On Correctable Errors of Binary Linear Codes

Kenji Yasunaga and Toru Fujiwara, *Member, IEEE*

***Abstract*—The error correction capability of binary linear codes with minimum distance decoding, in particular the number of correctable/uncorrectable errors, is investigated for general linear codes and the first-order Reed–Muller codes. For linear codes, a lower bound on the number of uncorrectable errors is derived. The bound for uncorrectable errors with a weight of half the minimum distance asymptotically coincides with the corresponding upper bound for Reed–Muller codes and random linear codes. For the first-order Reed–Muller codes, the number of correctable/uncorrectable errors with a weight of half the minimum distance plus one is determined. This result is equivalent to deriving the number of Boolean functions of m variables with nonlinearity $2^{m-2}+1$. The *monotone error structure* and its related notions *larger half* and *trial set*, which were introduced by Helleseth, Kløve, and Levenshtein, are mainly used to derive the results.**

***Index Terms*—Boolean function, error correction capability, monotone error structure, nonlinearity, Reed–Muller code, trial set.**

I. Introduction

A FUNDAMENTAL problem in coding theory is the error performance analysis of codes. In this paper, we investigate the error correction capability of binary linear codes with minimum distance decoding, which is a maximum likelihood decoding for binary symmetric channels. In particular, we investigate the numbers of correctable/uncorrectable errors.

It is well known that if the Hamming weight of an error vector is less than $d/2$, where d is the minimum distance of the code, then the minimum distance decoder always corrects the error. Therefore, the correction capability for errors with weight $\geq d/2$ is crucial to the performance analysis of minimum distance decoding. Particularly important is an analysis for errors with weight around $d/2$ because the ratio in such cases of the correctable errors is highest with weight $\geq d/2$.

In the analysis of minimum distance decoding, syndrome decoding is commonly used. Syndrome decoding performs as a minimum distance decoding if a minimum weight vector is selected as the coset leader in each coset. Then the correctable errors are the coset leaders of the code, and, thus, the weight distribution of the coset leaders represents the number of correctable errors for each weight. Considering this fact, the error correction capabilities for certain specific codes are completely determined [1]–[4]. For general linear codes, some bounds on the number of correctable errors were presented in [5]–[7]. Although the first-order Reed–Muller codes have a simple structure, the exact number of correctable errors for them was known only for weight $d/2$ [8]. Determining the number of correctable errors of weight i for the first-order Reed–Muller codes is equivalent to determining the number of Boolean functions with nonlinearity i, and the nonlinearity of Boolean functions is an important criterion in cryptography [9, Section 4]. The relation of Boolean function to error correction is described in Section IV.

In this study, we examine the number of correctable errors of weight $\geq d/2$ using a *monotone error structure*, which is an old result in coding theory [10, Theorem 3.11]. The monotone error structure is the following property: If $\boldsymbol{x}$ is a correctable error, then any vector that is covered by $\boldsymbol{x}$ is also correctable, and if $\boldsymbol{x}$ is an uncorrectable error, then any vector that covers $\boldsymbol{x}$ is also uncorrectable. We say that $\boldsymbol{x}$ covers $\boldsymbol{y}$ if the support of $\boldsymbol{x}$ contains that of $\boldsymbol{y}$. This structure is useful for error analysis since the correctable (and uncorrectable) errors are characterized by the maximal correctable (and minimal uncorrectable) errors. Helleseth, Kløve, and Levenshtein [6] analyzed an asymptotic error correctability of binary linear codes using the monotone error structure, and introduced two useful notions, *larger half* and *trial set*, which characterizes the minimal uncorrectable errors (and thus the uncorrectable errors). A trial set for the code is defined as a set of nonzero codewords whose larger halves contain the minimal uncorrectable errors. In [6] two applications of a trial set were presented: one that provides an upper bound on the number of uncorrectable errors, and the other that is for minimum distance decoding.

For weight $\lceil d/2 \rceil$, we derive a lower bound on the number of uncorrectable errors for general linear codes. The bound is derived in terms of the numbers of codewords with weights d and $d+1$ in a trial set for the code. Because the set of nonzero codewords is a trial set, the bound is evaluated by the weight distribution of the codes. The lower bound asymptotically coincides with the upper bound of [6, Corollary 7] for Reed–Muller codes and random linear codes. By generalizing the idea of the lower bound, we also derive a lower bound on the number of uncorrectable errors for weight $i > d/2$. However, as i increases, the generalized becomes weaker.

Furthermore, for the first-order Reed–Muller codes, we provide explicit expressions for the numbers of correctable errors of weights $d/2$ and $d/2+1$. Although the case of weight $d/2$ has already been solved by Wu [8], we present a simpler proof in this paper. As a direct consequence of this solution, the number of Boolean functions of m variables with nonlinearity $2^{m-2}+1$

Manuscript received September 22, 2008; revised November 13, 2009. Current version published May 19, 2010. This work was supported in part by the JSPS Global COE Program "Computationism as a Foundation for the Sciences." Most of this study was conducted when K. Yasunaga was a student at Osaka University and a postdoctoral fellow at Kwansei Gakuin University.

K. Yasunaga is with the Department of Mathematical and Computing Sciences, Tokyo Institute of Technology, Tokyo, Japan (e-mail: kenji.yasunaga@gmail.com).

T. Fujiwara is with Graduate School of Information Science and Technology, Osaka University, Osaka, Japan (e-mail: fujiwara@ist.osaka-u.ac.jp).

Communicated by L. M. G. M. Tolhuizen, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2010.2046209

0018-9448/$26.00 © 2010 IEEE

is determined. We also determine the weight distribution of the minimal uncorrectable errors.

Finally, because smaller trial sets have desirable applications, we investigate the sizes of *minimum trial* sets for codes. We derive upper and lower bounds on the size of minimum trial sets. Experimental results show that our bounds are tighter than the known bounds, and the sizes of minimum trial sets are determined for several codes because upper and lower bounds coincides for them. For the first-order Reed–Muller codes of length ≥ 16, it is elucidated that the minimum trial set is the set of the codewords except the all-zero and all-one codewords.

This paper is organized as follows: In Section II, we describe the monotone error structure and some properties of larger halves and trial sets needed for our results. In Section III, we derive lower bounds on the number of uncorrectable errors of weight $\lceil d/2 \rceil$ and that of weight greater than $\lceil d/2 \rceil$ for general linear codes. In Section IV, we provide the results for the first-order Reed–Muller codes. The numbers of uncorrectable errors of weight $d/2$ and $d/2+1$ are provided in Sections IV-A and IV-B, respectively. The weight distribution of the minimal uncorrectable errors is determined in Section IV-C. The size of minimum trial sets is studied in Section V. In Section VI, we conclude the paper.

II. Monotone Error Structure

In this section, we describe the monotone error structure and provide definitions and properties of larger halves and trial sets.

Let $\mathbb{F} = \{0,1\}$ and $\mathbb{F}^n$ be the set of all binary vectors of length n. Let $C \subseteq \mathbb{F}^n$ be a binary linear code of length n, dimension k, and minimum distance d, or for short, an (n,k,d) code. Then $\mathbb{F}^n$ is partitioned into the 2^{n-k} cosets of C, denoted by $D_1, D_2, \ldots, D_{2^{n-k}}$; $\mathbb{F}^n = \bigcup_{i=1}^{2^{n-k}} D_i$ and $D_i \cap D_j = \emptyset$ for $i \neq j$, where each $D_i = \{\boldsymbol{v}_i + \boldsymbol{c} : \boldsymbol{c} \in C\}$ with $\boldsymbol{v}_i \in \mathbb{F}^n$. The vector $\boldsymbol{v}_i$ is called a coset leader of the coset D_i, and every vector in D_i can be considered as $\boldsymbol{v}_i$.

Let H be a parity check matrix of C. The syndrome of a vector $\boldsymbol{v} \in \mathbb{F}^n$ is defined as $\boldsymbol{v}H^T$. All vectors having the same syndrome are in the same coset. 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 that contains $\boldsymbol{y}$. Thus, the set of correctable errors by syndrome decoding is the set of coset leaders. If each $\boldsymbol{v}_i$ has the minimum weight in the coset D_i, then the syndrome decoder performs as a minimum distance decoder, or a maximum likelihood decoder for a binary symmetric channel. Let $E^0(C)$ be the set of the coset leaders $\boldsymbol{v}_i$. Then the set of uncorrectable errors $E^1(C)$ is $\mathbb{F}^n \setminus E^0(C)$. For $0 \leq i \leq n$ and $b \in \{0,1\}$, we define

$$E_i^b(C) = \{\boldsymbol{v} \in E^b(C) : w(\boldsymbol{v}) = i\}$$

where $w(\boldsymbol{x})$ denotes the Hamming weight of a vector $\boldsymbol{x} \in \mathbb{F}^n$. The error probability of C after maximum likelihood decoding over the binary symmetric channel with cross-over probability p is given by

$$\sum_{i=1}^{n} \left| E_i^1(C) \right| p^i (1-p)^{n-i}.$$

In this paper, as in [6], we consider $\boldsymbol{v}_i$ as the minimum element in D_i with respect to the following total ordering $\preceq$: for $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{F}^n$

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

where $v(\boldsymbol{x})$ denotes the numerical value of $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$

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

The relation $v(\boldsymbol{x}) < v(\boldsymbol{y})$ also means that $\boldsymbol{x}$ is lexicographically smaller than $\boldsymbol{y}$.

When the minimum element with respect to $\preceq$ in each coset is considered as its coset leader, both $E^0(C)$ and $E^1(C)$ have a monotone structure.[1] Let $\subseteq$ denote the 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 of $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$. We write $\boldsymbol{x} \subset \boldsymbol{y}$ if $\boldsymbol{x} \subseteq \boldsymbol{y}$ and $\boldsymbol{x} \neq \boldsymbol{y}$. Consider $\boldsymbol{x}$ and $\boldsymbol{y}$ with $\boldsymbol{x} \subseteq \boldsymbol{y}$. The monotone structure is the following property: 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 [11], [18] elucidated that the error probability after the maximum likelihood decoding over the binary symmetric channels displays a threshold behavior. Helleseth *et al.* [6] studied this structure and introduced *larger halves* and *trial sets*.

Since the set of uncorrectable errors $E^1(C)$ has a monotone structure, $E^1(C)$ can be characterized by the *minimal uncorrectable errors* in $E^1(C)$. An uncorrectable error $\boldsymbol{y} \in E^1(C)$ is minimal if there exists no $\boldsymbol{x} \in E^1(C)$ such that $\boldsymbol{x} \subset \boldsymbol{y}$. We denote by $M^1(C)$ the set of minimal uncorrectable errors in C. Larger halves of a codeword $\boldsymbol{c} \in C$ are introduced to characterize the minimal uncorrectable errors, and are defined as minimal (w.r.t. $\subseteq$) vectors in the set of vectors $\boldsymbol{v} \in \mathbb{F}^n$ satisfying $\boldsymbol{v} + \boldsymbol{c} \preceq \boldsymbol{v}$ and $\boldsymbol{v} + \boldsymbol{c} \neq \boldsymbol{v}$. From the definition, we know that the set of larger halves of all nonzero codewords contains the set of minimal uncorrectable errors. The following condition is a necessary and sufficient condition that $\boldsymbol{v}$ is a larger half of $\boldsymbol{c} \in C$:

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

$$w(\boldsymbol{c}) \leq 2w(\boldsymbol{v}) \leq w(\boldsymbol{c}) + 2, \tag{2}$$

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

where

$$l(\boldsymbol{x}) = \min\{i : x_i \neq 0\}.$$

The condition (3) is not applicable if $w(\boldsymbol{c})$ is odd. The proof of equivalence between the definition and the above condition is

[1] In this paper, we use the total ordering $\preceq$ in selecting coset leaders for the monotone error structure. All orderings that give a monotone error structure are discussed in [6, Appendix I].

found in the proof of [6, Theorem 1]. Let $LH(\boldsymbol{c})$ denote the set of larger halves of $\boldsymbol{c} \in C \setminus \{\boldsymbol{0}\}$. For a set $U \subseteq C \setminus \{\boldsymbol{0}\}$, we define

$$LH(U) = \bigcup_{\boldsymbol{c} \in U} LH(\boldsymbol{c}).$$

When the weight of $\boldsymbol{c}$ is odd, all the vectors in $LH(\boldsymbol{c})$ have the same weight $(w(\boldsymbol{c})+1)/2$; whereas when the weight of $\boldsymbol{c}$ is even, $LH(\boldsymbol{c})$ consists of vectors of weights $w(\boldsymbol{c})/2$ and $w(\boldsymbol{c})/2+1$. For convenience, we denote by $LH^-(\boldsymbol{c})$ and $LH^+(\boldsymbol{c})$ the sets of larger halves of $\boldsymbol{c}$ with weight $w(\boldsymbol{c})/2$ and $w(\boldsymbol{c})/2+1$, respectively. Then, for an even-weight codeword $\boldsymbol{c} \in C$, $LH(\boldsymbol{c}) = LH^-(\boldsymbol{c}) \cup LH^+(\boldsymbol{c})$. In addition let $LH^-(U) = \bigcup_{\boldsymbol{c} \in U} LH^-(\boldsymbol{c})$ and $LH^+(U) = \bigcup_{\boldsymbol{c} \in U} LH^+(\boldsymbol{c})$ for an even-weight subcode $U \subseteq C \setminus \{\boldsymbol{0}\}$.

A set T of nonzero codewords in C is called a trial set [6] for C if the set of larger halves of codewords in T contains the set of minimal uncorrectable errors, that is

$$M^1(C) \subseteq LH(T).$$

From the definition of larger half, the set of nonzero codewords in C is a trial set for C. Since every larger half is an uncorrectable error, we have the relation

$$M^1(C) \subseteq LH(T) \subseteq E^1(C). \tag{4}$$

A codeword $\boldsymbol{c}$ is called *minimal* if $\boldsymbol{c}' \subset \boldsymbol{c}$ for $\boldsymbol{c}' \in C$ implies $\boldsymbol{c}' = \boldsymbol{0}$. Basic properties and applications of minimal codewords are seen in [12]. Let C^* denote the set of minimal codewords in C. Then we have the following property [6, Corollary 5]:

If T is a trial set for C
then $T \cap C^*$ is also a trial set for C. (5)

It follows from the above fact that the set of minimal codewords is a trial set and a trial set can consist of only minimal codewords.

A trial set can be used to provide an upper bound on the number of uncorrectable errors. Let T be a trial set for an (n,k,d) linear code C. For an integer i, we define $T_i = \{\boldsymbol{v} \in T : w(\boldsymbol{v}) = i\}$. Then, for i with $\lfloor (d-1)/2 \rfloor < i \le n$, it holds that [6, Corollary 7]

$$\left|E_i^1(C)\right| \le \sum_{j=d}^{2i} |T_j| \sum_{l=\lceil j/2 \rceil}^{\min\{i,j\}} \binom{j}{l}\binom{n-j}{i-l} - \sum_{l=\lceil d/2 \rceil}^{i} |T_{2l}| \binom{2l-1}{l}\binom{n-2l}{i-l}. \tag{6}$$

For two trial sets T and T' with $T \subset T'$, the bound using T is tighter than that using T'. The size of trial sets is discussed in Section V.

In the rest of the paper, for $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{F}^n$, we write $\boldsymbol{u} \cap \boldsymbol{v}$ as the vector in $\mathbb{F}^n$ whose support is $\mathrm{S}(\boldsymbol{u}) \cap \mathrm{S}(\boldsymbol{v})$. For an integer i we define $C_i = \{\boldsymbol{v} \in C : w(\boldsymbol{v}) = i\}$ for a code C, $A_i = |C_i|$, $M_i^1(C) = \{\boldsymbol{v} \in M^1(C) : w(\boldsymbol{v}) = i\}$, and $LH_i(U) = \{\boldsymbol{v} \in LH(U) : w(\boldsymbol{v}) = i\}$ for $U \subseteq C \setminus \{\boldsymbol{0}\}$.

III. Correctable Errors for Linear Codes

In this section, we investigate the number of correctable errors for general linear codes. We provide some lower bounds on $|E_i^1(C)|$ for $d/2 \le i \le n$. These lower bounds also provide upper bounds on $|E_i^0(C)|$ since we have the relation $|E_i^0(C)| + |E_i^1(C)| = \binom{n}{i}$ for $0 \le i \le n$.

A. Correctable Errors With a Weight of Half the Minimum Distance

We derive a lower bound on the number of uncorrectable errors with a weight that is half the minimum distance, which is $|E_{\lceil d/2 \rceil}^1(C)|$. The bound is expressed in the numbers of codewords with weights d and $d+1$ in the code.

Since the weight $\lceil d/2 \rceil$ is the minimum weight in $E^1(C)$, every vector in $E_{\lceil d/2 \rceil}^1(C)$ is not covered by other uncorrectable errors, and, thus, $M_{\lceil d/2 \rceil}^1(C) = E_{\lceil d/2 \rceil}^1(C)$. From (4), we have

$$M_{\lceil d/2 \rceil}^1(C) = LH_{\lceil d/2 \rceil}(T) = E_{\lceil d/2 \rceil}^1(C) \tag{7}$$

where T is a trial set for C. We will give a lower bound on $|E_{\lceil d/2 \rceil}^1(C)|$ by giving that on $|LH_{\lceil d/2 \rceil}(T)|$.

1) Even Minimum-Weight Case: When d is even, $LH_{\lceil d/2 \rceil}(T) = LH^-(T_d)$. The next lemma implies that the number of common larger halves among $LH^-(T_d)$ is small.

Lemma 1: Let C be a linear code with even minimum distance d. For every distinct $\boldsymbol{c}_1, \boldsymbol{c}_2 \in C_d$, $LH^-(\boldsymbol{c}_1) \cap LH^-(\boldsymbol{c}_2)$ is $\{\boldsymbol{c}_1 \cap \boldsymbol{c}_2\}$ or the empty set.

Proof: Suppose $\boldsymbol{v} \in LH^-(\boldsymbol{c}_1) \cap LH^-(\boldsymbol{c}_2)$. Then $w(\boldsymbol{v}) = d/2$, $\boldsymbol{v} \subseteq \boldsymbol{c}_1 \cap \boldsymbol{c}_2$ from (1), and $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2) = (w(\boldsymbol{c}_1) + w(\boldsymbol{c}_2) - w(\boldsymbol{c}_1 + \boldsymbol{c}_2))/2 \le d/2$. Hence, $\boldsymbol{v} = \boldsymbol{c}_1 \cap \boldsymbol{c}_2$. □

We provide a lower bound in the next theorem. The upper bound in the theorem is derived by (6).

Theorem 1: Let C be a linear code with even minimum distance d and T a trial set for C. Then

$$\left(\frac{1}{2}\binom{d}{\frac{d}{2}} - |T_d| + 1\right)|T_d| \le \left|E_{\frac{d}{2}}^1(C)\right| \le \frac{1}{2}\binom{d}{\frac{d}{2}}|T_d|.$$

Proof: We provide a bound on $|LH^-(T_d)|$, which equals to $|E_{d/2}^1(C)|$. For every $\boldsymbol{c} \in T_d$, the number of vectors in $LH^-(\boldsymbol{c})$ that are also larger halves of other codewords in T_d is at most $|T_d| - 1$ from Lemma 1. Thus, we have the lower bound $\sum_{\boldsymbol{c} \in T_d}(|LH^-(\boldsymbol{c})| - (|T_d| - 1))$. □

The bound can be improved when $T_d = C_d$.

Corollary 1: Let C be a linear code with even minimum distance d. Then

$$\left|E_{\frac{d}{2}}^1(C)\right| \ge \left(\frac{1}{2}\binom{d}{\frac{d}{2}} - \left\lfloor \frac{A_d - 1}{2} \right\rfloor\right) A_d.$$

Proof: Recall the proof of Theorem 1 in the case that $C \setminus \{\boldsymbol{0}\}$ is considered as a trial set for C. Suppose $\boldsymbol{c}, \boldsymbol{c}' \in C_d$ have the common larger half $\boldsymbol{c} \cap \boldsymbol{c}'$. Then $\boldsymbol{c}$ has no common larger half of weight $d/2$ with the codeword $\boldsymbol{c} + \boldsymbol{c}'$, since $l(\boldsymbol{c}) \ne l(\boldsymbol{c} + \boldsymbol{c}')$. Therefore, for every $\boldsymbol{c} \in C_d$, the number of vectors in $LH^-(\boldsymbol{c})$

that are also larger halves of other codewords in C_d is at most $\lfloor (A_d-1)/2 \rfloor$. We obtain the lower bound $\sum_{\boldsymbol{c}\in C_d}(|LH^-(\boldsymbol{c})| - \lfloor (A_d-1)/2 \rfloor)$. □

It would be good to find a set T_d that provides a tight bound. We note, however, that we cannot find any nontrivial set T_d if the lower bound in Corollary 1 is positive. In this case, it must be that $T_d = C_d$ because every $\boldsymbol{c} \in C_d$ has at least one larger half that has no common larger half with other codewords in C_d, which means that every $\boldsymbol{c} \in C_d$ should be in T_d.

The difference between the upper and the lower bounds is at most $|T_d|^2$. If the fraction $|T_d|/\binom{d}{d/2}$ tends to zero as the code length increases, the lower bound asymptotically coincides with the upper one.

2) Odd Minimum-Weight Case: When d is odd, $LH_{\lceil d/2 \rceil}(T) = LH(T_d) \cup LH^-(T_{d+1})$. The next lemma implies that the number of common larger halves among $LH(T_d)$ and $LH^-(T_{d+1})$ is small.

Lemma 2: Let C be a linear code with odd minimum distance d. For every distinct $\boldsymbol{c}_1, \boldsymbol{c}_1' \in C_d$ and distinct $\boldsymbol{c}_2, \boldsymbol{c}_2' \in C_{d+1}$, the following conditions hold: (a) $LH(\boldsymbol{c}_1) \cap LH(\boldsymbol{c}_1') = \emptyset$; (b) $LH(\boldsymbol{c}_1) \cap LH^-(\boldsymbol{c}_2)$ is $\{\boldsymbol{c}_1 \cap \boldsymbol{c}_2\}$ or the empty set; and (c) $LH^-(\boldsymbol{c}_2) \cap LH^-(\boldsymbol{c}_2')$ is $\{\boldsymbol{c}_2 \cap \boldsymbol{c}_2'\}$ or the empty set.

Proof: Every vector $\boldsymbol{v} \in LH(\boldsymbol{c}_1) \cup LH(\boldsymbol{c}_1') \cup LH^-(\boldsymbol{c}_2) \cup LH^-(\boldsymbol{c}_2')$ has weight $w(\boldsymbol{v}) = (d+1)/2$. For $\boldsymbol{c}, \boldsymbol{c}' \in C \setminus \{\boldsymbol{0}\}$, every vector $\boldsymbol{v} \in LH(\boldsymbol{c}) \cap LH(\boldsymbol{c}')$ has the property from (1) that $\boldsymbol{v} \subseteq \boldsymbol{c} \cap \boldsymbol{c}'$. From the equality $w(\boldsymbol{c} \cap \boldsymbol{c}') = (w(\boldsymbol{c}) + w(\boldsymbol{c}') - w(\boldsymbol{c} + \boldsymbol{c}'))/2$ and the fact $w(\boldsymbol{c} + \boldsymbol{c}') \ge d$, we have that $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_1') < (d+1)/2$, $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2) \le (d+1)/2$, and $w(\boldsymbol{c}_2 \cap \boldsymbol{c}_2') \le (d+1)/2$. Thus, the statement follows. □

We provide a lower bound by a similar argument as in the even case. The upper bound is derived by (6).

Theorem 2: Let C be a linear code with odd minimum distance d and T a trial set for C. Then

$$\begin{aligned}&\binom{d}{\frac{d+1}{2}}|T_d| \\ &\quad + \max\left\{\binom{d}{\frac{d+1}{2}} - |T_d| - |T_{d+1}| + 1, 0\right\}|T_{d+1}| \\ &\qquad \le \left|E^1_{\frac{d+1}{2}}(C)\right| \le \binom{d}{\frac{d+1}{2}}(|T_d| + |T_{d+1}|).\end{aligned}$$

Proof: We provide a bound on $|LH(T_d)| + |LH^-(T_{d+1}) \setminus LH(T_d)|$, which equals $|E^1_{(d+1)/2}(C)|$. Since $\boldsymbol{c} \in C_d$ has no common larger half with $\boldsymbol{c}' \in C_d \setminus \{\boldsymbol{c}\}$ from Lemma 2, we have that $|LH(T_d)| = |LH(\boldsymbol{c})| \cdot |T_d| = \binom{d}{(d+1)/2}|T_d|$.

Next we provide a lower bound on $|LH^-(T_{d+1}) \setminus LH(T_d)|$. For every $\boldsymbol{c} \in T_{d+1}$, the numbers of vectors in $LH^-(\boldsymbol{c})$ that are also in $LH(T_d)$ and $LH^-(T_{d+1} \setminus \{\boldsymbol{c}\})$ are at most $|T_d|$ and $|T_{d+1}| - 1$, respectively, from Lemma 1. Thus, we obtain the lower bound $\sum_{\boldsymbol{c}\in T_{d+1}}(|LH^-(\boldsymbol{c})| - |T_d| - (|T_{d+1}| - 1))$. □

The above lower bound can be improved when $T_d = C_d$ and $T_{d+1} = C_{d+1}$.

Corollary 2: Let C be a linear code with odd minimum distance d. Then

$$\begin{aligned}\left|E^1_{\frac{d+1}{2}}(C)\right| \ge \binom{d}{\frac{d+1}{2}}&A_d \\ &+ \max\left\{\binom{d}{\frac{d+1}{2}} - \left\lfloor\frac{A_d}{2}\right\rfloor - \left\lfloor\frac{A_{d+1}-1}{2}\right\rfloor, 0\right\}.\end{aligned}$$

Proof: Recall the proof of Theorem 2 in the case when $T_d = C_d$ and $T_{d+1} = C_{d+1}$. We improve the lower bound on $|LH^-(C_{d+1}) \setminus LH(C_d)|$. Suppose $\boldsymbol{c} \in C_{d+1}$ and $\boldsymbol{c}' \in C_d$ have the common larger half $\boldsymbol{c} \cap \boldsymbol{c}'$. Then $\boldsymbol{c} + \boldsymbol{c}' \in C_d$ has no common larger half with $\boldsymbol{c}$ since $l(\boldsymbol{c} \cap \boldsymbol{c}') = l(\boldsymbol{c})$ and $l(\boldsymbol{c}) \notin S(\boldsymbol{c} + \boldsymbol{c}')$. Likewise, suppose $\boldsymbol{c} \in C_{d+1}$ and $\boldsymbol{c}'' \in C_{d+1}$ have the common larger half $\boldsymbol{c} \cap \boldsymbol{c}''$. Then $\boldsymbol{c} + \boldsymbol{c}'' \in C_{d+1}$ has no common larger half with $\boldsymbol{c}$ since $l(\boldsymbol{c}) = l(\boldsymbol{c}'')$, and, thus, $l(\boldsymbol{c}) \notin S(\boldsymbol{c} + \boldsymbol{c}'')$. Therefore, for every $\boldsymbol{c} \in C_{d+1}$, the numbers of vectors in $LH^-(\boldsymbol{c})$ that are also in $LH(C_d)$ and $LH^-(C_{d+1})$ are at most $\lfloor A_d/2 \rfloor$ and $\lfloor (A_{d+1}-1)/2 \rfloor$, respectively. We have the lower bound $\sum_{\boldsymbol{c}\in C_{d+1}}(|LH^-(\boldsymbol{c})| - \lfloor A_d/2 \rfloor - \lfloor (A_{d+1}-1)/2 \rfloor)$. □

The difference between the upper and lower bounds is at most $(|T_d| + |T_{d+1}|)|T_{d+1}|$. Therefore, if the fraction $|T_{d+1}|/\binom{d}{(d+1)/2}$ tends to zero as the code length increases, the lower bound asymptotically coincides with the upper one.

In what follows, we see that the lower and upper bounds asymptotically coincide for Reed–Muller codes and random linear codes.

a) Reed–Muller Codes: For the rth-order Reed–Muller code of length 2^m, the minimum distance is 2^{m-r} and the number of minimum weight codewords is presented in Theorem 9 of [13, Chapter 13], which is upper bounded by $(2^{m+1}-2)^r$.

The fraction $A_d/\binom{d}{d/2}$ is upper bounded by

$$\frac{A_d}{\binom{d}{\frac{d}{2}}} \le \frac{(2^{m+1}-2)^r}{2^{2^{m-r-1}}} \le 2^{(m+1)r-2^{m-r-1}}.$$

Thus, for a fixed r the fraction tends to zero as m increases. This means that the upper and lower bounds in Theorem 1 asymptotically coincide.

b) Random Linear Codes: A random linear code is a code whose generator matrix has equiprobable entries. That is, first we set a parameter $R = k/n$, and then choose a generator matrix from all the 2^{nk} possible generator matrices with probability 2^{-nk}. We investigate the typical behavior of codes from this ensemble. All logarithms in this subsection are taken to the base two.

Let $\epsilon > 0$ be any constant. It is known [14, Section 2.1] that with high probability the minimum distance is δn with $\delta_{\mathrm{GV}} < \delta \le \delta_{\mathrm{GV}} + \epsilon$, where δ_{GV} is the smaller value satisfying $1 - H(\delta_{\mathrm{GV}}) = R$ and $H(x)$ is the binary entropy function of x. Using Stirling's approximation [15, pp. 52–54]

$$\sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n+1}} < n! < \sqrt{2\pi n}\left(\frac{n}{e}\right)^n e^{\frac{1}{12n}} \qquad (8)$$

for any $0 < \lambda < 1$, we have that $n^{-1}\log\binom{n}{\lambda n} = H(\lambda) - o(1)$. Since $\binom{x}{x/2}$ is a monotonically increasing function of x, we have that $n^{-1}\log\binom{d}{d/2} \geq n^{-1}\log\binom{\delta_{\rm GV}n}{\delta_{\rm GV}n/2} \geq \delta_{\rm GV}(H(1/2) - o(1)) = \delta_{\rm GV} - o(1)$ for typical random linear codes.

The weight distribution of typical random linear codes is studied in [16]. Let $\bar{A}_{\alpha n}$ with $0 < \alpha \leq 1$ be the number of codewords of weight αn for typical random linear codes. It is shown that $n^{-1}\log \bar{A}_{\alpha n} \leq R - 1 + H(\alpha) + o(1)$, which is a monotonically increasing function of α for $\alpha < 1/2$. Thus, we have that $n^{-1}\log \bar{A}_d \leq n^{-1}\log \bar{A}_{(\delta_{\rm GV}+\epsilon)n} \leq R - 1 + H(\delta_{\rm GV}+\epsilon) + o(1)$ for $\delta_{\rm GV} + \epsilon < 1/2$.

From the above results, for even d

$$\begin{aligned} n^{-1}\log\frac{\bar{A}_d}{\binom{d}{d/2}} &\leq R - 1 + H(\delta_{\rm GV}+\epsilon) - \delta_{\rm GV} + o(1) \\ &= H(\delta_{\rm GV}+\epsilon) - H(\delta_{\rm GV}) - \delta_{\rm GV} + o(1). \end{aligned} \tag{9}$$

It follows from the concavity of $H(x)$ that $H(\delta_{\rm GV}+\epsilon) - H(\delta_{\rm GV}) < \epsilon H'(\delta_{\rm GV})$, where $H'(x) = dH(x)/dx = \log((1-x)/x)$. If we choose $\epsilon < \delta_{\rm GV}/H'(\delta_{\rm GV})$, (9) is negative for large n, which means that the ratio $\bar{A}_d/\binom{d}{d/2}$ tends to zero as n tends to infinity. For odd d, the ratio $A_{d+1}/\binom{d}{(d+1)/2}$ tends to zero as n tends to infinity by a similar argument, since $n^{-1}\log\binom{d}{(d+1)/2} \geq n^{-1}\log\binom{\delta_{\rm GV}n}{(\delta_{\rm GV}n+1)/2} \geq \delta_{\rm GV}(H(1/2+1/(2\delta_{\rm GV}n)) - o(1)) \approx \delta_{\rm GV}$ and $n^{-1}\log \bar{A}_{d+1} \leq n^{-1}\log \bar{A}_{(\delta_{\rm GV}+\epsilon)n+1} \leq R - 1 + H(\delta_{\rm GV}+\epsilon+1/n) + o(1) \approx R - 1 + H(\delta_{\rm GV}+\epsilon)$. Therefore, the upper and lower bounds in Theorems 1 and 2 asymptotically coincide for typical random linear codes.

B. Correctable Errors With a Weight Greater Than Half the Minimum Distance

By generalizing the results in the previous section, we give a lower bound on $|LH_i(C \setminus \{\mathbf{0}\})|$ for $\lceil d/2 \rceil \leq i \leq \lfloor n/2 \rfloor$. This lower bound is also a lower bound on $|E_i^1(C)|$ based on the relation $M_i^1(C) \subseteq LH_i(T) \subseteq E_i^1(C)$ for a trial set T for C.

Theorem 3: Let C be a linear code with minimum distance d and T a trial set for C. We define $\mathcal{T}_i = |T_{2i-2}| + |T_{2i-1}| + |T_{2i}|$ and $\mathcal{T}_i' = |T_{2i-2}||T_{2i-1}| + |T_{2i-1}||T_{2i}| + |T_{2i}||T_{2i-2}|$. For an integer i with $\lceil d/2 \rceil \leq i \leq \lfloor n/2 \rfloor$, if

$$\binom{2i-3}{i} > \binom{2i - \lceil \frac{d}{2} \rceil}{i} \mathcal{T}_i$$

holds, then

$$\binom{2i-3}{i}\mathcal{T}_i - \binom{2i-\lceil \frac{d}{2} \rceil}{i}\left(\mathcal{T}_i^2 - \mathcal{T}_i'\right) \leq |LH_i(T)| \leq \binom{2i-1}{i}\mathcal{T}_i.$$

Proof: First we observe that $|LH_i(T)| = |LH^+(T_{2i-2}) \cup LH(T_{2i-1}) \cup LH^-(T_{2i})| = |LH^+(T_{2i-2})| + |LH(T_{2i-1}) \setminus LH^+(T_{2i-2})| + |LH^-(T_{2i}) \setminus \{LH^+(T_{2i-2}) \cup LH(T_{2i-1})\}|$. Let $\boldsymbol{c}$ and $\boldsymbol{c}'$ be codewords in $T_{2i-2} \cup T_{2i-1} \cup T_{2i}$. Then $w(\boldsymbol{c} \cap \boldsymbol{c}') = (w(\boldsymbol{c}) + w(\boldsymbol{c}') - w(\boldsymbol{c}+\boldsymbol{c}'))/2 \leq (2i+2i-d)/2 = 2i - \lceil d/2 \rceil$. Therefore, the number of common larger halves of weight i between $\boldsymbol{c}$ and $\boldsymbol{c}'$ is at most $\binom{2i-\lceil d/2 \rceil}{i}$. For $\boldsymbol{c} \in T_{2i-2} \cup T_{2i-1} \cup T_{2i}$, the number of larger halves of $\boldsymbol{c}$ with weight i is at least $\binom{2i-3}{i}$. Let $P = \binom{2i-\lceil d/2 \rceil}{i}$ and $Q = \binom{2i-3}{i}$. Then a lower bound on $|LH^+(T_{2i-2})|$ is $(Q - P|T_{2i-2}|)|T_{2i-2}|$. Similarly, lower bounds on $|LH(T_{2i-1}) \setminus LH^+(T_{2i-2})|$ and $|LH^-(T_{2i}) \setminus \{LH^+(T_{2i-2}) \cup LH(T_{2i-1})\}|$ are $(Q - P(|T_{2i-2}| + |T_{2i-1}|))|T_{2i-1}|$ and $(Q - P(|T_{2i-2}| + |T_{2i-1}| + |T_{2i}|))|T_{2i}|$, respectively. Thus, the lower bound follows.

The upper bound is obtained from the inequality $|LH_i(T)| \leq |LH^+(T_{2i-2})| + |LH(T_{2i-1})| + |LH^-(T_{2i})| \leq \binom{2i-3}{i}|T_{2i-2}| + \binom{2i-1}{i}|T_{2i-1}| + \binom{2i-1}{i}|T_{2i}| \leq \binom{2i-1}{i}\mathcal{T}_i$. □

The lower bound in the above theorem is based on the fact that the set of the larger halves of a trial set is contained in the set of uncorrectable errors. From the fact that a larger half is introduced to characterize the minimal uncorrectable errors and that the number of minimal uncorrectable errors is small for large weight, the bound in Theorem 3 is weak for large i. In addition, the condition that a trial set should satisfy is more restrictive.

Note that, for the case of weight $i = \lceil d/2 \rceil$, the bound in the previous section is better than that in Theorem 3.

IV. Correctable Errors for the First-Order Reed–Muller Codes

In this section, we study the error structure of the first-order Reed–Muller codes. Let RM_m denote the first-order Reed–Muller codes of length 2^m. Before presenting our results, we describe the relation between the correctable errors of RM_m and the nonlinearity of Boolean functions, and provide some properties of RM_m used later.

The binary rth-order Reed–Muller code of length 2^m corresponds to the Boolean functions of m variables with degree at most r. RM_m corresponds to the set of affine functions of m variables. The *nonlinearity* of a Boolean function f is defined as the minimum distance between f and affine functions, and is equal to the weight of the coset leader in the coset to which f belongs. Hence, the weight distribution of coset leaders of RM_m represents the distribution of the nonlinearity of Boolean functions. The number of Boolean functions of m variables with nonlinearity i is equal to $|E_i^0(\mathrm{RM}_m)| \cdot |\mathrm{RM}_m| = |E_i^0(\mathrm{RM}_m)|2^{m+1}$. Nonlinearity is an important criterion for cryptographic system, block ciphers and stream ciphers. Many studies have been conducted on the nonlinearity of Boolean functions in cryptography. For further details, see [17], [9] and references therein.

For an integer $m \geq 1$, RM_m is defined recursively as

$$\mathrm{RM}_m = \begin{cases} \mathbb{F}^2, & \text{for } m = 1 \\ \displaystyle\bigcup_{\boldsymbol{c} \in \mathrm{RM}_{m-1}} \{\boldsymbol{c} \circ \boldsymbol{c}, \boldsymbol{c} \circ \bar{\boldsymbol{c}}\}, & \text{for } m \geq 2 \end{cases}$$

where $\boldsymbol{u} \circ \boldsymbol{v}$ denotes the concatenation of $\boldsymbol{u}$ and $\boldsymbol{v}$, and $\overline{\boldsymbol{v}} = \mathbf{1} + \boldsymbol{v}$. Since all codewords in RM_m except the all-zero and the all-one codewords are minimum weight codewords, the set RM_m^* of the minimal codewords is $\mathrm{RM}_m \setminus \{\mathbf{0}, \mathbf{1}\}$.

From the conditions (1)–(3) we have

$$|LH^-(\boldsymbol{c})| = \binom{2^{m-1}-1}{2^{m-2}-1} = \frac{1}{2}\binom{2^{m-1}}{2^{m-2}}$$
$$|LH^+(\boldsymbol{c})| = \binom{2^{m-1}-1}{2^{m-2}+1}$$

for every $\boldsymbol{c} \in \mathrm{RM}_m^*$.

We define

$$S_m = \{l(\boldsymbol{c}) : \boldsymbol{c} \in \mathrm{RM}_m\}.$$

Then S_m forms message coordinates for RM_m, and $|S_m| = m+1$. For notational simplicity, we write $S_m = \{s_1, s_2, \ldots, s_{m+1}\}$, where $s_1 = 1$ and $s_i = 2^{i-2}+1$ for $2 \leq i \leq m+1$. We define the set $C_m(s_i) \subseteq \mathrm{RM}_m^*$ for $1 \leq i \leq m+1$ as follows:

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

Then $\mathrm{RM}_m^* = \bigcup_{i=1}^{m+1} C_m(s_i)$. We obtain

$$|C_m(s_i)| = \begin{cases} 2^m - 1, & \text{for } i = 1 \\ 2^{m+1-i}, & \text{for } 2 \leq i \leq m+1. \end{cases} \tag{10}$$

We provide some facts that are used later.

Lemma 3 ([8, Lemma 2]): For $2 \leq l \leq m$, let $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_l$ be codewords in RM_m^* such that $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_l$, and $\boldsymbol{1}$ are linearly independent. Then $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \cdots \cap \boldsymbol{c}_l) = 2^{m-l}$.

Lemma 4: Let $\boldsymbol{c}_1, \boldsymbol{c}_2$ be distinct codewords in RM_m^* such that $\boldsymbol{c}_1 \neq \overline{\boldsymbol{c}_2}$. Then $\{\boldsymbol{v} : w(\boldsymbol{v}) = 2^{m-2}, \boldsymbol{v} \subseteq \boldsymbol{c}_1, \boldsymbol{v} \subseteq \boldsymbol{c}_2\} = \{\boldsymbol{c}_1 \cap \boldsymbol{c}_2\}$.

Proof: Since $\boldsymbol{c}_1, \boldsymbol{c}_2$, and $\boldsymbol{1}$ are linearly independent, $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2) = 2^{m-2}$ by Lemma 3. Since $\boldsymbol{v} \subseteq \boldsymbol{c}_1$ and $\boldsymbol{v} \subseteq \boldsymbol{c}_2$, we have $\boldsymbol{v} \subseteq \boldsymbol{c}_1 \cap \boldsymbol{c}_2$. Then $\boldsymbol{v} = \boldsymbol{c}_1 \cap \boldsymbol{c}_2$ must hold. □

Lemma 5: Let $\boldsymbol{c}_1, \boldsymbol{c}_2$ be distinct codewords in RM_m^*. Then

$$LH^-(\boldsymbol{c}_1) \cap LH^-(\boldsymbol{c}_2) = \begin{cases} \{\boldsymbol{c}_1 \cap \boldsymbol{c}_2\}, & \text{if } l(\boldsymbol{c}_1) = l(\boldsymbol{c}_2), \\ \emptyset, & \text{otherwise.} \end{cases}$$

Proof: Suppose $LH^-(\boldsymbol{c}_1) \cap LH^-(\boldsymbol{c}_2)$ is not empty. Then for any $\boldsymbol{v} \in LH^-(\boldsymbol{c}_1) \cap LH^-(\boldsymbol{c}_2)$, $l(\boldsymbol{v}) = l(\boldsymbol{c}_1) = l(\boldsymbol{c}_2)$ from (3). If $l(\boldsymbol{c}_1) = l(\boldsymbol{c}_2)$, then $l(\boldsymbol{c}_1 \cap \boldsymbol{c}_2) = l(\boldsymbol{c}_1) = l(\boldsymbol{c}_2)$ and $\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \in LH^-(\boldsymbol{c}_1) \cap LH^-(\boldsymbol{c}_2)$. The lemma follows from these facts and Lemma 1. □

Lemma 6: Let $\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3$ be distinct codewords in RM_m^*. For $m \geq 3$ (see the equation shown at the bottom of the page).

Proof: The statement follows from the fact that $w(\boldsymbol{c}_1 + \boldsymbol{c}_2 + \boldsymbol{c}_3) = w(\boldsymbol{c}_1) + w(\boldsymbol{c}_2) + w(\boldsymbol{c}_3) - 2(w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2) + w(\boldsymbol{c}_2 \cap \boldsymbol{c}_3) + w(\boldsymbol{c}_1 \cap \boldsymbol{c}_3)) + 4w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \boldsymbol{c}_3)$ and Lemma 3. □

A. Correctable Errors With a Weight of Half the Minimum Distance

In this section, we determine the number of correctable errors with a weight of half the minimum distance for RM_m. The proof has already been provided in [8]; however, here we present a slightly simpler proof.

In the proof of [8], the cosets that have uncorrectable errors of weight 2^{m-2} are partitioned into three types. Then the number of cosets for each type is determined, and the structure of cosets containing the vectors of weight 2^{m-2} is revealed. On the other hand, in our proof, we first observe that the uncorrectable errors of weight 2^{m-2} are equivalent to the set of larger halves of weight 2^{m-2} of codewords in RM_m^*. Next, we count the number of larger halves that are common among more than one codeword leads to the result. Our approach does not clarify the structure of cosets containing the vectors of weight 2^{m-2}. Therefore, our proof leads directly to the result and is thus simpler than that of [8].

From (5) and (7) we have $E_{2^{m-2}}^1(\mathrm{RM}_m) = LH^-(\mathrm{RM}_m^*)$. There may be some $\boldsymbol{v} \in E_{2^{m-2}}^1(\mathrm{RM}_m)$ that is a larger half of more than one codeword in RM_m^*. Let $i \geq 1$ be an integer. We define

$$D_m^i = \big\{\boldsymbol{v} \in E_{2^{m-2}}^1(\mathrm{RM}_m) \\ : \big|\{\boldsymbol{c} \in \mathrm{RM}_m^* : \boldsymbol{v} \in LH^-(\boldsymbol{c})\}\big| = i\big\}.$$

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

$$\left|E_{2^{m-2}}^1(\mathrm{RM}_m)\right| = \sum_{i \geq 1} \left|D_m^i\right|. \tag{11}$$

The following lemma states that more than three codewords in RM_m^* cannot have a common larger half of weight 2^{m-2}.

Lemma 7: $D_m^i = \emptyset$ for $m \geq 2$ and $i \geq 4$.

Proof: For $\boldsymbol{v} \in E_{2^{m-2}}^1(\mathrm{RM}_m)$, suppose that there are four distinct codewords $\boldsymbol{c}_j \in \mathrm{RM}_m^*$ with $1 \leq j \leq 4$ such that $\boldsymbol{v} \in LH^-(\boldsymbol{c}_j)$. It holds from the condition (1) that $\boldsymbol{v} \subseteq \bigcap_{j=1}^4 \boldsymbol{c}_j$. Since the weight of $\boldsymbol{v}$ is 2^{m-2}, from Lemma 6, a sum of any three $\boldsymbol{c}_j$'s must be the all-one codeword, which is impossible if $\boldsymbol{c}_j$'s are distinct. □

Corollary 3: For $m \geq 2$

$$\left|E_{2^{m-2}}^1(\mathrm{RM}_m)\right| = \left|D_m^1\right| + \left|D_m^2\right| + \left|D_m^3\right| \tag{12}$$
$$(2^m - 1)\binom{2^{m-1}}{2^{m-2}} = \left|D_m^1\right| + 2\left|D_m^2\right| + 3\left|D_m^3\right|. \tag{13}$$

$$w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \boldsymbol{c}_3) = \begin{cases} 2^{m-2}, & \text{if } \boldsymbol{c}_1 + \boldsymbol{c}_2 + \boldsymbol{c}_3 = \boldsymbol{1} \\ 0, & \text{if } \boldsymbol{c}_1 + \boldsymbol{c}_2 + \boldsymbol{c}_3 = \boldsymbol{0} \\ & \text{or } \boldsymbol{c}_i + \boldsymbol{c}_j = \boldsymbol{1} \text{ for some } i, j \in \{1,2,3\} \\ 2^{m-3}, & \text{otherwise.} \end{cases}$$

Proof: Equation (12) is obtained from (11) and Lemma 7. The left-hand side of (13) is the product of $|\mathrm{RM}_m^*| = 2^{m+1} - 2$ and $|LH^-(\boldsymbol{c})|$ for $\boldsymbol{c} \in \mathrm{RM}_m^*$, which is equal to the right-hand side by Lemma 7. □

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

Lemma 8: For $m \geq 2$

$$D_m^2 = \bigcup_{s_i \in S_m \setminus \{s_1, s_{m+1}\}} \{\boldsymbol{c}_1 \cap \boldsymbol{c}_2 : \boldsymbol{c}_1, \boldsymbol{c}_2 \in C_m(s_i), \boldsymbol{c}_1 \neq \boldsymbol{c}_2\},$$
$$D_m^3 = \{\boldsymbol{c}_1 \cap \boldsymbol{c}_2 : \boldsymbol{c}_1, \boldsymbol{c}_2 \in C_m(s_1), \boldsymbol{c}_1 \neq \boldsymbol{c}_2\}.$$

Proof: Suppose two distinct codewords $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathrm{RM}_m^*$ have a common larger half $\boldsymbol{v}$ of weight 2^{m-2}. Then $l(\boldsymbol{c}_1) = l(\boldsymbol{c}_2)$ and $\boldsymbol{v} = \boldsymbol{c}_1 \cap \boldsymbol{c}_2$ from Lemma 5. We consider codewords in $C_m(s_i)$ only for $1 \leq i \leq m$, since there is only one codeword in $C_m(s_i)$ for $i = m+1$. If another codeword $\boldsymbol{c}_3 \in \mathrm{RM}_m^*$ has the same larger half $\boldsymbol{v}$, then $\boldsymbol{c}_3 = \overline{\boldsymbol{c}_1 + \boldsymbol{c}_2}$ from Lemma 6, and the condition $l(\boldsymbol{c}_1) = l(\boldsymbol{c}_2) = l(\overline{\boldsymbol{c}_1 + \boldsymbol{c}_2})$ holds if and only if $\boldsymbol{c}_1, \boldsymbol{c}_2 \in C_m(s_1)$. □

Corollary 4: For $m \geq 2$

$$|D_m^2| = |D_m^3| = \frac{1}{3}\binom{2^m - 1}{2}.$$

Proof: From the proof of Lemma 8, for each pair of distinct codewords $\boldsymbol{c}_1, \boldsymbol{c}_2 \in C_m(s_1)$, they and $\overline{\boldsymbol{c}_1 + \boldsymbol{c}_2} \in C_m(s_1)$ have the common larger half. Each pair of distinct codewords in $C_m(s_i)$ for $2 \leq i \leq m$ has the common larger half. Therefore, we have

$$|D_m^3| = \frac{|C_m(s_1)|(|C_m(s_1)| - 1)}{6} = \frac{1}{3}\binom{2^m - 1}{2}$$

and

$$|D_m^2| = \sum_{i=2}^{m} \frac{|C_m(s_i)|(|C_m(s_i)| - 1)}{2} = \frac{1}{3}\binom{2^m - 1}{2}$$

from (10). □

The number of uncorrectable errors of weight half the minimum distance is determined by Corollaries 3 and 4.

Theorem 4 ([8]): For $m \geq 2$

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

The number of correctable errors is obtained by the equation $|E_{2^{m-2}}^0(\mathrm{RM}_m)| + |E_{2^{m-2}}^1(\mathrm{RM}_m)| = \binom{2^m}{2^{m-2}}$. These expressions can be evaluated from (8) as follows:

$$|E_{2^{m-2}}^0(\mathrm{RM}_m)| \approx \frac{2}{\sqrt{3\pi 2^{m-1}}}\left(\frac{16}{3\sqrt{3}}\right)^{2^{m-1}}$$
$$|E_{2^{m-2}}^1(\mathrm{RM}_m)| \approx \frac{2^{2^{m-1}+\frac{m}{2}+1}}{\sqrt{\pi}}.$$

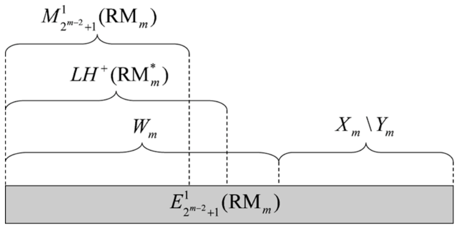
$M_{2^{m-2}+1}^1(\mathrm{RM}_m)$
$LH^+(\mathrm{RM}_m^*)$
W_m
$X_m \setminus Y_m$
$E_{2^{m-2}+1}^1(\mathrm{RM}_m)$

Fig. 1. Structure of $E_{2^{m-2}+1}^1(\mathrm{RM}_m)$.

B. Correctable Errors With a Weight of Half the Minimum Distance Plus One

We determine the number of correctable errors with a weight of half the minimum distance plus one for the first-order Reed–Muller codes. We partition the set $E_{2^{m-2}+1}^1(\mathrm{RM}_m)$ into two subsets. The first one is the set of vectors of weight $2^{m-2} + 1$ that are covered by a codeword in RM_m^*. The set is defined as

$$W_m = \left\{\boldsymbol{v} \in \mathbb{F}_{2^{m-2}+1}^n : \boldsymbol{v} \subseteq \boldsymbol{c} \ \text{ for some } \ \boldsymbol{c} \in \mathrm{RM}_m^*\right\} \tag{14}$$

where

$$\mathbb{F}_i^n = \{\boldsymbol{v} \in \mathbb{F}^n : w(\boldsymbol{v}) = i\} \quad \text{for} \ \ 1 \leq i \leq n.$$

Note that every $\boldsymbol{v} \in W_m$ is an uncorrectable error because the coset containing $\boldsymbol{v}$ contains the smaller weight vector $\boldsymbol{c} + \boldsymbol{v}$.

The second subset is the set of the remaining vectors, $E_{2^{m-2}+1}^1(\mathrm{RM}_m) \setminus W_m$. Here note that W_m contains $LH^+(\mathrm{RM}_m^*)$, which in turn contains all minimal uncorrectable errors. Hence, a vector in the second set is a nonminimal vector. Such a vector covers a minimal uncorrectable error of weight 2^{m-2}. Since the set of minimal uncorrectable errors of weight 2^{m-2} is $LH^-(\mathrm{RM}_m^*)$, we consider the set of vectors obtained by adding a weight-one vector to vectors in $LH^-(\mathrm{RM}_m^*)$ that are not covered by codewords in RM_m^*. We define

$$\mathbb{F}_1^n(\boldsymbol{c}) = \{\boldsymbol{e} \in \mathbb{F}_1^n : \boldsymbol{e} \cap \boldsymbol{c} = \boldsymbol{0}\}$$

for $\boldsymbol{c} \in \mathrm{RM}_m^*$. Then, the second subset can be represented as $\mathrm{X}_m \setminus \mathrm{Y}_m$, where

$$\mathrm{X}_m = \bigcup_{\boldsymbol{c} \in \mathrm{RM}_m^*} \{\boldsymbol{v} + \boldsymbol{e} : \boldsymbol{v} \in LH^-(\boldsymbol{c}), \boldsymbol{e} \in \mathbb{F}_1^n(\boldsymbol{c})\}$$
$$\mathrm{Y}_m = \{\boldsymbol{u} \in \mathrm{X}_m : \boldsymbol{u} \subseteq \boldsymbol{c} \ \text{ for some } \ \boldsymbol{c} \in \mathrm{RM}_m^*\}$$

and, thus, we have

$$|E_{2^{m-2}+1}^1(\mathrm{RM}_m)| = |W_m| + |X_m \setminus Y_m|. \tag{15}$$

The relations between $M^1(\mathrm{RM}_m)$, $LH^+(\mathrm{RM}_m^*)$, W_m, and $X_m \setminus Y_m$ in $E_{2^{m-2}+1}^1(\mathrm{RM}_m)$ are shown in Fig. 1.

The set W_m contains $\binom{2^{m-1}}{2^{m-2}+1}$ vectors for each codeword in RM_m^*, and all $|\mathrm{RM}_m^*| \cdot \binom{2^{m-1}}{2^{m-2}+1}$ such vectors are distinct as shown in the following lemma.

Lemma 9: Let $\boldsymbol{c}$ be a codeword in RM_m^* and $\boldsymbol{v}$ a vector of weight $2^{m-2} + 1$ such that $\boldsymbol{v} \subseteq \boldsymbol{c}$. Then there is no other codeword $\boldsymbol{c}'$ in RM_m^* such that $\boldsymbol{v} \subseteq \boldsymbol{c}'$.

Proof: If $\boldsymbol{v} \subseteq \boldsymbol{c}'$, then $\boldsymbol{c}' \neq \bar{\boldsymbol{c}}$ and $w(\boldsymbol{c} \cap \boldsymbol{c}') \geq w(\boldsymbol{v}) = 2^{m-2}+1$. These contradict Lemma 3. □

Now we have

$$|W_m| = 2(2^m-1)\binom{2^{m-1}}{2^{m-2}+1}.$$

Next, we will determine the size of $X_m \setminus Y_m$. For X_m and Y_m, we define the corresponding multisets $\tilde{\mathrm{X}}_m$ and $\tilde{\mathrm{Y}}_m$. That is, $\tilde{\mathrm{X}}_m$ is a multiset obtained by taking the union of the sets of vectors obtained by adding vectors $\boldsymbol{e} \in \mathbb{F}_1^n(\boldsymbol{c})$ to larger halves $\boldsymbol{v} \in LH^-(\boldsymbol{c})$ for each $\boldsymbol{c} \in \mathrm{RM}_m^*$. The set $\tilde{\mathrm{Y}}_m$ is a multiset of vectors in $\tilde{\mathrm{X}}_m$ that are covered by some codeword in RM_m^*. Then we have

$$\begin{aligned}|\tilde{\mathrm{X}}_m| &= |\mathrm{RM}_m^*| \cdot \binom{2^{m-1}-1}{2^{m-2}-1} \cdot 2^{m-1} \\ &= 2^{m-1}(2^m-1)\binom{2^{m-1}}{2^{m-2}}\end{aligned} \quad (16)$$

since the number of larger halves of each codeword is $\binom{2^{m-1}-1}{2^{m-2}-1}$ from (1)–(3), and there are 2^{m-1} choices for $\boldsymbol{e} \in \mathbb{F}_1^n(\boldsymbol{c})$. We determine $|\mathrm{X}_m \setminus \mathrm{Y}_m|$ by using $\tilde{\mathrm{X}}_m$ and $\tilde{\mathrm{Y}}_m$. First we show that the multiplicity of vectors in $\tilde{\mathrm{X}}_m$ is not greater than two.

Lemma 10: The multiplicity of a vector in $\tilde{\mathrm{X}}_m$ is less than or equal to two for $m \geq 5$.

Proof: Let $\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3$ be codewords in RM_m^*. Suppose there exist $\boldsymbol{v}_i, \boldsymbol{e}_i$ for $1 \leq i \leq 3$ such that $\boldsymbol{v}_i \in LH^-(\boldsymbol{c}_i)$, $\boldsymbol{e}_i \in \mathbb{F}_1^n(\boldsymbol{c}_i)$, and $\boldsymbol{v}_i + \boldsymbol{e}_i = \boldsymbol{v}_j + \boldsymbol{e}_j$ for any $i, j \in \{1,2,3\}$. From the definition of $\tilde{\mathrm{X}}_m$, it easily follows that $\boldsymbol{c}_1, \boldsymbol{c}_2$, and $\boldsymbol{c}_3$ are all distinct.

First we prove that $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \boldsymbol{c}_3) = 2^{m-3}$. It follows from the assumption that $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \boldsymbol{c}_3) \neq 0$ for $m \geq 4$ and that $\boldsymbol{v}_i \neq \overline{\boldsymbol{v}_j}$ for any $i, j \in \{1,2,3\}$ for $m \geq 3$. By Lemma 6, it is sufficient to show that $\boldsymbol{c}_1 + \boldsymbol{c}_2 + \boldsymbol{c}_3 \neq \mathbf{1}$. Suppose $\boldsymbol{c}_1 + \boldsymbol{c}_2 + \boldsymbol{c}_3 = \mathbf{1}$. Then $\overline{\boldsymbol{c}_1} \cap \overline{\boldsymbol{c}_2} \cap \overline{\boldsymbol{c}_3} = \mathbf{0}$, and, thus, $\boldsymbol{e}_1 \cap \boldsymbol{e}_2 \cap \boldsymbol{e}_3 = \mathbf{0}$, leading to a contradiction. Hence, $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \boldsymbol{c}_3) = 2^{m-3}$.

Since $\boldsymbol{v}_i \subseteq \boldsymbol{c}_i$ for any i, $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \boldsymbol{c}_3) \geq w(\boldsymbol{v}_1 \cap \boldsymbol{v}_2 \cap \boldsymbol{v}_3) \geq 2^{m-2}-2$. Thus, we have $2^{m-3} \geq 2^{m-2}-2$. A contradiction arises for $m \geq 5$. □

It is easy to see from the definitions that if $\boldsymbol{x} \in \mathrm{X}_m \cap \mathrm{Y}_m$, then $\boldsymbol{x}$ has the same multiplicity in $\tilde{\mathrm{X}}_m$ and $\tilde{\mathrm{Y}}_m$. Thus, the size of $\mathrm{X}_m \setminus \mathrm{Y}_m$ is represented as follows:

$$|\mathrm{X}_m \setminus \mathrm{Y}_m| = |\tilde{\mathrm{X}}_m| - |\tilde{\mathrm{Y}}_m| - \frac{|\tilde{\mathrm{Z}}_m|}{2} \quad (17)$$

where $\tilde{\mathrm{Z}}_m$ is the multiset defined as

$$\tilde{\mathrm{Z}}_m = \left\{\boldsymbol{u} \in \tilde{\mathrm{X}}_m : \begin{array}{c}\boldsymbol{u} \nsubseteq \boldsymbol{c} \text{ for every } \boldsymbol{c} \in \mathrm{RM}_m^*, \\ \text{the multiplicity of } \boldsymbol{u} \text{ is two}\end{array}\right\}.$$

We will determine $|\tilde{\mathrm{Y}}_m|$ and $|\tilde{\mathrm{Z}}_m|$. Note that

$$|\tilde{\mathrm{Y}}_m| = \sum_{\boldsymbol{c}_1 \in \mathrm{RM}_m^*} \sum_{\boldsymbol{c}_2 \in \mathrm{RM}_m^*} \left|\left\{(\boldsymbol{v}, \boldsymbol{e}) : \begin{array}{c}\boldsymbol{v} \in LH^-(\boldsymbol{c}_1), \\ \boldsymbol{e} \in \mathbb{F}_1^n(\boldsymbol{c}_1), \boldsymbol{v} + \boldsymbol{e} \subseteq \boldsymbol{c}_2\end{array}\right\}\right|.$$

The next lemma is useful to determine $|\tilde{\mathrm{Y}}_m|$.

Lemma 11: For $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathrm{RM}_m^*$, if $\{(\boldsymbol{v}, \boldsymbol{e}) : \boldsymbol{v} \in LH^-(\boldsymbol{c}_1), \boldsymbol{e} \in \mathbb{F}_1^n(\boldsymbol{c}_1), \boldsymbol{v} + \boldsymbol{e} \subseteq \boldsymbol{c}_2\}$ is not empty, then

$$\boldsymbol{c}_1 \neq \boldsymbol{c}_2 \text{ and } l(\boldsymbol{c}_1) \in S(\boldsymbol{c}_2). \quad (18)$$

If (18) holds, the set is equivalent to

$$\{(\boldsymbol{c}_1 \cap \boldsymbol{c}_2, \boldsymbol{e}) : \boldsymbol{e} \in \mathbb{F}_1^n(\boldsymbol{c}_1), S(\boldsymbol{e}) \subseteq S(\boldsymbol{c}_2) \setminus S(\boldsymbol{c}_1)\}. \quad (19)$$

Proof: If $\boldsymbol{c}_1 = \boldsymbol{c}_2$, we cannot choose $\boldsymbol{e}$ such that $\boldsymbol{e} \in \mathbb{F}_1^n(\boldsymbol{c}_1)$ and $\boldsymbol{v} + \boldsymbol{e} \subseteq \boldsymbol{c}_2$. If $l(\boldsymbol{c}_1) \notin S(\boldsymbol{c}_2)$, there is no $\boldsymbol{v}$ satisfying $\boldsymbol{v} \subseteq \boldsymbol{c}_2$ since $l(\boldsymbol{c}_1) = l(\boldsymbol{v})$. Next we prove the equivalence of the sets. Using Lemma 4, we have $\boldsymbol{v} = \boldsymbol{c}_1 \cap \boldsymbol{c}_2$. The fact that $\boldsymbol{e}$ is selected as $S(\boldsymbol{e}) \subseteq S(\boldsymbol{c}_2) \setminus S(\boldsymbol{c}_1)$ is obvious. □

For each $\boldsymbol{c}_1 \in \mathrm{RM}_m^*$, the number of codewords $\boldsymbol{c}_2$ satisfying (18) is $|\mathrm{RM}_m|/2 - 2 = 2^m - 2$. For $\boldsymbol{c}_1$ and $\boldsymbol{c}_2$ satisfying (18), there is only one $\boldsymbol{c}_1 \cap \boldsymbol{c}_2$, and there are $|S(\boldsymbol{c}_2) \setminus S(\boldsymbol{c}_1)| = 2^{m-2}$ choices of $\boldsymbol{e}$, and, thus, the size of (19) is 2^{m-2}. Therefore, we have

$$\begin{aligned}|\tilde{\mathrm{Y}}_m| &= |\mathrm{RM}_m^*| \cdot (2^m-2) \cdot 2^{m-2} \\ &= 2^m(2^m-1)(2^{m-1}-1).\end{aligned} \quad (20)$$

The following lemma is useful to derive $|\tilde{\mathrm{Z}}_m|$.

Lemma 12: Let $\boldsymbol{u} \in \tilde{\mathrm{X}}_m$ of multiplicity two. That is, $\boldsymbol{u}$ is represented as $\boldsymbol{u} = \boldsymbol{v}_1 + \boldsymbol{e}_1 = \boldsymbol{v}_2 + \boldsymbol{e}_2$ where $\boldsymbol{v}_i \in LH^-(\boldsymbol{c}_i)$, $\boldsymbol{c}_i \in \mathrm{RM}_m^*$, $\boldsymbol{e}_i \in \mathbb{F}_1^n(\boldsymbol{c}_i)$ for $i = 1, 2$, and $\boldsymbol{c}_1 \neq \boldsymbol{c}_2$. Then, for $m \geq 4$, there exists $\boldsymbol{c}_3 \in \mathrm{RM}_m^*$ such that $\boldsymbol{u} \subseteq \boldsymbol{c}_3$ if and only if $\boldsymbol{e}_1 = \boldsymbol{e}_2$.

Proof: (For the "only if" part) We have that $\boldsymbol{c}_1 \neq \overline{\boldsymbol{c}_3}$ from $\boldsymbol{v}_1 + \boldsymbol{e}_1 \subseteq \boldsymbol{c}_3$, and that $\boldsymbol{c}_1 \neq \boldsymbol{c}_3$ from $\boldsymbol{v}_1 + \boldsymbol{e}_1 \nsubseteq \boldsymbol{c}_1$ and $\boldsymbol{v}_1 + \boldsymbol{e}_1 \subseteq \boldsymbol{c}_3$. Since $\boldsymbol{v}_1 \subseteq \boldsymbol{c}_1$ and $\boldsymbol{v}_1 \subseteq \boldsymbol{c}_3$, we have $\boldsymbol{v}_1 = \boldsymbol{c}_1 \cap \boldsymbol{c}_3$ by Lemma 4. Equivalently, $\boldsymbol{v}_2 = \boldsymbol{c}_2 \cap \boldsymbol{c}_3$. Then $\boldsymbol{v}_1 \cap \boldsymbol{v}_2 = \boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \boldsymbol{c}_3$, and, hence, $w(\boldsymbol{v}_1 \cap \boldsymbol{v}_2) = w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \boldsymbol{c}_3)$. On one hand, $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \boldsymbol{c}_3)$ is either 2^{m-2}, 2^{m-3}, or 0 from Lemma 6, because $\boldsymbol{c}_1$, $\boldsymbol{c}_2$, and $\boldsymbol{c}_3$ are distinct. On the other hand, $w(\boldsymbol{v}_1 \cap \boldsymbol{v}_2)$ is 2^{m-2} if $\boldsymbol{v}_1 = \boldsymbol{v}_2$, and is $2^{m-2}-1$ otherwise because $\boldsymbol{v}_1 + \boldsymbol{e}_1 = \boldsymbol{v}_2 + \boldsymbol{e}_2$. Therefore, $w(\boldsymbol{v}_1 \cap \boldsymbol{v}_2) = 2^{m-2}$ for $m \geq 4$. Hence, $\boldsymbol{v}_1 = \boldsymbol{v}_2$, and, thus, $\boldsymbol{e}_1 = \boldsymbol{e}_2$.

(For the "if" part) Since $\boldsymbol{v}_1 \neq \mathbf{0}$, $\boldsymbol{v}_1 \subseteq \boldsymbol{c}_1$, and $\boldsymbol{v}_1 = \boldsymbol{v}_2 \subseteq \boldsymbol{c}_2$, we have $\boldsymbol{c}_1 \neq \overline{\boldsymbol{c}_2}$. Then we have $\boldsymbol{v}_1 = \boldsymbol{c}_1 \cap \boldsymbol{c}_2$ by Lemma 4. Thus, $\boldsymbol{v}_1 = \boldsymbol{c}_1 \cap \boldsymbol{c}_2 \subseteq \overline{\boldsymbol{c}_1 + \boldsymbol{c}_2}$. Since $\boldsymbol{e}_1 \cap \boldsymbol{c}_1 = \boldsymbol{e}_1 \cap \boldsymbol{c}_2 = \mathbf{0}$, we have $\boldsymbol{e}_1 \subseteq \overline{\boldsymbol{c}_1 + \boldsymbol{c}_2}$. Note that $\overline{\boldsymbol{c}_1 + \boldsymbol{c}_2} \in \mathrm{RM}_m^*$ since $\overline{\boldsymbol{c}_1 + \boldsymbol{c}_2} \neq \mathbf{0}, \mathbf{1}$. By considering $\boldsymbol{c}_3 = \overline{\boldsymbol{c}_1 + \boldsymbol{c}_2}$, there is $\boldsymbol{c}_3 \in \mathrm{RM}_m^*$ such that $\boldsymbol{u} = \boldsymbol{v}_1 + \boldsymbol{e}_1 \subseteq \boldsymbol{c}_3$. □

From Lemma 12, we obtain

$$|\tilde{\mathrm{Z}}_m| = \sum_{\boldsymbol{c}_1 \in \mathrm{RM}_m^*} \left| \bigcup_{\boldsymbol{c}_2 \in \mathrm{RM}_m^* \setminus \{\boldsymbol{c}_1\}} \mathcal{Z}_m(\boldsymbol{c}_1, \boldsymbol{c}_2) \right|$$

where

$$\mathcal{Z}_m(\boldsymbol{c}_1, \boldsymbol{c}_2) = \left\{ (\boldsymbol{v}_1, \boldsymbol{e}_1) : \begin{array}{c} \boldsymbol{v}_1 \in LH^-(\boldsymbol{c}_1), \boldsymbol{e}_1 \in \mathbb{F}_1^n(\boldsymbol{c}_1) \\ \text{there are } \boldsymbol{v}_2 \in LH^-(\boldsymbol{c}_2) \text{ and } \boldsymbol{e}_2 \in \mathbb{F}_1^n(\boldsymbol{c}_2) \\ \text{such that } \boldsymbol{v}_1 + \boldsymbol{e}_1 = \boldsymbol{v}_2 + \boldsymbol{e}_2, \boldsymbol{e}_1 \neq \boldsymbol{e}_2 \end{array} \right\}.$$

It is easily inferred that

$$\mathcal{Z}_m(\boldsymbol{c}_1,\boldsymbol{c}_2) = \left\{ (\boldsymbol{w}+\boldsymbol{e}_2,\boldsymbol{e}_1) : \begin{array}{c} \boldsymbol{w}\in\mathbb{F}^n_{2^{m-2}-1}, \boldsymbol{w}\subseteq \boldsymbol{c}_1\cap\boldsymbol{c}_2 \\ \boldsymbol{e}_1\in\mathbb{F}^n_1(\boldsymbol{c}_1), \boldsymbol{e}_2\in\mathbb{F}^n_1(\boldsymbol{c}_2), \boldsymbol{e}_1\neq\boldsymbol{e}_2, \\ l(\boldsymbol{w}+\boldsymbol{e}_2)=l(\boldsymbol{c}_1), l(\boldsymbol{w}+\boldsymbol{e}_1)=l(\boldsymbol{c}_2) \end{array} \right\}.$$

Fixing $\boldsymbol{c}_1\in\mathrm{RM}^*_m$, to determine the size of $\mathcal{Z}_m(\boldsymbol{c}_1,\boldsymbol{c}_2)$, we consider three cases depending on $\boldsymbol{c}_2$. Hereafter, we omit the conditions $\boldsymbol{w}\in\mathbb{F}^n_{2^{m-2}-1}, \boldsymbol{w}\subseteq\boldsymbol{c}_1\cap\boldsymbol{c}_2, \boldsymbol{e}_1\in\mathbb{F}^n_1, \boldsymbol{e}_2\in\mathbb{F}^n_1$ in the expression for $\mathcal{Z}_m(\boldsymbol{c}_1,\boldsymbol{c}_2)$.

1) $l(\boldsymbol{c}_1)=l(\boldsymbol{c}_2)$. It can be shown that

$$\mathcal{Z}_m(\boldsymbol{c}_1,\boldsymbol{c}_2) = \left\{ (\boldsymbol{w}+\boldsymbol{e}_2,\boldsymbol{e}_1) : \begin{array}{c} l(\boldsymbol{w})=l(\boldsymbol{c}_1\cap\boldsymbol{c}_2) \\ S(\boldsymbol{e}_2)\subseteq S(\boldsymbol{c}_1)\setminus S(\boldsymbol{c}_2), \\ S(\boldsymbol{e}_1)\subseteq S(\boldsymbol{c}_2)\setminus S(\boldsymbol{c}_1) \end{array} \right\}.$$

This set is not empty for all $\boldsymbol{c}_2$ satisfying $l(\boldsymbol{c}_1)=l(\boldsymbol{c}_2)$. For each $\boldsymbol{c}_1\in C_m(s_i)$ there are $|C_m(s_i)|-1$ such codewords $\boldsymbol{c}_2$ in RM^*_m. The size of the set is $(2^{m-2}-1)\cdot 2^{m-2}\cdot 2^{m-2}$.

2) $l(\boldsymbol{c}_1)>l(\boldsymbol{c}_2)$. There are two subcases.

a) $l(\boldsymbol{c}_1)\in S(\boldsymbol{c}_2)$. Then

$$\mathcal{Z}_m(\boldsymbol{c}_1,\boldsymbol{c}_2) = \left\{ (\boldsymbol{w}+\boldsymbol{e}_2,\boldsymbol{e}_1) : \begin{array}{c} S(\boldsymbol{e}_1)=\{l(\boldsymbol{c}_2)\}, \\ S(\boldsymbol{e}_2)\subseteq S(\boldsymbol{c}_1)\setminus S(\boldsymbol{c}_2) \end{array} \right\}.$$

This set is not empty for all $\boldsymbol{c}_2$ satisfying the conditions. For each $\boldsymbol{c}_1\in C_m(s_i)$ with $i\geq 2$, there are $((\sum_{j<i}|C_m(s_j)|+1)/2-1)$ such codewords $\boldsymbol{c}_2$ in RM^*_m. The size of the set is $(2^{m-2}-1)\cdot 2^{m-2}$.

b) $l(\boldsymbol{c}_1)\notin S(\boldsymbol{c}_2)$. Then

$$\mathcal{Z}_m(\boldsymbol{c}_1,\boldsymbol{c}_2) = \left\{ (\boldsymbol{w}+\boldsymbol{e}_2,\boldsymbol{e}_1) : \begin{array}{c} S(\boldsymbol{e}_1)=\{l(\boldsymbol{c}_2)\} \\ S(\boldsymbol{e}_2)=\{l(\boldsymbol{c}_1)\} \end{array} \right\}.$$

This set is not empty for all $\boldsymbol{c}_2$ satisfying the conditions except for the case $\boldsymbol{c}_1=\overline{\boldsymbol{c}_2}$. For each $\boldsymbol{c}_1\in C_m(s_i)$ with $i\geq 2$, there are $((\sum_{j<i}|C_m(s_j)|+1)/2-1)$ such codewords $\boldsymbol{c}_2$ in RM^*_m. The size of the set is 2^{m-2}.

3) $l(\boldsymbol{c}_1)<l(\boldsymbol{c}_2)$. The number of vectors we should count is equal to that for the Case 2.

From the above analysis, we have

$$\begin{aligned} |\tilde{\mathrm{Z}}_m| &= \sum_{i=1}^{m+1}|C_m(s_i)| \\ &\quad\times(|C_m(s_i)|-1)(2^{m-2}-1)(2^{m-2})^2 \\ &\quad+2\sum_{i=2}^{m+1}|C_m(s_i)| \\ &\quad\times\left(\frac{1}{2}\left(\sum_{j=1}^{i-1}|C_m(s_j)|+1\right)-1\right) \\ &\quad\times\left((2^{m-2}-1)2^{m-2}+2^{m-2}\right) \\ &=\Bigg((2^m-1)(2^m-2) \\ &\quad+\frac{1}{3}(2^{2m}-1)-(2^m-1)\Bigg) \\ &\quad\times(2^{m-2}-1)(2^{m-2})^2 \\ &\quad+2\left((2^m-1)^2-\frac{1}{3}(2^{2m}-1)\right)(2^{m-2})^2 \\ &=2^{2m-3}\binom{2^m}{3}. \end{aligned} \tag{21}$$

From (15), (16), (17), (20), and (21), we determine the number of uncorrectable errors of weight $2^{m-2}+1$ for RM_m.

Theorem 5: For $m\geq 5$

$$\left|E^1_{2^{m-2}+1}(\mathrm{RM}_m)\right| = (2^m-1)(2^{m-1}+4) \times\binom{2^{m-1}}{2^{m-2}+1}-(4^{m-2}+3)\binom{2^m}{3}.$$

The number of correctable errors of weight $2^{m-2}+1$ is obtained from the equation $|E^0_{2^{m-2}+1}(\mathrm{RM}_m)|+|E^1_{2^{m-2}+1}(\mathrm{RM}_m)|=\binom{2^m}{2^{m-2}+1}$. Using (8), the expressions for $|E^0_{2^{m-2}+1}(\mathrm{RM}_m)|$ and $|E^1_{2^{m-2}+1}(\mathrm{RM}_m)|$ can be evaluated as

$$|E^0_{2^{m-2}+1}(\mathrm{RM}_m)| \approx \sqrt{\frac{3}{\pi 2^{m-3}}}\left(\frac{16}{3\sqrt{3}}\right)^{2^{m-1}}$$

$$|E^1_{2^{m-2}+1}(\mathrm{RM}_m)| \approx \frac{2^{2^{m-1}+\frac{3}{2}m}}{\sqrt{\pi}}.$$

C. Minimal Uncorrectable Errors

In this section, we determine the weight distribution of the minimal uncorrectable errors in the first-order Reed–Muller codes, which is defined as $(|M^1_0(\mathrm{RM}_m)|, |M^1_1(\mathrm{RM}_m)|, \ldots, |M^1_n(\mathrm{RM}_m)|)$. The weight distribution of the minimal uncorrectable errors provides a better upper bound on the numbers of uncorrectable errors than (6) using the bound of [6, Eq. (6)].

It follows from the fact that $M^1(\mathrm{RM}_m)\subseteq LH(\mathrm{RM}^*_m)=LH_{2^{m-2}}(\mathrm{RM}^*_m)\cup LH_{2^{m-2}+1}(\mathrm{RM}^*_m)$ and (7) that

$$\left|M^1_i(\mathrm{RM}_m)\right| = \begin{cases} 0, & \text{for } \begin{array}{c} 0\leq i\leq 2^{m-2}-1 \\ 2^{m-2}+2\leq i\leq n \end{array} \\ \left|E^1_{2^{m-2}}(\mathrm{RM}_m)\right|, & \text{for } i=2^{m-2}. \end{cases} \tag{22}$$

The size of $E^1_{2^{m-2}}(\mathrm{RM}_m)$ is given in Theorem 4.

For the weight $2^{m-2}+1$, we have

$$\left|M^1_{2^{m-2}+1}(\mathrm{RM}_m)\right| = |LH^+(\mathrm{RM}^*_m)| - |LH^+(\mathrm{RM}^*_m)\setminus M^1(\mathrm{RM}_m)|. \tag{23}$$

We will determine $|LH^+(\mathrm{RM}^*_m)|$ and $|LH^+(\mathrm{RM}^*_m)\setminus M^1(\mathrm{RM}_m)|$ in the rest of this section.

The size of $LH^+(\mathrm{RM}^*_m)$ is immediately determined. From Lemma 9, there is no common larger half of weight $2^{m-2}+1$ of more than one codeword in RM^*_m. Therefore

$$\begin{aligned} |LH^+(\mathrm{RM}^*_m)| &= \binom{2^{m-1}-1}{2^{m-2}+1}\cdot|\mathrm{RM}^*_m| \\ &= 2(2^m-1)\binom{2^{m-1}-1}{2^{m-2}+1}. \end{aligned} \tag{24}$$

Next we will determine $|LH^{+}(\mathrm{RM}_m^*) \setminus M^1(\mathrm{RM}_m)|$. For $\boldsymbol{v}_1 \in LH^{+}(\mathrm{RM}_m^*)$, $\boldsymbol{v}_1$ is not minimal if and only if there is $\boldsymbol{v}_2 \in LH^{-}(\mathrm{RM}_m^*)$ such that $\boldsymbol{v}_2 \subseteq \boldsymbol{v}_1$. Then the following lemma holds.

Lemma 13: For $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathrm{RM}_m^*$, if $\{(\boldsymbol{v}_1, \boldsymbol{v}_2) : \boldsymbol{v}_1 \in LH^{+}(\boldsymbol{c}_1), \boldsymbol{v}_2 \in LH^{-}(\boldsymbol{c}_2), \boldsymbol{v}_2 \subseteq \boldsymbol{v}_1\}$ is not empty, then

$$l(\boldsymbol{c}_1) < l(\boldsymbol{c}_2) \text{ and } l(\boldsymbol{c}_2) \in S(\boldsymbol{c}_1). \tag{25}$$

If (25) holds, the set is equivalent to

$$\left\{ (\boldsymbol{v}_2 + \boldsymbol{e}, \boldsymbol{v}_2) : \begin{array}{c} \boldsymbol{v}_2 = \boldsymbol{c}_1 \cap \boldsymbol{c}_2, \boldsymbol{e} \in \mathbb{F}_1^n, \\ S(\boldsymbol{e}) \subseteq S(\boldsymbol{c}_1) \setminus \{S(\boldsymbol{c}_2) \cup \{l(\boldsymbol{c}_1)\}\} \end{array} \right\}. \tag{26}$$

Proof: The inequality $l(\boldsymbol{c}_1) < l(\boldsymbol{c}_2)$ comes from $l(\boldsymbol{c}_1) < l(\boldsymbol{v}_1) \leq l(\boldsymbol{v}_2) = l(\boldsymbol{c}_2)$, and $l(\boldsymbol{c}_2) \in S(\boldsymbol{c}_1)$ comes from $l(\boldsymbol{c}_2) = l(\boldsymbol{v}_2) \in S(\boldsymbol{v}_2) \subseteq S(\boldsymbol{v}_1) \subseteq S(\boldsymbol{c}_1)$. Next, we prove the equivalence of the sets. Using Lemma 4, we have that $\boldsymbol{v}_2 = \boldsymbol{c}_1 \cap \boldsymbol{c}_2$. Then $\boldsymbol{v}_1 = \boldsymbol{v}_2 + \boldsymbol{e}$, and $\boldsymbol{e}$ is selected as $\boldsymbol{e} \in \mathbb{F}_1^n, S(\boldsymbol{e}) \subseteq S(\boldsymbol{c}_1) \setminus \{S(\boldsymbol{c}_2) \cup \{l(\boldsymbol{c}_1)\}\}$. □

Next we consider the number of $\boldsymbol{v}_2 \in LH^{-}(\mathrm{RM}_m^*)$ covered by $\boldsymbol{v}_1 \in LH^{+}(\mathrm{RM}_m^*)$.

Lemma 14: For $\boldsymbol{v}_1 \in LH^{+}(\mathrm{RM}_m^*)$, there is at most one $\boldsymbol{v}_2 \in LH^{-}(\mathrm{RM}_m^*)$ such that $\boldsymbol{v}_2 \subseteq \boldsymbol{v}_1$ for $m \geq 4$.

Proof: Suppose there are two distinct vectors $\boldsymbol{v}_2 \in LH^{-}(\boldsymbol{c}_2)$ and $\boldsymbol{v}_3 \in LH^{-}(\boldsymbol{c}_3)$ such that $\boldsymbol{v}_2 \subseteq \boldsymbol{v}_1$ and $\boldsymbol{v}_3 \subseteq \boldsymbol{v}_1$ for some $\boldsymbol{c}_2, \boldsymbol{c}_3 \in \mathrm{RM}_m^*$. Then we have $\boldsymbol{v}_2 = \boldsymbol{c}_1 \cap \boldsymbol{c}_2$ and $\boldsymbol{v}_3 = \boldsymbol{c}_1 \cap \boldsymbol{c}_3$ from Lemma 13. The vector $\boldsymbol{v}_1$ is represented as $\boldsymbol{v}_2 + \boldsymbol{e}_1$ and $\boldsymbol{v}_3 + \boldsymbol{e}_2$ for vectors $\boldsymbol{e}_1, \boldsymbol{e}_2 \in \mathbb{F}_1^n$. Then $d(\boldsymbol{v}_2, \boldsymbol{v}_3) = d(\boldsymbol{v}_1 + \boldsymbol{e}_1, \boldsymbol{v}_1 + \boldsymbol{e}_2) = 2$, where $d(\boldsymbol{x}, \boldsymbol{y})$ is the Hamming distance between $\boldsymbol{x}$ and $\boldsymbol{y}$. However, $d(\boldsymbol{v}_2, \boldsymbol{v}_3) = d(\boldsymbol{c}_1 \cap \boldsymbol{c}_2, \boldsymbol{c}_1 \cap \boldsymbol{c}_3) \geq 2^{m-2}$ because $\boldsymbol{v}_2$ and $\boldsymbol{v}_3$ are distinct codewords in the second-order Reed–Muller code, the minimum distance of which is 2^{m-2}. Therefore, a contradiction arises if $m \geq 4$. □

If $\boldsymbol{v}_1 \in LH^{+}(\boldsymbol{c}_1)$ covers $\boldsymbol{v}_2 \in LH^{-}(\boldsymbol{c}_2)$ for $\boldsymbol{c}_2 \in \mathrm{RM}_m^*$, then $\boldsymbol{v}_2$ is unique for $\boldsymbol{v}_1$ from Lemma 14. Then the number of $\boldsymbol{v}_1$ in $LH^{+}(\boldsymbol{c}_1)$ that covers $\boldsymbol{v}_2$ is the size of $S(\boldsymbol{c}_1) \setminus \{S(\boldsymbol{c}_2) \cup \{l(\boldsymbol{c}_1)\}\}$ from (26), which is equal to $2^{m-2} - 1$. If we know the number of larger halves in $LH^{-}(\mathrm{RM}_m^*)$ that are covered by larger halves in $LH^{+}(\mathrm{RM}_m^*)$, then the product of it and $2^{m-2} - 1$ yields the number of vectors in $LH^{+}(\mathrm{RM}_m^*)$ that cover some larger half in $LH^{-}(\mathrm{RM}_m^*)$, which is $|LH^{+}(\mathrm{RM}_m^*) \setminus M^1(\mathrm{RM}_m)|$.

We determine the number of $\boldsymbol{v}_2 \in LH^{-}(\mathrm{RM}_m^*)$ such that $\boldsymbol{v}_2 \subseteq \boldsymbol{v}_1$ for some $\boldsymbol{v}_1 \in LH^{+}(\mathrm{RM}_m^*)$. Suppose $\boldsymbol{v}_2 \in LH^{-}(\boldsymbol{c}_2)$ and $\boldsymbol{c}_2 \in C_m(s_i), 1 \leq i \leq m+1$. For $\boldsymbol{c}_2 \in C_m(s_i)$, the number of $\boldsymbol{c}_1 \in \mathrm{RM}_m^*$ satisfying (25) is

$$\frac{|C_m(s_1)| + 1}{2} - 1 + \sum_{j=2}^{i-1} \frac{|C_m(s_j)|}{2} = 2^m - 1 + 2^{m-i+1}.$$

From (26) we have $\boldsymbol{v}_2 = \boldsymbol{c}_1 \cap \boldsymbol{c}_2$. Then there may be another codeword $\boldsymbol{c}_3 \in \mathrm{RM}_m^*$ such that $\boldsymbol{v}_2 = \boldsymbol{c}_1 \cap \boldsymbol{c}_3$. That is, $\boldsymbol{v}_2$ is a common larger half of $\boldsymbol{c}_2$ and $\boldsymbol{c}_3$. Fortunately, the number of such larger halves is obtained in Section IV-A and is $|D_m^2|$. In the case we consider here, there is no common larger half of three codewords, which is a larger half of a codeword in D_m^3. This result occurs because, as in the proof of Lemma 8, D_m^3 consists of larger halves of codewords in $C_m(s_1)$, but the larger halves we consider here are those in $C_m(s_i)$ for $i \geq 2$. Therefore, the number of $\boldsymbol{v}_2 \in LH^{-}(\mathrm{RM}_m^*)$ such that $\boldsymbol{v}_2 \subseteq \boldsymbol{v}_1$ for some $\boldsymbol{v}_1 \in LH^{+}(\mathrm{RM}_m^*)$ is

$$\begin{aligned} &\sum_{i=2}^{m+1} |C_m(s_i)|(2^m - 1 + 2^{m-i+1}) - \left|D_m^2\right| \\ &\quad = \sum_{i=2}^{m+1} 2^{m-i+1}(2^m - 1 + 2^{m-i+1}) - \frac{1}{3}\binom{2^m - 1}{2} \\ &\quad = \binom{2^m - 1}{2}. \end{aligned}$$

Thus, the product of $\binom{2^m-1}{2}$ and $2^{m-2} - 1$ gives the size of $|LH^{+}(\mathrm{RM}_m^*) \setminus M^1(\mathrm{RM}_m)|$.

Lemma 15: For $m \geq 4$

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

Now the weight distribution of the minimal uncorrectable errors for RM_m is determined.

Theorem 6: For $m \geq 4$ and $0 \leq i \leq n$ (see the equation shown at the bottom of the page).

Proof: The statement follows from Theorem 4, (22), (23), (24), and Lemma 15. □

$$\left|M_i^1(\mathrm{RM}_m)\right| = \begin{cases} (2^m - 1)\dbinom{2^{m-1}}{2^{m-2}} - \dbinom{2^m - 1}{2}, & \text{for } i = 2^{m-2} \\ \begin{array}{l} 2(2^m - 1)\dbinom{2^{m-1} - 1}{2^{m-2} + 1} \\ \quad -(2^{m-2} - 1)\dbinom{2^m - 1}{2} \end{array}, & \text{for } i = 2^{m-2} + 1 \\ 0, & \text{otherwise.} \end{cases}$$

TABLE I
BOUNDS OF THE SIZES OF MINIMUM TRIAL SETS FOR SOME BCH, EXTENDED BCH, AND REED–MULLER CODES

(n,k) code C	Lower bounds		$\lvert T_{\rm min}\rvert$	Upper bounds	
	New			[6]	New
	k	$\lvert T_{\rm nec}\rvert$		$\lvert C^*\rvert$	$\lvert T_{\rm nec}\rvert + \lvert M^1(C) \setminus LH(T_{\rm nec})\rvert$
(15,11) BCH	11*	11*	11 – 83	308	83*
(15,7) BCH	7	44*	44 – 87	108	87*
(15,5) BCH	5	30*	30	30*	30*
(16,11) exBCH	11	16*	16 – 79	588	79*
(16,7) exBCH	7	45*	45 – 86	126	86*
(16,5) exBCH	5	30*	30	30*	30*
(16,11) RM	11	15*	15 – 79	588	79*

* The maximum/minimum value for the lower/upper bounds.

Using (8), we obtain

$$\left|M^1_{2^{m-2}+1}(\mathrm{RM}_m)\right| \approx \frac{2^{2^{m-1}+\frac{m}{2}+1}}{\sqrt{\pi}}.$$

V. TRIAL SETS

In this section, we study the sizes of trial sets for general linear codes and the first-order Reed–Muller codes. As presented in (6), a trial set can be used for deriving an upper bound on the number of uncorrectable errors. Also, trial sets can be used for minimum distance decoding. The algorithm is described in [6]. Although no reasonable upper bounds on the complexity of the algorithm is known, the complexity seems to depend on the size of a trial set used in the algorithm. In both applications, smaller trial sets are desirable. Therefore, we consider a smallest trial set. Define a *minimum trial set* for C as the smallest trial set for C, denoted by $T_{\rm min}$. Note that $T_{\rm min}$ itself may not be unique. The size of minimum trial sets is discussed for general linear codes in Section V-A and for the first-order Reed–Muller codes in Section V-B.

A. Linear Codes

We provide some upper and lower bounds on the size of minimum trial sets for general linear codes. It is clear from (5) that $|T_{\rm min}| \le |C^*|$. Let us define $T_{\rm nec}$ as the set of minimal codewords $\boldsymbol{c} \in C^*$ such that, for some $\boldsymbol{v} \in M^1(C)$, $\boldsymbol{v} \in LH(\boldsymbol{c})$, and $\boldsymbol{v} \notin LH(\boldsymbol{c}')$ for all $\boldsymbol{c}' \in C^* \setminus \{\boldsymbol{c}\}$. That is, for $\boldsymbol{c} \in C^*$

$$\boldsymbol{c} \in T_{\rm nec} \Leftrightarrow LH(\boldsymbol{c}) \setminus LH(C^* \setminus \{\boldsymbol{0}, \boldsymbol{c}\}) \neq \emptyset.$$

The codewords in $T_{\rm nec}$ are necessary to compose a trial set. We have the following bounds on the size of minimum trial sets.

Theorem 7: Let $T_{\rm min}$ be a minimum trial set for an (n,k) linear code C with minimum distance $d \ge 2$. Then

$$\max\{k, |T_{\rm nec}|\} \le |T_{\rm min}| \le |T_{\rm nec}| + |M^1(C) \setminus LH(T_{\rm nec})|.$$

Proof: If a codeword $\boldsymbol{c} \in C$ is an input into a trial set decoder, then the decoder finds the coset leader $\boldsymbol{0}$ and thus outputs $\boldsymbol{c}$. For the correctness of the decoder, see [6, Section 2]. The coset leader found by the decoder is the sum of codewords in $T_{\rm min}$ and the input. Therefore, the linear span of a trial set forms the code C. This leads to $k \le |T_{\rm min}|$. The inequality $|T_{\rm nec}| \le |T_{\rm min}|$ is obvious.

From the definition of $T_{\rm nec}$, $T_{\rm min}$ contains $T_{\rm nec}$. We show that the number of remaining codewords that should be in $T_{\rm min}$, that is $|T_{\rm min} \setminus T_{\rm nec}|$, is upper bounded by $|M^1(C) \setminus LH(T_{\rm nec})|$. First, note that, since $LH(T_{\rm min})$ contains $M^1(C)$, $M^1(C) \setminus LH(T_{\rm nec})$ consists of larger halves of codewords in $T_{\rm min} \setminus T_{\rm nec}$. Next, for every $\boldsymbol{c} \in T_{\rm min} \setminus T_{\rm nec}$, there is at least one vector $\boldsymbol{v} \in LH(\boldsymbol{c}) \cap (M^1(C) \setminus LH(T_{\rm nec}))$ such that $\boldsymbol{v}$ is not a larger half of the other codewords in $T_{\rm min} \setminus T_{\rm nec}$. This is because, if every larger half of $\boldsymbol{c}$ in $M^1(C) \setminus LH(T_{\rm nec})$ is also a larger half of another codeword in $T_{\rm min} \setminus T_{\rm nec}$, then $LH(T_{\rm min} \setminus \{\boldsymbol{c}\})$ contains $M^1(C)$, and, thus, $\boldsymbol{c}$ can be removed from $T_{\rm min}$, which contradicts the definition of a minimum trial set. Since every $\boldsymbol{c} \in T_{\rm min} \setminus T_{\rm nec}$ has at least one larger half that cannot be a larger half of another codeword in $T_{\rm min} \setminus T_{\rm nec}$, the number of codewords in $T_{\rm min} \setminus T_{\rm nec}$ is upper bounded by $|M^1(C) \setminus LH(T_{\rm nec})|$. □

While a naive algorithm for computing $|T_{\rm min}|$ requires $2^{2^{O(n)}}$ time, the time complexity for computing $|T_{\rm nec}|$ and $|M^1(C) \setminus LH(T_{\rm nec})|$ is $2^{O(n)}$. Therefore, the above bounds are useful in estimating $|T_{\rm min}|$.

We compute the bounds in Theorem 7 and the upper bound $|C^*|$ for some codes. The results are shown in Table I. The new upper bound is tight for all codes compared to the known bound. The upper and lower bounds coincide for two codes, the (15,5) BCH code and the (16,5) extended BCH code.

B. First-Order Reed–Muller Codes

We determine the minimum trial set $T_{\rm min}$ for the first-order Reed–Muller code of length 2^m, RM_m. The next lemma shows that all codewords in RM^*_m are in $T_{\rm nec}$ for $m \ge 4$.

Lemma 16: Let $\boldsymbol{c} \in \mathrm{RM}^*_m$ with $m \ge 4$. Then

$$LH^-(\boldsymbol{c}) \setminus LH^-(\mathrm{RM}^*_m \setminus \{\boldsymbol{c}\}) \neq \emptyset.$$

Proof: Since $l(\boldsymbol{v}) = l(\boldsymbol{c})$ for every $\boldsymbol{v} \in LH^-(\boldsymbol{c})$ from (3), we consider $LH^-(C_m(l(\boldsymbol{c})) \setminus \{\boldsymbol{c}\})$ rather than $LH^-(\mathrm{RM}^*_m \setminus \{\boldsymbol{c}\})$. For every $\boldsymbol{c}' \in C_m(l(\boldsymbol{c})) \setminus \{\boldsymbol{c}\}$, $\boldsymbol{c}$ and $\boldsymbol{c}'$ have a common larger half of weight 2^{m-2}, which is $\boldsymbol{c} \cap \boldsymbol{c}'$, from Lemma 5. Therefore, if the size of $LH^-(\boldsymbol{c})$ is larger than that of $C_m(l(\boldsymbol{c})) \setminus \{\boldsymbol{c}\}$, there is at least one larger half in $LH^-(\boldsymbol{c})$ that is not a larger half in $LH^-(C_m(l(\boldsymbol{c})) \setminus \{\boldsymbol{c}\})$. The size of $C_m(l(\boldsymbol{c}))$ is at most $2^m - 1$ from (10). The inequality $|LH^-(\boldsymbol{c})| = \binom{2^{m-1}}{2^{m-2}}/2 > 2^m - 1$ holds for $m \ge 4$. □

Theorem 8: The minimum trial set for RM_m with $m \ge 4$ is RM^*_m.

Proof: From Lemma 16, for every $\boldsymbol{c} \in \mathrm{RM}^*_m$, there exists at least one vector $\boldsymbol{v} \in LH^-(\boldsymbol{c})$ such that $\boldsymbol{v} \notin LH(\mathrm{RM}^*_m \setminus \{\boldsymbol{c}\})$.

Thus, $\mathrm{RM}_m^* \subseteq T_{\mathrm{nec}} \subseteq T_{\mathrm{min}}$. From (5), we obtain $T_{\mathrm{min}} \subseteq \mathrm{RM}_m^*$. □

Note that some of codewords in RM_3^* may not be in T_{min} for RM_3. In fact, $|\mathrm{RM}_3^*| = 14$ but $|T_{\mathrm{min}}| = 10$.

VI. Conclusion and Future Work

In this paper, we have examined the number of correctable/ uncorrectable errors of weight $\geq d/2$ for binary linear codes. For general linear codes, lower bounds on the number of uncorrectable errors of weight $\geq d/2$ have been derived. For the first-order Reed–Muller codes, we have determined the number of correctable errors of weight $d/2+1$ and the weight distribution of the minimal uncorrectable errors. For the sake of applications, we have analyzed the size of minimum trial sets.

An interesting future work would be to derive a good lower bound on the number of uncorrectable errors of weight $>d/2$. Our lower bound in Section III-B is a lower bound on the set of larger halves, which is a subset of the set of uncorrectable errors. Since the larger half was introduced for characterizing minimal uncorrectable errors, our lower bound cannot be good enough for the size of uncorrectable errors.

Another avenue for future study is to apply the analysis using the monotone error structure for other specific codes, such as the second-order Reed–Muller codes and BCH codes. Also, the number of uncorrectable errors of weight $\lceil d/2 \rceil$ is yet to be determined for these specific codes.

Furthermore, from the result of Section V-A, the size of minimum trial sets is quite smaller than that of the set of the minimal codewords. Estimating the sizes of minimum trial sets for longer codes or random linear codes will be important for applications of trial sets. In this connection, estimating the time-complexity of the trial set decoding could be another future work.

Acknowledgment

The authors would like to thank the anonymous referees for their helpful comments and for identifying some errors in an earlier draft of this paper.

References

[1] E. R. Berlekamp and L. R. Welch, "Weight distributions of the cosets of the (32,6) Reed–Muller code," *IEEE Trans. Inf. Theory*, vol. 18, no. 1, pp. 203–207, Jan. 1972.

[2] P. Charpin, "Weight distributions of cosets of two-error-correcting binary BCH codes, extended or not," *IEEE Trans. Inf. Theory*, vol. 40, no. 5, pp. 1425–1442, Sep. 1994.

[3] P. Charpin, T. Helleseth, and V. A. Zinoviev, "The coset distribution of triple-error-correcting binary primitive BCH codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1727–1732, Apr. 2006.

[4] M. Maeda and T. Fujiwara, "Weight distribution of the coset leaders of some Reed–Muller codes and BCH codes," *IEICE Trans. Fundam.*, vol. E84-A, no. 3, pp. 851–859, May 2001.

[5] T. Helleseth and T. Kløve, "The Newton radius of codes," *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1820–1831, Nov. 1997.

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

[7] G. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra," *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1284–1292, Jul. 1994.

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

[9] C. Carlet, "Boolean functions for cryptography and error correcting codes," in *Boolean Methods and Models*, Y. Crama and P. Hammer, Eds. Cambridge, U.K.: Cambridge Univ. Press, to be published.

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

[11] G. Zémor, "Threshold effects in codes," presented at the Algebraic Coding, Paris, France, 1993.

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

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

[14] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1963.

[15] W. Feller*, An Introduction to Probability Theory and Its Applications*, 3rd ed. Hoboken, NJ: Wiley, 1968, vol. 1.

[16] A. Barg and G. D. Forney, Jr., "Random codes: Minimum distances and error exponents," *IEEE Trans. Inf. Theory*, vol. 48, no. 9, pp. 2568–2573, Sep. 2002.

[17] A. Canteaut, C. Carlet, P. Charpin, and C. Fontaine, "On cryptographic properties of the cosets of $R(1,m)$," *IEEE Trans. Inf. Theory*, vol. 47, no. 4, pp. 1949–1513, May 2001.

[18] *Lecture Notes in Computer Science*. Berlin, Germany: Springer-Verlag, 1994, vol. 781, pp. 278–286.

Kenji Yasunaga received the B.E. degree in information and computer sciences in 2003 and the M.Sc. and Ph.D. degrees in information science and technology in 2005 and 2008, from Osaka University, Japan.

His research interests are in coding theory, cryptography, pseudorandomness, and computational complexity theory.

Toru Fujiwara (S'83–M'86) received the B.E., M.E., and Ph.D. degrees in information and computer sciences from Osaka University, Toyonaka, Osaka, Japan, in 1981, 1983, and 1986, respectively.

In 1986, he jointed the faculty of Osaka University. During 1989–1990, he was on leave as a Post Doctoral Fellow in the Department of Electrical Engineering, University of Hawaii, Honolulu. From 1992 to 1997, he was an Associate Professor at the Department of Information and Computer Sciences, Osaka University. From 1997 to 2003, he was a Professor in the Department of Informatics and Mathematical Science, Graduate School of Engineering Science, Osaka University. He is now with the Department of Multimedia Engineering, Graduate School of Information Science and Technology, Osaka University. From 1998 to 2000, he was simultaneously a Professor in the Graduate School of Information Science and Technology, Nara, Japan, and at Osaka University. His current research interests include coding theory and cryptography.

Dr. Fujiwara was the chair person of IEEE Information Theory Society Japan Chapter in 2006 and 2007. He is an Associate Editor of IEEE Transactions on Information Theory. He is a Fellow of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan, and a Member of the Information Processing Society of Japan (IPSJ), and the Association for Computing Machinery (ACM).