The 29th Symposium on Information Theory
and its Applications (SITA2006)
Hakodate, Hokkaido, Japan, Nov. 28 – Dec. 1, 2006

Correctable Errors of Weight Half the Minimum Distance for the First-Order Reed-Muller Codes

Kenji Yasunaga * Toru Fujiwara *

Abstract— The number of correctable errors of weight half the minimum distance is given for the first-order binary Reed-Muller codes. It is shown that the size of trial set, which is introduced by Helleseth et al. and can be used for a minimum distance decoding or estimating the number of uncorrectable errors, for the first-order Reed-Muller codes is at least that of minimal codewords except for small code length.

Keywords— Error-correction capability, trial set, first-order Reed-Muller codes.

1 Introduction

In syndrome decoding, coset leaders of a code are the correctable error vectors. If a minimum weight vector is taken as the coset leader in each coset, the syndrome decoding performs maximum likelihood decoding over a binary symmetric channel. When there are two or more minimum weight vectors in a coset, we have choices of the coset leader. If the lexicographically smallest minimum weight vector is taken as the coset leader, then both the correctable errors and the uncorrectable errors have a monotone structure. That is, when $\boldsymbol{y}$ covers $\boldsymbol{x}$ ($x_i \leq y_i$ for all i), if $\boldsymbol{y}$ is correctable, then $\boldsymbol{x}$ is also correctable, and if $\boldsymbol{x}$ is uncorrectable, then $\boldsymbol{y}$ is also uncorrectable. Using this structure, Zémor showed that the residual error probability after maximum likelihood decoding displays a threshold behavior [2], and Helleseth et al. introduced *trial sets* for a code [1]. A trial set for a code can be used for a minimum distance decoding and for improving an upper bound on the number of uncorrectable errors. They introduced a notion *larger halves* of a codeword. Larger halves of a codeword $\boldsymbol{c}$ are minimal vectors $\boldsymbol{v}$ with respect to covering such that $\boldsymbol{v} + \boldsymbol{c} \prec \boldsymbol{v}$, where $\boldsymbol{v} \prec \boldsymbol{u}$ means the Hamming weight of $\boldsymbol{v}$ is smaller than that of $\boldsymbol{u}$ or the Hamming weights of $\boldsymbol{v}$ and $\boldsymbol{u}$ are equal but $\boldsymbol{v}$ is lexicographically smaller than $\boldsymbol{u}$. Trial sets for a code is the set of codewords whose larger halves contain all minimal uncorrectable errors. The code itself and the set of minimal codewords [3] in the code are examples of trial sets.

In this paper, we investigate trial sets for the first-order Reed-Muller codes. Let RM_m denote the first-order Reed-Muller code of length 2^m. We show that, except for small m, trial sets for RM_m must contain all codewords with weight 2^{m-1}, which is equivalent to the set of minimal codewords in RM_m. RM_m is a $(2^m, m+1, 2^{m-1})$ code and has only three types of weights, 0, 2^{m-1}, and 2^m. Hence, all codewords except $\mathbf{0}$ and $\mathbf{1}$ have the minimum weight 2^{m-1}. We observe the fact that all uncorrectable errors of weight half the minimum distance are minimal uncorrectable errors, and they are larger halves of codewords with weight 2^{m-1}. We show that, except for small m, all codewords with weight 2^{m-1} are necessary for forming minimal uncorrectable errors with weight 2^{m-2} as larger halves of them. In the process of deriving this result, we determine the number of correctable errors of weight half the minimum distance for RM_m.

2 Monotone structure of errors and trial sets

2.1 Definitions and properties

Let $\mathbf{F}^n$ be the set of all binary vectors of length n. Let $C \subseteq \mathbf{F}^n$ be an (n, k, d) binary linear code. $\mathbf{F}^n$ is partitioned into 2^{n-k} cosets $C_1, C_2, C_3, \ldots, C_{2^{n-k}}$;

$$\mathbf{F}^n = \bigcup_{i=1}^{2^{n-k}} C_i, \quad C_i \cap C_j = \emptyset \text{ for } i \neq j,$$

where each $C_i = \{\boldsymbol{v}_i + \boldsymbol{c} : \boldsymbol{c} \in C\}$ with $\boldsymbol{v}_i \in \mathbf{F}^n$. $\boldsymbol{v}_i$ is called the coset leader of the coset. $\boldsymbol{v}_i$ can be taken from any element in the coset. Let H be a parity check matrix of C. The syndrome of a vector $\boldsymbol{v} \in \mathbf{F}^n$ is defined as $\boldsymbol{v}H^T$. The syndromes of the vectors in the same coset are the same. Syndrome decoding associates an error vector to each syndrome. The syndrome decoder presumes that the error vector added to the received vector $\boldsymbol{y}$ is the coset leader of the coset which contains $\boldsymbol{y}$. The syndrome decoding function $D : \mathbf{F}^n \to C$ is defined as

$$D(\boldsymbol{y}) = \boldsymbol{y} + \boldsymbol{v}_i, \quad \text{if } \boldsymbol{y} \in C_i.$$

If the coset leader is taken as a minimum weight vector in the coset, the syndrome decoding performs maximum likelihood (minimum distance or complete) decoding over a binary symmetric channel under the condition all codewords are equally likely to be transmitted. Let $\preceq$ denote a linear ordering such that

$$\boldsymbol{x} \preceq \boldsymbol{y} \text{ if and only if } \begin{cases} \|\boldsymbol{x}\| < \|\boldsymbol{y}\|, & \text{or} \\ \|\boldsymbol{x}\| = \|\boldsymbol{y}\| \text{ and } v(\boldsymbol{x}) \leq v(\boldsymbol{y}), \end{cases}$$

where $\|\boldsymbol{x}\|$ denotes the Hamming weight of a vector $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$ and $v(\boldsymbol{x})$ denotes the numerical value of $\boldsymbol{x}$: $v(\boldsymbol{x}) = \sum_{i=1}^{n} x_i 2^{n-i}$. We write $\boldsymbol{x} \prec \boldsymbol{y}$ if $\boldsymbol{x} \preceq \boldsymbol{y}$ and $\boldsymbol{x} \neq \boldsymbol{y}$. Let $\boldsymbol{z}_i$ be the minimum element in the coset C_i with respect to the ordering $\preceq$. We choose

* Graduate School of Information Science and Technology, Osaka University, 1-5 Yamadaoka, Suita, Osaka 565-0871, Japan. E-mail: {k-yasunaga, fujiwara}@ist.osaka-u.ac.jp

$\boldsymbol{z}_i$ as the coset leader of the coset C_i throughout this paper. Let $E^0(C)$ be the set of all coset leaders of C. In the syndrome decoding, $E^0(C)$ becomes the set of correctable errors and $E^1(C) = \mathbf{F}^n \setminus E^0(C)$ becomes the set of uncorrectable errors. Both $E^0(C)$ and $E^1(C)$ have a monotone structure. Let $\subseteq$ denote a partial ordering called "covering" such that:

$$\boldsymbol{x} \subseteq \boldsymbol{y} \text{ if and only if } S(\boldsymbol{x}) \subseteq S(\boldsymbol{y}),$$

where $S(\boldsymbol{v}) = \{i : v_i \neq 0\}$ is the support set of $\boldsymbol{v} = (v_1, v_2, \dots, v_n)$. Consider $\boldsymbol{x}$ and $\boldsymbol{y}$ with $\boldsymbol{x} \subseteq \boldsymbol{y}$. If $\boldsymbol{y}$ is a correctable error, then $\boldsymbol{x}$ is also correctable. If $\boldsymbol{x}$ is uncorrectable, then $\boldsymbol{y}$ is also uncorrectable. This monotone structure is well-known (see [4, Theorem 3.11]). Using this structure, Zémor showed that the residual error probability after maximum likelihood decoding displays a threshold behavior [2].

Helleseth et al. have studied this structure and introduced some notions [1]. They proposed a minimum distance decoding, which we call *trial set decoding*. A trial set $T \subseteq C$ of the code C is defined as the set of codewords in C that has the following property:

$$\boldsymbol{y} \in E^0(C) \text{ if and only if } \boldsymbol{y} \prec \boldsymbol{y} + \boldsymbol{c} \text{ for all } \boldsymbol{c} \in T.$$

Equivalently,

$$\boldsymbol{y} \in E^1(C) \text{ if and only if } \boldsymbol{y} + \boldsymbol{c} \prec \boldsymbol{y} \text{ for some } \boldsymbol{c} \in T.$$

The trial set decoding for a received vector $\boldsymbol{y} \in \mathbf{F}^n$ is as follows:

1. $\boldsymbol{e} \leftarrow \boldsymbol{y}$.
2. Find a codeword $\boldsymbol{c} \in T$ such that $\boldsymbol{e} + \boldsymbol{c} \prec \boldsymbol{e}$. $\boldsymbol{e} \leftarrow \boldsymbol{e} + \boldsymbol{c}$.
3. Repeat Step 2 until no such $\boldsymbol{c}$ is found.
4. Output $\boldsymbol{e} + \boldsymbol{y}$.

The trial set decoding is a type of gradient-like decoding [5]. Estimating the complexity of the trial set decoding is an open problem. The complexity of trial set decoding seems to depend on the size of a trial set used in the algorithm. Therefore, we consider the smallest trial set. Define a *minimum* trial set for C as the smallest trial set for C, denoted by $T_{\min}$. We should note that, though the size of $T_{\min}$ for C is unique, $T_{\min}$ may not be unique. We show some new results for the size of minimum trial sets in Section 2.2. To describe a necessary and sufficient condition for a set to be a trial set, we need to introduce *minimal uncorrectable errors* and *larger halves* of codewords.

Since the set of uncorrectable errors $E^1(C)$ has a monotone structure, $E^1(C)$ can be characterized by *minimal uncorrectable errors* in $E^1(C)$. An uncorrectable error $\boldsymbol{y} \in E^1(C)$ is minimal if there is no $\boldsymbol{x}$ such that $\boldsymbol{x} \subseteq \boldsymbol{y}$ in $E^1(C) \setminus \{\boldsymbol{y}\}$. We denote by $M^1(C)$ the set of all minimal uncorrectable errors in C. Next, we introduce *larger halves* of a codeword. Larger halves of a codeword $\boldsymbol{c} \in C$ are minimal vectors $\boldsymbol{v}$ with respect to covering such that $\boldsymbol{v} + \boldsymbol{c} \prec \boldsymbol{v}$. The following condition is a necessary and sufficient condition that $\boldsymbol{v} \in \mathbf{F}^n$ is a larger half of $\boldsymbol{c} \in C$:

$$\boldsymbol{v} \subseteq \boldsymbol{c}, \tag{1}$$

$$\|\boldsymbol{c}\| \leq 2\|\boldsymbol{v}\| \leq \|\boldsymbol{c}\| + 2, \tag{2}$$

$$m(\boldsymbol{v}) \triangleq \min S(\boldsymbol{v}) \begin{cases} = m(\boldsymbol{c}) & \text{if } 2\|\boldsymbol{v}\| = \|\boldsymbol{c}\|, \\ > m(\boldsymbol{c}) & \text{if } 2\|\boldsymbol{v}\| = \|\boldsymbol{c}\| + 2. \end{cases} \tag{3}$$

The proof of equivalence between the definition and the above condition is found in the proof of Theorem 1 of [1]. Let $L(\boldsymbol{c})$ be the set of all larger halves of $\boldsymbol{c} \in C$. For a set U of codewords, let $L(U) = \bigcup_{\boldsymbol{c} \in U \setminus \{\mathbf{0}\}} L(\boldsymbol{c})$. A necessary and sufficient condition for a set to be a trial set is as follows:

Theorem 1 ([1, Corollary 3])**.** *For a linear code C and $T \subseteq C \setminus \{\mathbf{0}\}$, T is a trial set for C if and only if $M^1(C) \subseteq L(T)$.*

A codeword $\boldsymbol{c}$ is called *minimal* if $\boldsymbol{v} \subset \boldsymbol{c}$ for $\boldsymbol{v} \in C$ implies $\boldsymbol{v} = \mathbf{0}$. Let $M(C)$ be the set of all minimal codewords in C. The following corollary shows that a minimum trial set for C should consist of minimal codewords in C.

Corollary 1 ([1, Corollary 5])**.** *For a linear code C with $d > 1$, if T is a trial set for C, then $T \cap M(C)$ is also a trial set for C.*

Let

$$E_i^1(C) = \{\boldsymbol{v} \in E^1(C) : \|\boldsymbol{v}\| = i\},$$

and, for $U \subseteq C$,

$$A_i(U) = \{\boldsymbol{c} \in U : \|\boldsymbol{c}\| = i\}.$$

A trial set for a code C can be used for giving an upper bound on $|E_i^1(C)|$.

Corollary 2 ([1, Corollary 7])**.** *Let T be a trial set for a linear code C. For i with $\lfloor (d-1)/2 \rfloor < i \leq n$,*

$$|E_i^1(C)| \leq \sum_{j=i}^{2i} |A_j(T)| \sum_{l=\lceil j/2 \rceil} \binom{j}{l}\binom{n-j}{i-l} - \sum_{l=\lceil d/2 \rceil}^{i} |A_{2l}(T)| \binom{2l-1}{l}\binom{n-2l}{i-l}.$$

This bound becomes tight if a given trial set is small.

2.2 New results on the size of trial sets

We give some results on the size of $T_{\min}$ and $M^1(C)$.

Corollary 3. *For an (n, k, d) linear code C with $d > 1$, let $T_{\min}$ be a minimum trial set for C. Then*

$$k \leq |T_{\min}| \leq \min\{|M^1(C)|, |M(C)|\}.$$

Proof. When a codeword $\boldsymbol{c} \in C$ is sent as an input to a trial set decoder, the decoder outputs $\mathbf{0}$ since the coset leader of the coset C is $\mathbf{0}$. The output of the decoder is a sum of the codewords in $T_{\min}$ and the input. Therefore, for any $\boldsymbol{c} \in C$, $\boldsymbol{c} + \sum_i \boldsymbol{c}_i = \mathbf{0}$ for $\boldsymbol{c}_i \in T_{\min}$. Thus, the linear span of a trial set forms the code C. This leads to $k \leq |T_{\min}|$. $|T_{\min}| \leq |M(C)|$

is derived from Corollary 1. For each $\boldsymbol{c} \in T_{\min}$, there is at least one vector $\boldsymbol{v}$ such that $\boldsymbol{v} \in L(\boldsymbol{c})$ but $\boldsymbol{v} \notin L(\boldsymbol{c}')$ for any $\boldsymbol{c}' \in T_{\min} \setminus \{\boldsymbol{c}\}$. This is because, if some codeword $\boldsymbol{c}'' \in T_{\min}$ does not meet the above, $\boldsymbol{c}''$ can be eliminated, and then $T_{\min} \setminus \{\boldsymbol{c}''\}$ forms a trial set. This contradicts the definition of minimum trial set. Hence, $|T_{\min}| \le |M^1(C)|$. □

The bound $|M^1(C)|$ is tight when the code rate k/n of C is high, and $|M(C)|$ is tight when the code rate is low. We have the following fact regarding $M^1(C)$.

Corollary 4 ([1, Corollary 1])**.** *For a linear code C with $d > 1$, $M^1(C) \subseteq L(M(C))$.*

For $\boldsymbol{y} \in \mathbf{F}^n$, let $H(\boldsymbol{y}) = \{\boldsymbol{c} \in C : \boldsymbol{y} + \boldsymbol{c} \prec \boldsymbol{y}\}$. Note that if $\boldsymbol{y} \in L(\boldsymbol{c})$ for some $\boldsymbol{c} \in C$, then $\boldsymbol{y} \in E^1(C)$ and $\boldsymbol{c} \in H(\boldsymbol{y})$. For a linear code C with $d > 1$ and a minimal uncorrectable error $\boldsymbol{y}$ in C, $H(\boldsymbol{y}) \subseteq M(C)$ from [1, Theorem 1]. Thus, larger halves of non-minimal codeword cannot be minimal uncorrectable errors. From the above fact and Corollary 4, we have the following.

Corollary 5. *For a linear code C with $d > 1$, $M^1(C) \subseteq L(M(C)) \setminus L(C \setminus M(C)) \subseteq L(M(C))$.*

3 Trial sets of the first-order Reed-Muller codes

From Theorem 1, for a trial set $T \subseteq C$ for a code C, $L(T)$ contains all minimal uncorrectable errors in C. We show that, except for small code length, all codewords with weight 2^{m-1} in the first-order Reed-Muller codes RM_m are necessary for forming minimal uncorrectable errors with weight 2^{m-2} as larger halves of them. In the process of deriving this result, we determine the number of correctable errors of weight half the minimum distance for RM_m for all m.

RM_m is defined recursively as

$$\mathrm{RM}_0 = \{\mathbf{0}, \mathbf{1}\}, \tag{4}$$

$$\mathrm{RM}_{m+1} = \bigcup_{\boldsymbol{c} \in \mathrm{RM}_m} \{\boldsymbol{c} \circ \boldsymbol{c}, \boldsymbol{c} \circ \overline{\boldsymbol{c}}\}, \tag{5}$$

where $\boldsymbol{u} \circ \boldsymbol{v}$ denotes the concatenation of $\boldsymbol{u}$ and $\boldsymbol{v}$, and $\overline{\boldsymbol{v}} \triangleq \mathbf{1} + \boldsymbol{v}$. Since all codewords in RM_m except for $\mathbf{0}, \mathbf{1}$ are minimum weight codewords, $M(\mathrm{RM}_m) = \mathrm{RM}_m \setminus \{\mathbf{0}, \mathbf{1}\}$. Henceforth we denote $\mathrm{RM}_m \setminus \{\mathbf{0}, \mathbf{1}\}$ by RM_m^*.

The weight of all codewords in RM_m^* is 2^{m-1}. Thus, the weights of their larger halves are 2^{m-2} and $2^{m-2}+1$ from the condition (2). $\boldsymbol{v} \in E^1_{2^{m-2}}(\mathrm{RM}_m)$ must be in $M^1(\mathrm{RM}_m)$ because 2^{m-2} is the smallest weight in $E^1(\mathrm{RM}_m)$, and therefore $\boldsymbol{v}$ cannot cover any other uncorrectable error. $\boldsymbol{v} \in E^1_{2^{m-2}}(\mathrm{RM}_m)$ is a larger half of some codeword in a trial set for RM_m from Theorem 1. Therefore, we focus on the larger halves of weight 2^{m-2}. For an even weight codeword $\boldsymbol{c}$, let $\tilde{L}(\boldsymbol{c})$ denote the set of larger halves of $\boldsymbol{c}$ having the smaller weight. From the conditions (1)–(3) for larger half,

$$|\tilde{L}(\boldsymbol{c})| = \binom{2^{m-1}-1}{2^{m-2}-1} \tag{6}$$

for each $\boldsymbol{c} \in \mathrm{RM}_m^*$. There may be some $\boldsymbol{v} \in E^1_{2^{m-2}}(\mathrm{RM}_m)$ that is a larger half of two or more codewords in RM_m^*. Let

$$D_m^i = \{\boldsymbol{v} \in \mathbf{F}^n : |\{\boldsymbol{c} \in \mathrm{RM}_m^* : \boldsymbol{v} \in \tilde{L}(\boldsymbol{c})\}| = i\}.$$

That is, D_m^i is the set of all uncorrectable errors $\boldsymbol{v}$ with weight 2^{m-2} such that $\boldsymbol{v}$ is a common larger half among i codewords in RM_m^*. Then

$$|E^1_{2^{m-2}}(\mathrm{RM}_m)| = \sum_i |D_m^i|. \tag{7}$$

We show that four or more codewords in RM_m^* cannot have a common larger half of weight 2^{m-2}.

Lemma 1. *$D_m^i = \emptyset$ for $m > 1, i > 3$.*

Proof. Assume that there are four codewords $\boldsymbol{c}_i \in \mathrm{RM}_m^*$ $(1 \le i \le 4)$ such that $\boldsymbol{v} \in \tilde{L}(\boldsymbol{c}_i)$ for each i for some $\boldsymbol{v} \in \mathbf{F}^n$. Then, from the condition (1), $\boldsymbol{v} \subseteq \boldsymbol{c}_i$ for $1 \le i \le 4$. Thus, $|S(\boldsymbol{c}_i) \setminus S(\boldsymbol{v})| = 2^{m-2}$ for $1 \le i \le 4$. Since $S(\boldsymbol{c}_i) \setminus S(\boldsymbol{v}) \subset \{1, 2, \dots, n\} \setminus S(\boldsymbol{v})$ for $1 \le i \le 4$ and $|\{1, 2, \dots, n\} \setminus S(\boldsymbol{v})| = 3 \cdot 2^{m-2}$, there are two codeword (say $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$) such that $(S(\boldsymbol{c}_1) \setminus S(\boldsymbol{v})) \cap (S(\boldsymbol{c}_2) \setminus S(\boldsymbol{v})) \ne \emptyset$. Then $|S(\boldsymbol{c}_1) \cap S(\boldsymbol{c}_2)| = |S(\boldsymbol{v})| + |(S(\boldsymbol{c}_1) \setminus S(\boldsymbol{v})) \cap (S(\boldsymbol{c}_2) \setminus S(\boldsymbol{v}))| > 2^{m-2}$. Hence, for the codeword $\boldsymbol{c}_1 + \boldsymbol{c}_2$, $\|\boldsymbol{c}_1 + \boldsymbol{c}_2\| = |S(\boldsymbol{c}_1 + \boldsymbol{c}_2)| < 2^{m-1}$. This contradicts the property of RM_m. □

Corollary 6. *For $m > 1$,*

$$|E^1_{2^{m-2}}(\mathrm{RM}_m)| = |D_m^1| + |D_m^2| + |D_m^3|, \tag{8}$$

$$2(2^m - 1)\binom{2^{m-1}-1}{2^{m-2}-1} = |D_m^1| + 2|D_m^2| + 3|D_m^3|. \tag{9}$$

Proof. (8) is from (7) and Lemma 1. The left-hand side of (9) is the product of $|\mathrm{RM}_m^*| = 2^{m+1} - 2$ and $|\tilde{L}(\boldsymbol{c})|$ for each $\boldsymbol{c} \in \mathrm{RM}_m^*$. This value is equal to the right-hand side from Lemma 1. □

Next, we determine $|D_m^2|$ and $|D_m^3|$. Then $|D_m^1|$ and $|E^1_{2^{m-2}}(\mathrm{RM}_m)|$ can be determined from (8) and (9).

Let $S_m = \{m(\boldsymbol{c}) : \boldsymbol{c} \in \mathrm{RM}_m\}$. Then, from the definition of RM_m, S_m can be also defined recursively as $S_0 = \{1\}$, $S_{m+1} = S_m \cup \{2^{m-1} + 1\}$. We define the set $C_m(i) \subset \mathrm{RM}_m^*$ for $i \in S_m$ as follows:

$$C_m(i) = \{\boldsymbol{c} \in \mathrm{RM}_m^* : m(\boldsymbol{c}) = i\}.$$

Then $\mathrm{RM}_m^* = \sum_{i \in S_m} C_m(i)$. From the definition of RM_m, $C_m(i)$ is also defined recursively as

$$C_0(1) = \{\mathbf{1}\}, \tag{10}$$

$$C_{m+1}(1) = \{\boldsymbol{c} \circ \boldsymbol{c}, \boldsymbol{c} \circ \overline{\boldsymbol{c}} : \boldsymbol{c} \in C_m(1)\} \cup \{\mathbf{1} \circ \mathbf{0}\}, \tag{11}$$

$$C_{m+1}(2^{m-1} + 1) = \{\mathbf{0} \circ \mathbf{1}\}, \tag{12}$$

$$C_{m+1}(i) = \{\boldsymbol{c} \circ \boldsymbol{c}, \boldsymbol{c} \circ \overline{\boldsymbol{c}} : \boldsymbol{c} \in C_m(i)\} \text{ for } i > 1. \tag{13}$$

Lemma 2. *Let $\boldsymbol{c}_1, \boldsymbol{c}_2 (\ne \boldsymbol{c}_1) \in C_m(i)$ for $i \in S_m \setminus \{2^{m-2} + 1\}$. For $m > 1$,*

$$|S(\boldsymbol{c}_1) \cap S(\boldsymbol{c}_2)| = |S(\boldsymbol{c}_1) \cap S(\overline{\boldsymbol{c}_2})| = 2^{m-2}.$$

Proof. We show the statement by induction on m. For $m = 2$, $C_2(1) = \{1100, 1010, 1001\}$, $C_2(2) = \{0110, 0101\}$. We can confirm the statement is satisfied for $m = 2$. Let assume $|S(\boldsymbol{c}_1) \cap S(\boldsymbol{c}_2)| = |S(\boldsymbol{c}_1) \cap S(\overline{\boldsymbol{c}_2})| = 2^{m-2}$ for $\boldsymbol{c}_1, \boldsymbol{c}_2 \in C_m(i)$. The codewords in $C_{m+1}(i)$ for $i \neq 1$ is of the form of $\boldsymbol{c} \circ \boldsymbol{c}$ or $\boldsymbol{c} \circ \overline{\boldsymbol{c}}$ for $\boldsymbol{c} \in C_m(i)$ from (10)–(13). $|S(\boldsymbol{c}_1 \circ \boldsymbol{c}_1) \cap S(\boldsymbol{c}_2 \circ \boldsymbol{c}_2)| = 2 \cdot |S(\boldsymbol{c}_1) \cap S(\boldsymbol{c}_2)| = 2^{(m+1)-2}$ and $|S(\boldsymbol{c}_1 \circ \boldsymbol{c}_1) \cap S(\boldsymbol{c}_2 \circ \overline{\boldsymbol{c}_2})| = |S(\boldsymbol{c}_1) \cap S(\boldsymbol{c}_2)| + |S(\boldsymbol{c}_1) \cap S(\overline{\boldsymbol{c}_2})| = 2^{(m+1)-2}$ from the assumption. $|S(\boldsymbol{c}_1 \circ \boldsymbol{c}_1) \cap S(\boldsymbol{c}_1 \circ \overline{\boldsymbol{c}_1})| = |S(\boldsymbol{c}_1)| = \|\boldsymbol{c}_1\| = 2^{(m+1)-2}$. The codewords in $C_{m+1}(1)$ is of the form of $\boldsymbol{c} \circ \boldsymbol{c}$, $\boldsymbol{c} \circ \overline{\boldsymbol{c}}$, or $\mathbf{1} \circ \mathbf{0}$ for $\boldsymbol{c}, \mathbf{1}, \mathbf{0} \in C_m(i)$. $|S(\boldsymbol{c}_1 \circ \boldsymbol{c}_1) \cap S(\mathbf{1} \circ \mathbf{0})| = |S(\boldsymbol{c}_1 \circ \overline{\boldsymbol{c}_1}) \cap S(\mathbf{1} \circ \mathbf{0})| = |S(\boldsymbol{c}_1)| = \|\boldsymbol{c}_1\| = 2^{(m+1)-2}$. Thus, the statement is satisfied for $m + 1$. □

Lemma 3. *For $m > 1$,*

$$|D_m^2| = \sum_{i \in S_m \setminus \{1, 2^{m-1}+1\}} \frac{|C_m(i)|(|C_m(i)| - 1)}{2}, \qquad (14)$$

$$|D_m^3| = \frac{|C_m(1)|(|C_m(1)| - 1)}{6}. \qquad (15)$$

Proof. For $\boldsymbol{c}_1, \boldsymbol{c}_2 (\neq \boldsymbol{c}_1) \in C_m(i)$, $|S(\boldsymbol{c}_1) \cap S(\boldsymbol{c}_2)| = 2^{m-2}$ from Lemma 2, and $S(\boldsymbol{c}_1) \cap S(\boldsymbol{c}_2)$ contains i. Therefore, the vector $\boldsymbol{v}$ whose support set is $S(\boldsymbol{c}_1) \cap S(\boldsymbol{c}_2)$ is a larger half of both $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$. For the case of $i = 1$, $\boldsymbol{v}$ is also a larger half of the codeword of $\overline{\boldsymbol{c}_1 + \boldsymbol{c}_2}$ since $\overline{\boldsymbol{c}_1 + \boldsymbol{c}_2} \in C_m(1)$ and $S(\boldsymbol{c}_1) \cap S(\boldsymbol{c}_2) \subset S(\overline{\boldsymbol{c}_1 + \boldsymbol{c}_2})$. For the case of $i \neq 1, 2^{m-1}+1$, there is no other codeword $\boldsymbol{c} \in C_m(i) \backslash \{\boldsymbol{c}_1, \boldsymbol{c}_2\}$ such that $\boldsymbol{v} \in \tilde{L}(\boldsymbol{c})$. This can be shown by a similar argument of the proof of Lemma 1. For the case of $i = 2^{m-1} + 1$, there is only one codeword in $C_m(i)$. From above, for each codeword in $C_m(1)$, there are two other codewords such that those three have the common larger half. For each codeword in $C_m(i)$ for $i \neq 1, 2^{m-1}+1$, there is one other codeword such that those two have the common larger half. Hence, the statements follow. □

Corollary 7. *For $m > 1$,*

$$|D_m^2| = |D_m^3| = \frac{(2^m - 1)(2^m - 2)}{6}.$$

Proof. From (10) and (11), $|C_m(1)| = 2^{m-1}$. Hence, $|D_m^3| = (2^m - 1)(2^m - 2)/6$ from (15). From (12) and (13), $|C_m(i)| = 2^{m-m'}$ for $i = 2^{m'-1}$. Thus, from (14),

$$\begin{aligned} |D_m^2| &= \frac{1}{2} \sum_{m'=1}^{m} 2^{m-m'}(2^{m-m'} - 1) \\ &= \frac{(2^m - 1)(2^m - 2)}{6}. \end{aligned}$$

□

The number of uncorrectable errors with weight half the minimum distance is determined by Corollaries 6 and 7.

Theorem 2. *For $m > 1$,*

$$\begin{aligned} &|E^1_{2^{m-2}}(\mathrm{RM}_m)| \\ &= 2(2^m - 1)\binom{2^{m-1} - 1}{2^{m-2} - 1} - \frac{(2^m - 1)(2^m - 2)}{2}. \end{aligned}$$

Let $E^0_{2^{m-2}}(\mathrm{RM}_m)$ be the set of correctable errors with weight 2^{m-2} for RM_m. $|E^0_{2^{m-2}}(\mathrm{RM}_m)|$ can be obtained from Theorem 2 and the fact that $|E^0_{2^{m-2}}(\mathrm{RM}_m)| + |E^1_{2^{m-2}}(\mathrm{RM}_m)| = \binom{2^m}{2^{m-2}}$.

Theorem 3. *Let $T_{\min}$ be a minimum trial set for RM_m. Then, for $m > 1$,*

$$|T_{\min}| \geq 2(2^m - 1) - \frac{(2^m - 1)(2^m - 2)}{2\binom{2^{m-1}-1}{2^{m-2}-1}}. \qquad (16)$$

For $m > 4$,

$$|T_{\min}| = |M(\mathrm{RM}_m)| = 2(2^m - 1). \qquad (17)$$

Proof. For each $\boldsymbol{v} \in E^1_{2^{m-2}}(\mathrm{RM}_m)$, $\boldsymbol{v} = \tilde{L}(\boldsymbol{c})$ for some $\boldsymbol{c} \in \mathrm{RM}^*_m$. Therefore, $\sum_{\boldsymbol{c} \in T_{\min}} |\tilde{L}(\boldsymbol{c})| \geq |E^1_{2^{m-2}}(\mathrm{RM}_m)|$. Thus, $\binom{2^{m-1}-1}{2^{m-2}-1}|T_{\min}| \geq |E^1_{2^{m-2}}(\mathrm{RM}_m)|$ from (6). This leads to (16). The fraction $(2^m-1)(2^m-2)/2\binom{2^{m-1}-1}{2^{m-2}-1}$ in (16) will become less than 1 for $m > 4$. This fact leads to (17). □

Actually, we found that $|T_{\min}| = |M(\mathrm{RM}_m)|$ for $m = 4$ by computer search. For $m = 3$, $|T_{\min}| = 10$ though $|M(\mathrm{RM}_m)| = 14$.

4 Conclusions

We have shown that a minimum trial set for the first-order Reed-Muller codes should contains all minimal codewords except for small code length, and determined the number of correctable errors by the minimum distance decoding with weight half the minimum distance for the first-order Reed-Muller codes.

References

[1] T. Helleseth, T. Kløve, and V. Levenshtein, "Error-correction capability of binary linear codes," *IEEE Trans. Inform. Theory*, vol.51, no.4, pp.1408–1423, Apr. 2005.

[2] G. Zémor, "Threshold effects in codes," in *Proc. First French-Israel Workshop on Algebraic Coding, Paris, France, July, 1993,* Lecture Notes in Computer Science, vol.781, Springer-Verlag, pp.278–286, 1994.

[3] A. Ashikhmin and A. Barg, "Minimal vectors in linear codes," *IEEE Trans. Inform. Theory*, vol. 44, no. 5, pp.2010–2017, Sept. 1998.

[4] W.W. Peterson and E.J. Weldon, Jr., *Error-Correcting Codes, 2nd Edition*, MIT Press, 1972.

[5] A. Barg, "Complexity issues in coding theory," in V. Pless and W.C. Huffman, Eds. *Handbook of Coding Theory*, North-Holland, vol. 1, pp. 649–754, 1998.