}_2x_1x_4 + x_2x_3x_5 = (x_1x_4 + x_3x_5)x_2 + x_1x_4$ is Case II, too.

(ii) Consider the following type of Case II:

$$f_1 = B(f_1') + h', \qquad \text{for } h' \in \mathrm{RM}_{5,2}, \tag{51}$$

where $B \in \mathcal{B}_{*1***}$ such that

$$B(f_1')_{x_1=x_3=x_4=x_5=1} = 0. \tag{52}$$

From the second condition,

$$h'_{x_1=x_3=x_4=x_5=1} = 1. \tag{53}$$

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

$$f_{1,x_2=0} = x_1^{a_1}x_4^{a_4} + h', \qquad f_{1,x_2=1} = x_3^{a_3}x_5^{a_5} + h'.$$

From (52), the first term is zero, and therefore, $|f_{1,x_2=b}|_4 > 0$. Hence,

$$|f_{1,x_2=b}|_4 = 4, \qquad \text{for } b \in \{0, 1\}, \tag{54}$$

which implies that h' is a single term.

(ii-1) Let $h' = y_1y_2$, 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 $B = B_{1,3}$. Then,

$$\begin{aligned} f_1 &= B_{1,3}(f_1') + x_4x_5 \\ &= x_2\bar{x}_1x_4 + \bar{x}_2\bar{x}_3x_5 + x_4x_5 \\ &= x_2(\bar{x}_1 + x_5)x_4 + \bar{x}_2(\bar{x}_3 + x_4)x_5. \end{aligned} \tag{55}$$

Then, $|f_1|_5 = 8$ and $|f_0f_1|_5 = 2$. 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-$\mathcal{PT}(2, 6)$.

(ii-2) As another example, let $h' = (\bar{x}_1 + x_4)x_5$ and $B = B_{1,3,4}$. Then,

$$\begin{aligned} f_1 &= x_2\bar{x}_1\bar{x}_4 + \bar{x}_2\bar{x}_3x_5 + (\bar{x}_1 + x_4)x_5 \\ &= x_2(x_1 + \bar{x}_4)(\bar{x}_4 + x_5) + \bar{x}_2(x_1 + x_3 + x_4)x_5. \end{aligned} \tag{56}$$

Then, $|f_1|_5 = 8$ and $|f_0f_1|_5 = 2$. By transformations $A_{3,5}$, $A_{14,35}$ and B_2, we have 8 new codewords.

(ii-3) Let $h' = (\bar{x}_1 + x_4)(\bar{x}_3 + x_5)$ and $B = B_{1,3,4,5}$. Then,

$$\begin{aligned} f_1 &= x_2\bar{x}_1\bar{x}_4+\bar{x}_2\bar{x}_3\bar{x}_5+(\bar{x}_1+x_4)(\bar{x}_3+x_5) \\ &= x_2(\bar{x}_1+x_4)(x_1+x_3+x_5)+\bar{x}_2(\bar{x}_3+x_5)(x_1+x_3+x_4). \end{aligned}$$

Then, $|f_1|_5 = 8$ and $|f_0f_1|_5 = 2$. f and $B_2(f)$ are two new codewords of g_1-$\mathcal{PT}(2, 6)$.

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

3.2.3 Structure of $C(4, 4) \setminus \mathrm{RM}_{6,3}$

From Table 3, there are 320 (=2240/7) blocks of $\mathcal{PT}(4, 4)$ in g_1-$\Gamma_{\mathrm{RM}}(4, 4)$, and for a block D in $\mathcal{PT}(4, 4)$, $D = p_0D \circ p_1D$ and $|p_bD| = 2$ with $b \in \{0, 1\}$. For $f \in g_1$-Γ_{RM}, f can be expressed as $f = g_1 + h$, where $h = h_0 + x_6h_1$ with $h_0 \in \mathrm{RM}_{5,3}$ and $h_1 \in \mathrm{RM}_{5,2}$. Suppose that $f \in g_1$-$\Gamma_{\mathrm{RM}}(4, 4)$. Then,

$$w_0(f) = |x_1x_3x_4x_5 + h_0|_5 = 4, \tag{57}$$

$$w_1(f) = |x_1x_3x_4x_5 + (x_1x_4 + x_3x_5)x_2 + h_0 + h_1|_5 = 4. \tag{58}$$

From (57), $w_0(f) = 2+|h_0|_5-2|x_1x_3x_4x_5h_0|_5 = 4$, where $|h_0|_5 \geq 4$ and $0 \leq |x_1x_3x_4x_5h_0|_5 \leq 2$. There are two cases:

Case I: $|h_0|_5 = 4$ and $|h_{0,x_1=x_3=x_4=x_5=1}|_1 = 1$. Then, $h_0 = y_1y_2y_3$. By row operations, only y_3 is dependent on x_2, and $y_{i,x_1=x_3=x_4=x_5=1} = 1$ with $i \in \{1, 2\}$. By row operations, $p_0g_1 = y_1y_2y_4y_5$, and therefore

$$p_0f = y_1y_2(y_4y_5 + y_3). \tag{59}$$

Case II: $|h_0|_5 = 6$ and $|h_{0,x_1=x_3=x_4=x_5=1}|_1 = 2$. Then, $h_0 = z_1(z_2z_3 + z_4z_5)$, and by row and cross operations, only one of z_1 and z_2 depends on x_2. If z_2 dose not depend on x_2, then $h_{0,x_1=x_3=x_4=x_5=1}$ is 0 or x_2+b, where $|h_{0,x_1=x_3=x_4=x_5=1}|_1 = 0$ or 1, a contradiction. Hence, only z_2 depends on x_2. If and only if $z_1 = z_4 = z_5 = 1$ and $z_3 = 0$ at $x_1 = x_3 = x_4 = x_5 = 1$, $|h_{0,x_1=x_3=x_4=x_5=1}|_1 = 2$. By row operations of $p_0g_1 = y_1y_2y_3y_4$, $y_1 = z_1, y_2 = \bar{z}_3, y_3y_4 = z_4z_5$ and therefore,

$$\begin{aligned} p_0f &= y_1y_2y_3y_4 + y_1(z_2\bar{y}_2 + y_3y_4) \\ &= y_1\bar{y}_2(y_3y_4 + z_2). \end{aligned} \tag{60}$$

Next we consider (58). Define

$$h_0' \triangleq (x_1x_4 + x_3x_5)x_2 + h_0 + h_1 \in \mathrm{RM}_{5,3}. \tag{61}$$

Table 5: The 5 representative codewords of g_1-$\mathcal{PT}(2,6)$. The 32 codewords shown in 3.2.2 are $f_0+x_6f_1$, $f_0+x_6B(f_1)$ and $f_0+x_6A(f_1)$, where $f_0=x_1x_3x_4x_5$.

Case	f_1	Binary shift B	Transformation A	Group Size
I	$(x_1x_4+\bar{x}_3x_5)x_2$	$\mathcal{B}_{1*11*}, \mathcal{B}_{1*010}, \mathcal{B}_{0*0*1}, \mathcal{B}_{1*001}$	—	12
II (i)	$x_2x_1x_4+\bar{x}_2x_3x_5$	B_2	—	2
II (ii-1)	$x_2\bar{x}_1x_4+\bar{x}_2\bar{x}_3x_5+x_4x_5$	B_2	$A_{1,4}, A_{3,5}$	8
II (ii-2)	$x_2\bar{x}_1\bar{x}_4+\bar{x}_2\bar{x}_3x_5+(\bar{x}_1+x_4)x_5$	B_2	$A_{3,5}, A_{14,35}$	8
II (ii-3)	$x_2\bar{x}_1\bar{x}_4+\bar{x}_2\bar{x}_3\bar{x}_5+(\bar{x}_1+x_4)(\bar{x}_3+x_5)$	B_2	—	2

It follows from (61) that

$$g_1+h_0'+x_6h_1=B_6(g_1+h_0+x_6h_1)=B_6(f). \quad (62)$$

Since $h_1\in \mathrm{RM}_{5,2}$, $h_0'\neq h_0$, and therefore,

$$p_0f\neq p_1f. \quad (63)$$

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$'$: $h_0=y_1y_2x_2$ such that $y_1y_{2\,x_1=x_3=x_4=x_5=1}=1$. Since $h_0' = x_2(x_1x_4+x_3x_5+y_1y_2)+h_1$, h_0' is not Case II and if h_0' meets (58), then it is a Case I$'$ and $x_1x_4+x_3x_5+y_1y_2$ is reduced to a single term, say, $y_1y_2=x_1x_4, x_3x_5, (x_1+x_3+1)x_4,\ldots$ The number of those minimum weight codewords of $\mathrm{RM}_{4,2}$ which are one at $x_1=x_3=x_4=x_5=1$ is $\prod_{i=0}^{1}(2^{4-i}-1)/(2^2-1)=35$. We have found that for 20 y_1y_2's among the 35 codewords,

$$h_0'=(x_1x_4+x_3x_5+y_1y_2)x_2+h_1 \quad (64)$$

are Case I$'$. Table 6 lists the 10 y_1y_2's and the related h_1/x_2 and h_0'/x_2. Define $G_\phi \triangleq \{g_1+h_0+x_6h_1 = x_1x_3x_4x_5+h_0+x_2(x_1x_4+x_3x_5)x_6+x_6h_1$: h_0/x_2 and h_1/x_2 are listed in Table 6$\}$. G_ϕ consists of 10 codewords in g_1-$\Gamma_{\mathrm{RM}}(4,4)$. The 10 codewords corresponding found 10 remaining y_1y_2's can be obtained from those in G_ϕ by the binary shift B_6. Note that for any nonempty subset X of $\{x_i: 1\le i\le 6\}$, there are no binary shift equivalent pairs with respect to X in G_ϕ. For $f\in G_\phi$, $\deg_2(f)=2$. From Lemma 1-(ii), $f, B_2(f), B_2^{(0)}(f)$ and $B_2^{(1)}(f)$ are in the same block of $\mathcal{PT}(4,4)$ in g_1-Γ_{RM}, and they are all different. f is called the representative of the block. Note that for $f\in G_\phi$, the term of degree 4 is the same as $x_1x_3x_4x_5$. For each of the 32 subsets S of $\{1,3,4,5,6\}$ and $f\in G_\phi$, it follows from Lemma 1-(i) and (63) that

$$B_S(f)\in g_1\text{-}\Gamma_{\mathrm{RM}}(4,4). \quad (65)$$

For $S\subseteq\{1,3,4,5,6\}$, define $G_S\triangleq\{B_S(f): f\in G_\phi\}$. Then, the 320 blocks of $\mathcal{PT}(4,4)$ in g_1-$\Gamma_{\mathrm{RM}}(4,4)$ are

$$\{f, B_2(f), B_2^{(0)}(f), B_2^{(1)}(f)\} \quad \text{for} \quad f\in \bigcup_{S\subseteq\{1,3,4,5,6\}} G_S. \quad (66)$$

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

h_0/x_2	h_1/x_2	h_0'/x_2
$(\bar{x}_1+x_5)x_3$	x_1+x_3	$x_1(\bar{x}_3+x_4)$
$(x_1+x_4+x_5)x_3$	$\bar{x}_1+x_3+x_4$	$(\bar{x}_1+x_4)(\bar{x}_3+x_4)$
$(\bar{x}_1+x_5)(\bar{x}_3+x_5)$	$\bar{x}_1+x_3+x_5$	$x_1(x_3+x_4+x_5)$
$(x_1+x_4+x_5)(\bar{x}_3+x_5)$	$x_1+x_3+x_4+x_5$	$(\bar{x}_1+x_4)(x_3+x_4+x_5)$
x_1x_4	0	x_3x_5
$(\bar{x}_1+x_3)x_4$	x_3+x_4	$x_3(\bar{x}_4+x_5)$
$(\bar{x}_1+x_5)x_4$	x_4+x_5	$(\bar{x}_3+x_4)x_5$
$(x_1+x_3+x_5)x_4$	$\bar{x}_3+x_4+x_5$	$(\bar{x}_3+x_5)(\bar{x}_4+x_5)$
$x_1(\bar{x}_4+x_5)$	x_1+x_5	$(\bar{x}_1+x_3)x_5$
$(\bar{x}_1+x_5)(\bar{x}_4+x_5)$	$\bar{x}_1+x_4+x_5$	$(x_1+x_3+x_4)x_5$

4 Conclusion

For two EBCH codes, EBCH(32, 21, 6) and EBCH(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 EBCH(32, 21, 6) is smaller than that of the RM code $\mathrm{RM}_{5,2}$, while that of EBCH(64, 45, 8) is equal to the RM code $\mathrm{RM}_{6,3}$.

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

[1] J. Asatani, T. Koumoto, T. Fujiwara and T. Kasami, "Soft-input soft-output decoding algorithm of linear block codes based on minimum distance search," Proc. 2004 IEEE International Symposium on Information Theory, p. 345, Chicago, USA, June 2004.

[2] T. Kasami, T. Takata, T. Fujiwara and S. Lin, "On complexity of trellis structure of linear block codes," IEEE Trans. Inform. Theory, vol. 39, no. 3, pp. 1057–1064, May 1993.

[3] T. Kasami, T. Koumoto, T. Fujiwara, H. Yamamoto and S. Lin, "Low weight subtrellises for binary linear block codes and their applications," IEICE Trans. Fundamentals, vol. E80-A, no. 11, pp. 2095–2103, Nov. 1997.

[4] T. Fujiwara, H. Yamamoto, T. Kasami, and S. Lin, "A trellis-based recursive maximum likelihood decoding algorithm for lenear block codes," IEEE Trans. Inform. Theory, vol. 44, no. 2, pp. 714–729, Mar. 1998.

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

[6] W.W. Peterson and E.J. Weldon, Jr., Error-Correcting Codes, 2nd ed., MIT Press, Cambridge, 1972.

[7] T. Kasami, H. Tokushige, T. Fujiwara, H. Yamamoto and S. Lin, "A recursive maximum likelihood decoding algorithm for some transitive invariant binary block codes," IEICE Trans. Fundamentals, vol. E81-A, no. 11, pp. 1916–1924, Sept. 1998.

[8] T. Kasami, H. Tokushige, T. Fujiwara, H. Yamamoto and S. Lin, "A recursive maximum likelihood decoding algorithm for Reed-Muller codes and related codes," Nara Institute of Science and Technology Technical Report, NAIST-IS-TR97003, May 1997.

[9] J. Asatani, K. Tomita, T. Koumoto, T. Takata and T. Kasami, "A soft-decision iterative decoding algorithm using a top-down and recursive minimum distance search," IEICE Trans. Fundamentals, vol. E85-A, no. 10, pp. 2220–2228, Oct. 2002.