2007 Hawaii and SITA Joint Conference on Information Theory, HISC2007
Hawaii, USA, May 29–31, 2007

# On Trial Set and Uncorrectable Errors for the First-Order Reed-Muller Codes

Kenji Yasunaga and Toru Fujiwara

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

**Abstract**

*Trial set* of codewords is introduced by Helleseth, Kløve, and Levenshtein for a minimum distance decoding and for estimating the number of uncorrectable errors. In this paper, some upper and lower bounds on the size of trial sets are derived for general linear codes. For the first-order Reed-Muller codes, the size of trial set and minimal uncorrectable errors are determined.

## 1. Introduction

The correctable errors for syndrome decoding are coset leaders of a code. If a minimum weight vector in each coset is taken as the coset leader, the syndrome decoding performs maximum likelihood decoding over a binary symmetric channel [1]. 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 $\boldsymbol{x}$ (the support set of $\boldsymbol{y}$ contains that of $\boldsymbol{x}$), if $\boldsymbol{y}$ is correctable, then $\boldsymbol{x}$ is also correctable, and if $\boldsymbol{x}$ is uncorrectable, then $\boldsymbol{y}$ is also uncorrectable [1].

Using this monotone 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 [3]. 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 by minimum distance decoding. They characterized trial set using a notion *larger halves* of a codeword. A trial set for a code is the set of codewords whose larger halves contain all minimal uncorrectable errors. The set of minimal codewords [4] in the code is an example of trial sets. However, it is desirable to obtain the smaller trial sets for their applications.

In this paper, first we give some upper and lower bounds for the size of smallest trial sets for general linear codes. Experimental results show that some bound we obtained is tighter than known bounds.

Next, we determine the size of smallest trial sets and the number of minimal uncorrectable errors for the first-order Reed-Muller codes. In the proof of the size of smallest trial sets, the number of uncorrectable errors of weight half the minimum distance is significant, which was already given in [5]. We give another proof of it since some results in our proof are used in a proof of the number of minimal uncorrectable errors.

## 2. Larger halves and trial sets

In this section, we review definitions and properties of larger halves and trial sets, which are given in [3].

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 $C_1, C_2, C_3, \ldots, C_{2^{n-k}}$; $\mathbf{F}^n = \bigcup_{i=1}^{2^{n-k}} C_i$ and $C_i \cap C_j = \emptyset$ for $i \neq j$, where each $C_i = \{\boldsymbol{v}_i + \boldsymbol{c} : \boldsymbol{c} \in C\}$ with $\boldsymbol{v}_i \in \mathbf{F}^n$. The vector $\boldsymbol{v}_i$ is called the coset leader of the coset $C_i$. We choose the minimum element in the coset $C_i$ with respect to the following relation $\prec$ as the coset leader throughout this paper. The relation $\boldsymbol{x} \prec \boldsymbol{y}$ means that the Hamming weight of $\boldsymbol{x}$ is smaller than that of $\boldsymbol{y}$ or the Hamming weights of $\boldsymbol{x}$ and $\boldsymbol{y}$ are equal but $\boldsymbol{x}$ is lexicographically smaller than $\boldsymbol{y}$. Formally,

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

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 $\boldsymbol{x}$: $v(\boldsymbol{x}) = \sum_{i=1}^{n} x_i 2^{n-i}$.

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. Then both $E^0(C)$ and $E^1(C)$ have the following well-known monotone structure (see [1, Theorem 3.11]). 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 $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$. 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. 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 proposed a minimum distance decoding, which we call *trial set decoding* [3]. A trial set $T$ for the code $C$ is defined as the set of codewords in $C \setminus \{\mathbf{0}\}$ that has the following property:

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

See [3] for details of trial set decoding. 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. Furthermore, the weight distribution of a trial set gives an upper bound on the number of uncorrectable errors [3, Corollary 7], the value of which becomes small if a given trial set is small. 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 3. To describe a necessary and sufficient condition for a set to be a trial set, we need to review the notions *minimal uncorrectable errors* and *larger halves* of codewords [3].

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 $\boldsymbol{x} \subsetneq \boldsymbol{y}$ in $E^1(C)$. 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 $\boldsymbol{c} \in C$:

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

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

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

where

$$m(\boldsymbol{x}) = \min S(\boldsymbol{x}).$$

The proof of equivalence between the definition and the above condition is found in the proof of Theorem 1 of [3]. 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** ([3, 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 theorem shows that a minimum trial set for $C$ should consist of minimal codewords in $C$.

**Theorem 2** ([3, 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 $C$.*

## 3. Some upper and lower bounds on the size of trial sets

We give some bounds on the size of $T_{\min}$. Define $T_{\mathrm{nec}}$ as the set of minimal codewords $\boldsymbol{c} \in M(C)$ such that, for some $\boldsymbol{v} \in M^1(C)$, $\boldsymbol{v} \in L(\boldsymbol{c})$ and $\boldsymbol{v} \notin L(\boldsymbol{c}')$ for all $\boldsymbol{c}' \in M(C) \setminus \{\boldsymbol{c}\}$. Then codewords in $T_{\mathrm{nec}}$ are necessary to compose a trial set. Let

$$D^i(C) = \{\boldsymbol{v} \in M^1(C) \setminus L(T_{\mathrm{nec}}) : \\ |\{\boldsymbol{c} \in M(C) \setminus T_{\mathrm{nec}} : \boldsymbol{v} \in L(\boldsymbol{c})\}| = i\}.$$

$D^i(C)$ is the set of uncorrectable errors $\boldsymbol{v}$ such that $\boldsymbol{v}$ is not a larger half of codewords in $T_{\mathrm{nec}}$ and a common larger half among $i$ codewords in $M(C) \setminus T_{\mathrm{nec}}$. Note that $|M^1(C)| = |L(T_{\mathrm{nec}})| + \sum_i |D^i(C)|$.

**Theorem 3.** *For an $(n, k, d)$ linear code $C$ with $d > 1$, consider a minimum trial set $T_{\min}$. Then $|T_{\min}|$ is lower bounded by $k$ and $|T_{\mathrm{nec}}|$, and upper bounded by $|M(C)|$, $|M^1(C)|$, and $|T_{\mathrm{nec}}| + \sum_i |D^i(C)|$.*

*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 $k \leq |T_{\min}|$. $|T_{\mathrm{nec}}| \leq |T_{\min}|$ is obvious. $|T_{\min}| \leq |M(C)|$ is derived from Theorem 2. 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

Table 1: Estimation of the size of minimum trial sets for some BCH, extended BCH, and Reed-Muller codes.

| $C$ | Lower bounds | | $\lvert T_{\min}\rvert$ | Upper bounds | | | | |
|---|---|---|---|---|---|---|---|---|
| | New | | | [3] | | New | | |
| | $k$ | $\lvert T_{\rm nec}\rvert$ | | $\lvert M(C)\rvert$ | $\lvert M^1(C)\rvert$ | $\lvert L(M(C))\rvert$ | (a) | (b) |
| (15,11) BCH | 11* | 11* | 11∼83 | 308 | 105 | 525 | 151 | 83* |
| (15,7) BCH | 7 | 44* | 44∼87 | 108 | 351 | 4133 | 2713 | 87* |
| (15,5) BCH | 5 | 30* | 30 | 30* | 945 | 1260 | 1260 | 30* |
| (16,11) exBCH | 11 | 16* | 16∼79 | 588 | 116 | 1772 | 780 | 79* |
| (16,7) exBCH | 7 | 45* | 45∼86 | 126 | 434 | 8039 | 8039 | 86* |
| (16,5) exBCH | 5 | 30* | 30 | 30* | 1260 | 1575 | 1575 | 30* |
| (16,11) RM | 11 | 15* | 15∼79 | 588 | 116 | 1728 | 1728 | 79* |
| (16,5) RM | 5 | 30* | 30 | 30* | 1260 | 1575 | 1575 | 30* |

(a) is $|L(M(C)) \setminus L(C \setminus M(C))|$, and (b) is $|T_{\rm nec}| + \sum_i |D^i(C)|$.
* means the maximum/minimum value for the lower/upper bounds.

$T_{\min} \setminus \{\boldsymbol{c}''\}$ forms a trial set. This contradicts the definition of minimum trial set. Hence, $|T_{\min}| \le |M^1(C)|$. $\sum_i |D^i(C)| (= |M^1(C)| - |L(T_{\rm nec})|)$ is the number of minimal uncorrectable errors that are not larger halves of any codewords in $T_{\rm nec}$. From a similar argument as $|T_{\min}| \le |M^1(C)|$ for these uncorrectable errors, $|T_{\min}| \le |T_{\rm nec}| + \sum_i |D^i(C)|$. □

Since a naive algorithm for computing $|M^1(C)|$ is very time-consuming, the following lemmas may be useful.

**Lemma 1** ([3, 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 $H(\boldsymbol{y}) = \{\boldsymbol{c} \in C : \boldsymbol{y} + \boldsymbol{c} \prec \boldsymbol{y}\}$. For a linear code $C$ with $d > 1$ and a minimal uncorrectable error $\boldsymbol{y}$ in $C$, $H(\boldsymbol{y}) \subseteq M(C)$ from [3, Theorem 1]. Since $\boldsymbol{y} \in L(\boldsymbol{c})$ implies $\boldsymbol{c} \in H(\boldsymbol{y})$ from the property of $H(\cdot)$, larger halves of non-minimal codeword cannot be minimal uncorrectable errors. From the above fact and Lemma 1, we have the following.

**Lemma 2.** *For a linear code $C$ with $d > 1$, $M^1(C) \subseteq L(M(C)) \setminus L(C \setminus M(C)) \subseteq L(M(C))$.*

As a result, we have the following upper and lower bounds on $|T_{\min}|$ from Theorem 3 and Lemmas 1 and 2.

**Corollary 1.** *The size of a minimum trial set $T_{\min}$ for an $(n, k, d)$ linear code $C$ with $d > 1$ is bounded by*

$$\begin{aligned}\max\{k, |T_{\rm nec}|\} &\le |T_{\min}| \\ &\le \min\Big\{|M(C)|, |M^1(C)|, |L(M(C))|, \\ &\quad |L(M(C)) \setminus L(C \setminus M(C))|, |T_{\rm nec}| + \sum_i |D^i(C)|\Big\}.\end{aligned}$$

We compute above upper and lower bounds for some codes. The results are shown in Table 1. The upper bound $|T_{\rm nec}| + \sum_i |D^i(C)|$ is tight for all codes compared to known bounds ($|M(C)|$ and $|M^1(C)|$). The upper and lower bounds coincide for several codes.

## 4. Minimum trial sets for the first-order Reed-Muller codes

In this section, we determine the size of minimum trial sets for the first-order Reed-Muller codes. More precisely, we will show that $|T_{\min}| = 2(2^m - 1)$ for the first-order Reed-Muller code $\mathrm{RM}_m$ of length $2^m$ for $m > 4$. In the proof, the number of uncorrectable errors of weight half the minimum distance, which was already derived in [5], is significant. However, we give another proof here since some observations in it is used in the next section. In the proof of [5], the cosets that have uncorrectable errors of weight half the minimum distance are partitioned into three types. Then the number of cosets for each type is determined. On the other hand, in our proof, first we observe that uncorrectable errors of weight half the minimum distance are contained in the set of larger halves of codewords except all-zero and all-one codewords. Then counting the number of larger halves that are common among two or more codewords leads to the result. Many proofs in this section are omitted for space limitations. The reader is referred to [6] for details.

$\mathrm{RM}_m$ 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 all-zero and all-one codewords have the minimum weight $2^{m-1}$. $\mathrm{RM}_m$ is defined recursively as

$$\mathrm{RM}_0 = \{\mathbf{0}, \mathbf{1}\},$$
$$\mathrm{RM}_{m+1} = \bigcup_{\boldsymbol{c} \in \mathrm{RM}_m} \{\boldsymbol{c} \circ \boldsymbol{c}, \boldsymbol{c} \circ \overline{\boldsymbol{c}}\},$$

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 $\mathrm{RM}_m$ except all-zero and all-one codewords 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 $\mathrm{RM}_m^*$.

First we observe that $|T_{\min}| \leq |M(\mathrm{RM}_m)| = 2(2^m - 1)$ from Theorem 2. In the rest of the section, we show the lower bound, $|T_{\min}| \geq 2(2^m - 1)$, for $m > 4$. That is, all codewords of weight $2^{m-1}$ in $\mathrm{RM}_m$ are necessary for composing trial sets for $m > 4$.

The weight of all codewords in $\mathrm{RM}_m^*$ is $2^{m-1}$. Thus, the weights of their larger halves are $2^{m-2}$ and $2^{m-2}+1$ from the condition (2). Let $L^-(\boldsymbol{c})$ and $L^+(\boldsymbol{c})$ denote the sets of larger halves of weight $2^{m-2}$ and $2^{m-2}+1$, respectively. Also let $L^-(C) = \{L^-(\boldsymbol{c}) : \boldsymbol{c} \in C\}$ and $L^+(C) = \{L^+(\boldsymbol{c}) : \boldsymbol{c} \in C\}$. Define

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

A vector $\boldsymbol{v} \in E^1_{2^{m-2}}(\mathrm{RM}_m)$ 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. From Theorem 1, $\boldsymbol{v} \in E^1_{2^{m-2}}(\mathrm{RM}_m)$ is a larger half of some codeword in a trial set for $\mathrm{RM}_m$. We focus on the larger halves of weight $2^{m-2}$. We will show that all codewords in $\mathrm{RM}_m^*$ are necessary to generate $E^1_{2^{m-2}}(\mathrm{RM}_m)$ as their larger halves for $m > 4$.

From the conditions (1)–(3) for larger half,

$$|L^-(\boldsymbol{c})| = \binom{2^{m-1}-1}{2^{m-2}-1} \tag{4}$$

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 $\mathrm{RM}_m^*$. Let

$$\begin{aligned} D_m^i = &\{\boldsymbol{v} \in E^1_{2^{m-2}}(\mathrm{RM}_m) : \\ &|\{\boldsymbol{c} \in \mathrm{RM}_m^* : \boldsymbol{v} \in L^-(\boldsymbol{c})\}| = i\}. \end{aligned}$$

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

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

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

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

$$\begin{aligned} |E^1_{2^{m-2}}(\mathrm{RM}_m)| &= |D_m^1| + |D_m^2| + |D_m^3|, \\ (2^m - 1)\binom{2^{m-1}}{2^{m-2}} &= |D_m^1| + 2|D_m^2| + 3|D_m^3|. \end{aligned}$$

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

Let $S_m = \{m(\boldsymbol{c}) : \boldsymbol{c} \in \mathrm{RM}_m\}$. Then, from the definition of $\mathrm{RM}_m$, $S_m$ 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 $\mathrm{RM}_m$, $C_m(i)$ is also defined recursively as

$$C_0(1) = \{\mathbf{1}\}, \tag{5}$$

$$C_{m+1}(1) = \{\boldsymbol{c} \circ \boldsymbol{c}, \boldsymbol{c} \circ \overline{\boldsymbol{c}} : \boldsymbol{c} \in C_m(1)\} \cup \{\mathbf{1} \circ \mathbf{0}\}, \tag{6}$$

$$C_{m+1}(2^{m-1} + 1) = \{\mathbf{0} \circ \mathbf{1}\}, \tag{7}$$

$$C_{m+1}(i) = \{\boldsymbol{c} \circ \boldsymbol{c}, \boldsymbol{c} \circ \overline{\boldsymbol{c}} : \boldsymbol{c} \in C_m(i)\} \text{ for } i > 1. \tag{8}$$

**Lemma 4.** *Let $\boldsymbol{c}_1, \boldsymbol{c}_2 (\neq \boldsymbol{c}_1) \in C_m(i)$ for $i \in S_m \setminus \{2^{m-2} + 1\}$. For $m > 1$,*

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

**Lemma 5.** *For $m > 1$,*

$$\begin{aligned} |D_m^2| &= \sum_{i \in S_m \setminus \{1, 2^{m-1}+1\}} \frac{|C_m(i)|(|C_m(i)| - 1)}{2}, \\ |D_m^3| &= \frac{|C_m(1)|(|C_m(1)| - 1)}{6}. \end{aligned}$$

*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 4, 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 $\boldsymbol{c} \in C_m(i) \setminus \{\boldsymbol{c}_1, \boldsymbol{c}_2\}$ such that $\boldsymbol{v} \in L^-(\boldsymbol{c})$. This can be shown by a similar argument of the proof of Lemma 3. 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 3.** *For $m > 1$,*

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

The number of uncorrectable errors of weight half the minimum distance is determined by Corollaries 2 and 3.

**Theorem 4** ([5])**.** *For $m > 1$,*

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

**Corollary 4.** *Let $T_{\min}$ be a minimum trial set for $\mathrm{RM}_m$. Then, for $m > 1$,*

$$|T_{\min}| \geq 2(2^m - 1) - \frac{(2^m - 1)(2^m - 2)}{\binom{2^{m-1}}{2^{m-2}}}. \quad (9)$$

*For $m > 4$,*

$$|T_{\min}| \geq 2(2^m - 1). \quad (10)$$

*Proof.* For each $\boldsymbol{v} \in E^1_{2^{m-2}}(\mathrm{RM}_m)$, $\boldsymbol{v} = L^-(\boldsymbol{c})$ for some $\boldsymbol{c} \in \mathrm{RM}^*_m$. Therefore, $\sum_{\boldsymbol{c} \in T_{\min}} |L^-(\boldsymbol{c})| \geq |E^1_{2^{m-2}}(\mathrm{RM}_m)|$. Thus, $\binom{2^{m-1}-1}{2^{m-2}-1}|T_{\min}| \geq |E^1_{2^{m-2}}(\mathrm{RM}_m)|$ from (4). This leads to (9). The fraction $(2^m - 1)(2^m - 2)/\binom{2^{m-1}}{2^{m-2}}$ in (9) will become less than 1 for $m > 4$. This fact leads to (10). □

**Theorem 5.** *Let $T_{\min}$ be a minimum trial set for $\mathrm{RM}_m$. Then, for $m \geq 4$,*

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

*Proof.* $|T_{\min}| \leq |M(\mathrm{RM}_m)| = 2(2^m - 1)$ from Theorem 2. For $m > 4$, $|T_{\min}| \geq 2(2^m - 1)$ from Corollary 4. For $m = 4$, $|T_{\min}| = |M(\mathrm{RM}_m)| = 30$ from Table 1 ($\mathrm{RM}_4$ is the (16,5) Reed-Muller code). □

Note that, for $m = 4$, though $|T_{\min}| \geq 27$ from (9), $|T_{\min}| \geq |T_{\mathrm{nec}}| = 30$ is obtained by computer search in Section 3. Contrary to the above fact, one can verify that $|T_{\min}| = 10$ though $|M(\mathrm{RM}_m)| = 14$ for $m = 3$.

## 5. Minimal uncorrectable errors in the first-order Reed-Muller codes

In this section, we determine the number of minimal uncorrectable errors in the first-order Reed-Muller codes. The set of minimal uncorrectable errors $M^1(\mathrm{RM}_m)$ consists of the larger halves of $\mathrm{RM}^*_m$ that are not minimal in uncorrectable errors. The set $L(\mathrm{RM}^*_m)$ consists of $L^-(\mathrm{RM}^*_m)$ and $L^+(\mathrm{RM}^*_m)$. Since the vectors in $L^-(\mathrm{RM}^*_m)$ are not covered with any vectors in $E^1(\mathrm{RM}_m)$ and the size of $L^-(\mathrm{RM}^*_m) = E^1_{2^{m-2}}(\mathrm{RM}_m)$ are determined in the previous section, we would know the number of vectors in $L^+(\mathrm{RM}^*_m)$ that cover some vectors in $L^-(\mathrm{RM}^*_m)$. The followings show that if $\boldsymbol{v} \in L^+(\mathrm{RM}^*_m)$ covers a vector $\boldsymbol{v}' \in L^-(\mathrm{RM}^*_m)$, then the vector $\boldsymbol{v}'$ is uniquely determined for $m > 3$. For $\boldsymbol{u}, \boldsymbol{v} \in \mathbf{F}^n$, we define $\boldsymbol{u} \cap \boldsymbol{v}$ as the vector $\boldsymbol{w} \in \mathbf{F}^n$ such that $\mathrm{S}(\boldsymbol{w}) = \mathrm{S}(\boldsymbol{u}) \cap \mathrm{S}(\boldsymbol{v})$.

**Lemma 6.** *For $\boldsymbol{c}, \boldsymbol{c}' \in \mathrm{RM}^*_m$, there exist $\boldsymbol{v}, \boldsymbol{v}' \in \mathbf{F}^n$ such that $\boldsymbol{v} \in L^+(\boldsymbol{c})$, $\boldsymbol{v}' \in L^-(\boldsymbol{c})$, and $\boldsymbol{v}' \subseteq \boldsymbol{v}$ if and only if there exist $\boldsymbol{v}, \boldsymbol{v}' \in \mathbf{F}^n$ such that*

$$\boldsymbol{v}' = \boldsymbol{c} \cap \boldsymbol{c}', \quad (11)$$

$$\boldsymbol{v}' \subseteq \boldsymbol{v} \subseteq \boldsymbol{c}, \quad (12)$$

$$m(\boldsymbol{c}) < m(\boldsymbol{v}) \leq m(\boldsymbol{v}') = m(\boldsymbol{c}'), \quad (13)$$

$$\|\boldsymbol{v}\| = 2^{m-2} + 1. \quad (14)$$

*Proof.* From (1)–(3) and the properties of $\mathrm{RM}_m$, there exist $\boldsymbol{v} \in L^+(\boldsymbol{c})$ and $\boldsymbol{v}' \in L^-(\boldsymbol{c})$ that satisfy $\boldsymbol{v}' \subseteq \boldsymbol{v}$ if and only if there exist $\boldsymbol{v}, \boldsymbol{v}' \in \mathbf{F}^n$ such that $\boldsymbol{v} \subseteq \boldsymbol{c}$, $\|\boldsymbol{v}\| = 2^{m-2} + 1$, $m(\boldsymbol{v}) > m(\boldsymbol{c})$, $\boldsymbol{v}' \subseteq \boldsymbol{c}'$, $\|\boldsymbol{v}'\| = 2^{m-2}$, $m(\boldsymbol{v}') = m(\boldsymbol{c}')$, and $\boldsymbol{v}' \subseteq \boldsymbol{v}$. It follows that $\boldsymbol{v}' = \boldsymbol{c} \cap \boldsymbol{c}'$ from $\boldsymbol{v}' \subseteq \boldsymbol{c}'$ and $\boldsymbol{v}' \subseteq \boldsymbol{c}$. Then the statement follows. □

**Lemma 7.** *For $\boldsymbol{v} \in L^+(\boldsymbol{c})$ with $\boldsymbol{c} \in \mathrm{RM}^*_m$, there is at most one $\boldsymbol{v}' \in L^-(\mathrm{RM}^*_m)$ such that $\boldsymbol{v}' \subseteq \boldsymbol{v}$ for $m > 3$.*

*Proof.* Suppose there are two vectors $\boldsymbol{v}' \in L^-(\boldsymbol{c}')$ and $\boldsymbol{v}''(\neq \boldsymbol{v}') \in L^-(\boldsymbol{c}'')$ such that $\boldsymbol{v}' \subseteq \boldsymbol{v}$ and $\boldsymbol{v}'' \subseteq \boldsymbol{v}$ for some $\boldsymbol{c}', \boldsymbol{c}'' \in \mathrm{RM}^*_m$. From Lemma 6, $\boldsymbol{v}' = \boldsymbol{c} \cap \boldsymbol{c}'$ and $\boldsymbol{v}'' = \boldsymbol{c} \cap \boldsymbol{c}''$. The vector $\boldsymbol{v}$ is represented as $\boldsymbol{v}' + \boldsymbol{e}_1$ and $\boldsymbol{v}'' + \boldsymbol{e}_2$ for vectors $\boldsymbol{e}_1, \boldsymbol{e}_2$ with $\|\boldsymbol{e}_1\| = \|\boldsymbol{e}_2\| = 1$. Then $d(\boldsymbol{v}', \boldsymbol{v}'') = d(\boldsymbol{v} + \boldsymbol{e}_1, \boldsymbol{v} + \boldsymbol{e}_e) = 2$, where $d(\boldsymbol{x}, \boldsymbol{y})$ is the Hamming distance between $\boldsymbol{x}$ and $\boldsymbol{y}$. However $d(\boldsymbol{v}', \boldsymbol{v}'') = d(\boldsymbol{c} \cap \boldsymbol{c}', \boldsymbol{c} \cap \boldsymbol{c}'') = 2^{m-2}$ because $\{\boldsymbol{c} \cap \boldsymbol{v} : \boldsymbol{v} \in \mathrm{RM}_m\}$ forms a linear code and the distance is $2^{m-2}$. Thus a contradiction occurs if $m > 3$. □

Next, we show that if a larger half $\boldsymbol{v} \in L^+(\mathrm{RM}^*_m)$ covers a larger half $\boldsymbol{v}' \in L^-(\mathrm{RM}^*_m)$, then the number of larger halves in $L^+(\mathrm{RM}^*_m)$ that covers the vector $\boldsymbol{v}'$ is constant.

**Lemma 8.** *For $\boldsymbol{v}' \in L^-(\mathrm{RM}^*_m)$, the size of the set $\{\boldsymbol{v} \in L^+(\boldsymbol{c}) : \boldsymbol{v}' \subseteq \boldsymbol{v}\}$ is 0 or $2^{m-2} - 1$.*

*Proof.* If $\boldsymbol{v}' \subseteq \boldsymbol{v}$ for some $\boldsymbol{v} \in L^+(\boldsymbol{c})$ with $\boldsymbol{c} \in \mathrm{RM}^*_m$, then such $\boldsymbol{v}'$ is unique for the vectors in $L^+(\boldsymbol{c})$ from Lemma 7. The vector $\boldsymbol{v}$ is represented as $\boldsymbol{v} = \boldsymbol{v}' + \boldsymbol{e}$ with $\|\boldsymbol{e}\| = 1$. Then, the number of vectors $\boldsymbol{v} \in L^+(\boldsymbol{c})$ satisfying (11)–(14) is the number of existing vectors $\boldsymbol{e}$. Since $m(\boldsymbol{c}) < m(\boldsymbol{v})$, $S(\boldsymbol{e}) \subseteq S(\boldsymbol{c}) \setminus S(\boldsymbol{v}') \setminus \{m(\boldsymbol{c})\}$. The number of such $\boldsymbol{e}$ is $2^{m-1} - 2^{m-2} - 1 = 2^{m-2} - 1$. □

**Lemma 9.** *For any $\boldsymbol{c}, \boldsymbol{c}' \in \mathrm{RM}^*_m$ with $\boldsymbol{c} \neq \boldsymbol{c}'$, $L^+(\boldsymbol{c}) \cap L^+(\boldsymbol{c}') = \emptyset$.*

*Proof.* Suppose $\boldsymbol{v} \in L^+(\boldsymbol{c}) \cap L^+(\boldsymbol{c}')$. Since $\boldsymbol{v} \subseteq \boldsymbol{c}$ and $\boldsymbol{v} \subseteq \boldsymbol{c}'$, $d(\boldsymbol{c}, \boldsymbol{c}') \geq \|\boldsymbol{v}\| = 2^{m-1} + 1$. This contradicts the property of $\mathrm{RM}_m$. □

Now, we would know the number of $\boldsymbol{v} \in L^+(\boldsymbol{c})$ such that $\boldsymbol{v}' \subseteq \boldsymbol{v}$ for some $\boldsymbol{v}' \in L^-(\mathrm{RM}^*_m)$. From Lemma 7, there is unique such $\boldsymbol{v}'$ for each $\boldsymbol{v}$. From Lemma 8,

if $\boldsymbol{v}' \subseteq \boldsymbol{v}$, then the number of vectors $\boldsymbol{v} \in L^+(\boldsymbol{c})$ satisfying $\boldsymbol{v}' \subseteq \boldsymbol{v}$ is constant for each $\boldsymbol{v}'$ and $\boldsymbol{c}$. Moreover no vector in $L^+(\mathrm{RM}_m^*)$ is a common larger half of two or more codewords from Lemma 9. Thus, for each $\boldsymbol{v}' \in L^-(\mathrm{RM}_m^*)$, if we know the number of codewords whose larger halves covers $\boldsymbol{v}'$, then the number of vectors in $L^+(\mathrm{RM}_m^*)$ that covers some larger half in $L^-(\mathrm{RM}_m^*)$ is determined.

We write $S_m = \{a_1, a_2, \ldots, a_{m+1}\}$ where $a_1 = 1$ and $a_i = 2^{i-2} + 1$ for $2 \le i \le m+1$. It follows from the definitions of $\mathrm{RM}_m$ and $S_m$ that $S_m$ forms information bits for $\mathrm{RM}_m$. Let $\boldsymbol{c}(b_1, b_2, \ldots, b_{m+1})$ denotes the codeword in $\mathrm{RM}_m$ whose $a_i$-th position is $b_i$. Then

$$m(\boldsymbol{c}(\overbrace{0, \ldots, 0}^{i-1}, 1, \ldots)) = a_i.$$

From (13), if $\boldsymbol{v}' \subseteq \boldsymbol{v}$ for some $\boldsymbol{v}' \in L^-(\boldsymbol{c}')$ and $\boldsymbol{v} \in L^+(\boldsymbol{c})$, then $\boldsymbol{c}'$ is not of the form $\boldsymbol{c}(1, \ldots)$.

**Lemma 10.** *Let $\boldsymbol{c}' = \boldsymbol{c}(b'_1, \ldots, b'_{m+1}) \in \mathrm{RM}_m^*$ with $\sum_{j=1}^{i-1} b'_j = 0$ and $b'_i = 1$. Then vectors in $L^-(\boldsymbol{c}')$ are covered with vectors in $L^+(\boldsymbol{c})$ of $\boldsymbol{c} = \boldsymbol{c}(b_1, \ldots, b_{m+1}) \in \mathrm{RM}_m^*$ with $\sum_{j=1}^{i-1} b_j \neq 0$ and $b_i = 1$.*

*Proof.* Since $m(\boldsymbol{c}) < m(\boldsymbol{c}')$ from (13), the codeword $\boldsymbol{c}$ has non-zero element in $\{b_1, \ldots, b_{i-1}\}$, that is, $\sum_{j=1}^{i-1} b_j \neq 0$. From (11), the element in $m(\boldsymbol{c}')$-th position of $\boldsymbol{c}$ is 1. □

The above lemma says that any vector $\boldsymbol{v}' \in L^-(\boldsymbol{c}')$ of which $\boldsymbol{c}'$ is of the form $\boldsymbol{c}(0, \ldots, 0, 1, b'_{i+1}, \ldots, b'_{m+1})$ is covered with larger halves of codewords $\boldsymbol{c}$ of the form $\boldsymbol{c}(b_1, \ldots, b_{i-1}, 1, b_{i+1}, \ldots, b_{m+1})$ with $\sum_{j=1}^{i-1} b_j \neq 0$. Then it follows from Lemma 6 that $\boldsymbol{v}' = \boldsymbol{c} \cap \boldsymbol{c}'$, and the number of such $\boldsymbol{c}$ and that of $\boldsymbol{c}'$ are immediately determined because the parameters of $\boldsymbol{c}(b_1, \ldots, b_{m+1})$ are information bits of $\mathrm{RM}_m$. However, there may be other codeword $\boldsymbol{c}''$ of the form $\boldsymbol{c}(0, \ldots, 0, 1, b''_{i+1}, \ldots, b''_{m+1})$ such that $\boldsymbol{c} \cap \boldsymbol{c}'' = \boldsymbol{c} \cap \boldsymbol{c}'$. That is, $\boldsymbol{v}'$ is a common larger half of $\boldsymbol{c}'$ and $\boldsymbol{c}''$. Fortunately, the number of such larger halves is obtained in the previous section and is $|D_m^2|$. In the case we consider here, there is no common larger half of three codewords, which is $D_m^3$. This is because, as in the proof of Lemma 5, $D_m^3$ consists of larger halves of $\boldsymbol{c}(1, \ldots)$, but the larger halves we consider here are those of $\boldsymbol{c}(0, \ldots)$.

From the discussion above, we can count the number of vectors in $L^+(\mathrm{RM}_m^*)$ that are not in $M^1(\mathrm{RM}_m)$, and furthermore determine the size of $M^1(\mathrm{RM}_m)$.

**Lemma 11.** *For $m > 3$*

$$|L^+(\mathrm{RM}_m^*) \backslash M^1(\mathrm{RM}_m)| = (2^m - 1)(2^{m-1} - 1)(2^{m-2} - 1).$$

*Proof.* From Lemma 10, $L^-(\boldsymbol{c}')$ of $\boldsymbol{c}' = \boldsymbol{c}(b'_1, \ldots, b'_{m+1})$ with $\sum_{j=1}^{i-1} b'_j = 0$ and $b'_i = 1$ are covered with $L^+(\boldsymbol{c})$ of $\boldsymbol{c} = \boldsymbol{c}(b_1, \ldots, b_{m+1})$ with $\sum_{j=1}^{i-1} b_j \neq 0$ and $b_i = 1$. The number of codewords of the form $\boldsymbol{c}'$ is $2^{m+i-1}$ and that of $\boldsymbol{c}$ is $(2^{i-1} - 1) \cdot 2^{m-i+1} - 1$. Considering the above discussion of $D_m^2$, the number of $\boldsymbol{v} \in L^+(\boldsymbol{c})$ such that $\boldsymbol{v}' \subseteq \boldsymbol{v}$ for some $\boldsymbol{v}' \in L^-(\boldsymbol{c}')$ is $\sum_{i=2}^{m+1} 2^{m-i+1}((2^{i-1} - 1) \cdot 2^{m+1-i} - 1) - |D_m^2| = (2^m - 1)(2^m - 2)/2$. Therefore, from Lemma 8, we have the equation. □

**Theorem 6.** *For $m > 3$*

$$|M^1(\mathrm{RM}_m)| = 2(2^m - 1)\left(\binom{2^{m-1}}{2^{m-2} + 1} - 2^{m-3}(2^{m-1} - 1)\right).$$

*Proof.* The number of larger halves of weight $2^{m-2}$ in $M^1(\mathrm{RM}_m)$ is $|E^1_{2^{m-2}}(\mathrm{RM}_m)|$. The number of larger halves of weight $2^{m-2}+1$ is $\binom{2^{m-1}-1}{2^{m-2}+1} \cdot (2^{m+1} - 2)$ because there is no common larger halves of weight $2^{m-2} + 1$ of two or more codewords from Lemma 9 and $|L^+(\boldsymbol{c})|$ for each $\boldsymbol{c} \in \mathrm{RM}_m^*$ is $\binom{2^{m-1}-1}{2^{m-2}+1}$. The number of larger halves of weight $2^{m-2} + 1$ that is not in $M^1(\mathrm{RM}_m)$ is given in Lemma 11. Hence we have the equation. □

## References


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

[2] G. Zémor, "Threshold effects in codes," in *Proc. First French-Israel Workshop on Algebraic Coding, Paris, France, July, 1993,*

[3] 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.

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

[5] C.K. Wu,"On distribution of Boolean functions with nonlinearity $\le 2^{n-2}$", *Australasian Journal of Combinatorics*, vol.17, pp.51–59, Mar. 1998.

[6] K. Yasunaga and T. Fujiwara, "Correctable Errors of Weight Half the Minimum Distance for the First-Order Reed-Muller Codes," in *Proc. of the 29th Symposium on Information Theory and Its Applications (SITA2006)*, pp. 5–8, Nov. 2006.