On Correctable Errors of Binary Linear Codes

Kenji Yasunaga and Toru Fujiwara, *Member, IEEE*

September 22, 2008

Abstract

Error correction capability of binary linear codes with the 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 of weight 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 of weight 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 notion *larger half* and *trial set*, which are introduced by Helleseth, Kløve, and Levenshtein, are mainly used to derive the results.

Index Terms

Error correction capability, monotone error structure, trial set, Reed-Muller code, Boolean function, nonlinearity

K. Yasunaga is with Graduate School of Science and Technology, Kwansei Gakuin University (e-mail: kenji.yasunaga@gmail.com).

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

I. INTRODUCTION

Error performance analysis of codes is a fundamental problem in coding theory. In this paper, we deal with the error correction capability of binary linear codes with the 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 is less than $d/2$, where d is the minimum distance of the code, then the minimum distance decoder always correct it. Therefore, the correction capability for errors with weight $\geq d/2$ is crucial for the performance analysis of the minimum distance decoding. In particular, an analysis for errors with weight around $d/2$ is important because the ratio of the correctable errors for such errors is the highest in the errors with weight $\geq d/2$.

Determining the number of correctable errors of weight $\geq d/2$ is a difficult problem. A usual approach is to employ the syndrome decoding as a minimum distance decoding. The syndrome decoding is a minimum distance decoding if a minimum weight vector is selected as the coset leader in each cosets. Then the correctable errors are the coset leaders of the code, and thus the weight distribution of the coset leaders represents the numbers of correctable errors for each weight. Considering this fact, the error correction capabilities are completely determined for only some specific codes [3], [6], [7], [13]. For general linear codes, some bounds on the number of correctable errors were presented in [10], [11], [15]. For the first-order Reed-Muller codes, although they have a simple structure, the exact number of correctable errors was known only for weight $d/2$ [17]. 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 (see [5, Sec. 4]). The relation to the error correction is described in Section IV.

In this paper, we study the number of correctable errors of weight $\geq d/2$ by using the *monotone error structure*, which is an old result of coding theory [14, 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 arises if the lexicographically smallest minimum weight vector in each coset is selected as the

coset leader. The reason why this structure is useful for the error analysis is that, if the errors have the monotone structure, the correctable (and uncorrectable) errors are characterized by the maximal correctable (and minimal uncorrectable) errors. An analysis of correctable errors using the monotone error structure was first done by Helleseth, Kløve, and Levenshtein [11]. They introduced some useful notion, *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 [11] two applications of a trial set is presented, one is for giving an upper bound on the number of uncorrectable errors, the other is for a minimum distance decoding.

We derive a lower bound on the number of uncorrectable errors of weight $\lceil d/2 \rceil$ for general linear codes satisfying some condition. The bound is given in terms of the numbers of codewords with weights d and $d+1$ in the code. The condition is not too restrictive, and some primitive BCH codes, extended primitive BCH codes, Reed-Muller codes, and random linear codes satisfy the condition. For Reed-Muller codes and random linear codes, the lower bound asymptotically coincides with the upper bound of [11, Corollary 7]. By generalizing the idea of the lower bound, we also derive a lower bound on the number of uncorrectable errors for every weight $i > d/2$. However, as i becomes large, the generalized bound is worse and the condition for codes is more restrictive.

For the first-order Reed-Muller codes, we provide the explicit expressions of the numbers of correctable errors of weights $d/2$ and $d/2+1$. Although the case of weight $d/2$ was already solved by Wu [17], we give a simpler proof in this paper. As a direct consequence, the number of Boolean functions of m variables with nonlinearity $2^{m-2}+1$ is determined. We also determine the weight distribution of the minimal uncorrectable errors.

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

The organization of this paper is as follows. In Section II, we describe the monotone error structure and give 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 $d/2$ and that of weight beyond $d/2$ 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 Section IV-A and Section IV-B, respectively. The weight distribution of the minimal uncorrectable errors are 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, for short, an (n, k, d) code. Then $\mathbb{F}^n$ is partitioned into 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 the coset leader of the coset D_i, and every vector in D_i can be taken 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 which contains $\boldsymbol{y}$. Thus the set of correctable errors by the syndrome decoding is the set of coset leader. If each $\boldsymbol{v}_i$ has the minimum weight in the coset D_i, 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 $b \in \{0, 1\}$, 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 $\boldsymbol{x}$. The error probability of C after the maximum likelihood decoding over the binary symmetric channel with cross over probability p is given by

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

In this paper, as in [11], we take as $\boldsymbol{v}_i$ the minimum element in D_i with respect to the following total ordering $\preceq$:

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

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 $\boldsymbol{x}$ is lexicographically smaller than $\boldsymbol{y}$. We write $\boldsymbol{x} \prec \boldsymbol{y}$ if $\boldsymbol{x} \preceq \boldsymbol{y}$ and $\boldsymbol{x} \neq \boldsymbol{y}$.

When we take the minimum element with respect to $\preceq$ in each coset as its coset leader, both $E^0(C)$ and $E^1(C)$ have the monotone structure[1]. 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 of $\boldsymbol{v} = (v_1, v_2, \ldots, v_n)$. 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 [18] showed that the error probability after the maximum likelihood decoding over binary symmetric channels displays a threshold behavior. Helleseth, Kløve, and Levenshtein [11] studied this structure and introduced *larger halves* and *trial sets*.

Since the set of uncorrectable errors $E^1(C)$ has the 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 $\boldsymbol{x}$ such that $\boldsymbol{x} \subset \boldsymbol{y}$ in $E^1(C)$. We denote by $M^1(C)$ the set of the 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 vectors $\boldsymbol{v} \in \mathbb{F}^n$ with respect to covering such that $\boldsymbol{v} + \boldsymbol{c} \prec \boldsymbol{v}$. From the definition, we know that the set of larger halves

[1]In this paper we use the total ordering $\preceq$ in selecting coset leaders for the monotone error structure. All orderings that give the monotone error structure are discussed in [11, Appendix I].

of all nonzero codewords contains the set of the 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 applied if $w(\boldsymbol{c})$ is odd. The proof of equivalence between the definition and the above condition is found in the proof of [11, Theorem 1]. Let $LH(\boldsymbol{c})$ denote the set of the larger halves of $\boldsymbol{c} \in C \setminus \{\boldsymbol{0}\}$. For a set $U \subseteq C \setminus \{\boldsymbol{0}\}$, 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 $(w(\boldsymbol{c}) + 1)/2$. 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 the larger halves of $\boldsymbol{c}$ of weight $w(\boldsymbol{c})/2$ and $w(\boldsymbol{c})/2 + 1$, respectively. Then, for an even-weight codeword $\boldsymbol{c} \in C$, $LH(\boldsymbol{c}) = LH^-(\boldsymbol{c}) \cup LH^+(\boldsymbol{c})$. Also 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.

A set T of nonzero codewords in C is called a trial set [11] for C if the set of larger halves of codewords in T contains the set of the minimal uncorrectable errors, that is,

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

From the definition of larger half, the set of the 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 [1]. Let C^* denote the set of the minimal

codewords in C. Then we have the following property [11, Corollary 5]:

$$\text{If } T \text{ is a trial set for } C, \text{ then } T \cap C^* \text{ is also a trial set for } C. \tag{5}$$

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

A trial set can be used for providing 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, define $T_i = \{\boldsymbol{v} \in T : w(\boldsymbol{v}) = i\}$. Then, for i with $\lfloor (d-1)/2 \rfloor < i \leq n$, it holds that [11, Corollary 7]

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

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 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, $M_i^1(C) = \{\boldsymbol{v} \in M^1(C) : w(\boldsymbol{v}) = i\}$, 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

A. Correctable Errors of Weight Half the Minimum Distance

In this section, we derive a lower bound on the number of uncorrectable errors of weight half the minimum distance, which is $|E_{\lceil d/2 \rceil}^1(C)|$. The bound is given by 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 shows 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 $\boldsymbol{c}_1, \boldsymbol{c}_2 \in C_d$, $LH^-(\boldsymbol{c}_1) \cap LH^-(\boldsymbol{c}_2)$ 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 $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2) = (w(\boldsymbol{c}_1) + w(\boldsymbol{c}_2) - w(\boldsymbol{c}_1 + \boldsymbol{c}_2))/2 \leq d/2$. Hence $\boldsymbol{v} = \boldsymbol{c}_1 \cap \boldsymbol{c}_2$. □

We provide a lower bound based on the fact that $C \setminus \{\mathbf{0}\}$ is a trial set for C.

Theorem 1: Let C be a linear code with even minimum distance d. If

$$\frac{1}{2}\binom{d}{\frac{d}{2}} > \left\lceil \frac{|C_d| - 1}{2} \right\rceil \tag{8}$$

holds, then

$$\frac{1}{2}\binom{d}{\frac{d}{2}}|C_d| - \left\lceil \frac{|C_d| - 1}{2} \right\rceil |C_d| \leq |E^1_{\frac{d}{2}}(C)| \leq \frac{1}{2}\binom{d}{\frac{d}{2}}|C_d|.$$

Proof: We can take $C \setminus \{\mathbf{0}\}$ as a trial set T. Then $T_d = C_d$ and $|E^1_{d/2}(C)| = |LH^-(C_d)|$ from (7). From Lemma 1, $LH^-(\boldsymbol{c})$ and $LH^-(\boldsymbol{c}')$ with $\boldsymbol{c}, \boldsymbol{c}' \in C_d$ have at most one common larger half $\boldsymbol{c} \cap \boldsymbol{c}'$. If they have the common larger half, then it holds that $l(\boldsymbol{c}) = l(\boldsymbol{c}')$ from (3) and that the codeword $\boldsymbol{c} + \boldsymbol{c}'$ is in C_d. Since $l(\boldsymbol{c}) \neq l(\boldsymbol{c} + \boldsymbol{c}')$, $\boldsymbol{c}$ and $\boldsymbol{c} + \boldsymbol{c}'$ have no common larger half of weight $d/2$. Therefore at least $|LH^-(\boldsymbol{c})| - \lceil (|C_d| - 1)/2 \rceil$ vectors in $LH^-(\boldsymbol{c})$ are not in $LH^-(C_d \setminus \{\boldsymbol{c}\})$. Thus we have the lower bound $(\binom{d}{d/2}/2 - \lceil (|C_d| - 1)/2 \rceil)|C_d|$.

An upper bound is unconditionally given by (6) as $|E^1_{d/2}(C)| \leq 1/2 \cdot \binom{d}{d/2}|T_d|$. However, from the condition (8), every $\boldsymbol{c} \in C_d$ has at least one larger half that has no common larger half with other codewords in C. Therefore it must be that $T_d = C_d$. □

The difference between the upper and lower bounds is at most $|C_d|^2/2$. If the fraction $|C_d|/\binom{d}{d/2}$ tends to zero as the code length becomes large, 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 shows 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 $\boldsymbol{c}_1, \boldsymbol{c}_1' \in C_d$ and $\boldsymbol{c}_2, \boldsymbol{c}_2' \in C_{d+1}$, the followings 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. (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 $\boldsymbol{v} \in LH(\boldsymbol{c}_1) \cup LH(\boldsymbol{c}_1') \cup LH^-(\boldsymbol{c}_2) \cup LH^-(\boldsymbol{c}_2')$ have the 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 that $\boldsymbol{v} \subseteq \boldsymbol{c} \cap \boldsymbol{c}'$ from (1). From the equality $w(\boldsymbol{c} \cap \boldsymbol{c}') = (w(\boldsymbol{c}) + w(\boldsymbol{c}') - w(\boldsymbol{c} + \boldsymbol{c}'))/2$ and the fact $w(\boldsymbol{c} + \boldsymbol{c}') \geq d$, we have that $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_1') < (d+1)/2$, $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2) \leq (d+1)/2$, and $w(\boldsymbol{c}_2 \cap \boldsymbol{c}_2') \leq (d+1)/2$. Thus the statement follows. □

We provide a lower bound by a similar argument as in the even case.

Theorem 2: Let C be a linear code with odd minimum distance d. If

$$\binom{d}{\frac{d+1}{2}} > \left\lceil \frac{|C_d|}{2} \right\rceil + \left\lceil \frac{|C_{d+1}| - 1}{2} \right\rceil \tag{9}$$

holds, then

$$\binom{d}{\frac{d+1}{2}}(|C_d| + |C_{d+1}|) - \left(\left\lceil \frac{|C_d|}{2} \right\rceil + \left\lceil \frac{|C_{d+1}| - 1}{2} \right\rceil \right) |C_{d+1}| \leq |E^1_{\frac{d+1}{2}}(C)| \leq \binom{d}{\frac{d+1}{2}}(|C_d| + |C_{d+1}|).$$

Proof: We can take $C \setminus \{\boldsymbol{0}\}$ as a trial set T. Then it holds that $T_d = C_d$, $T_{d+1} = C_{d+1}$, and $|E^1_{(d+1)/2}(C)| = |LH(C_d) \cup LH^-(C_{d+1})| = |LH(C_d)| + |LH^-(C_{d+1}) \setminus LH(C_d)|$. From Lemma 2, a codeword $\boldsymbol{c} \in C_d$ has no common larger half with $\boldsymbol{c}' \in C_d$. Thus $|LH(C_d)| = |LH(\boldsymbol{c})| \cdot |C_d| = \binom{d}{(d+1)/2}|C_d|$. Next we consider a lower bound on $|LH(C_{d+1}) \setminus LH(C_d)|$. From Lemma 2, a codeword $\boldsymbol{c} \in C_{d+1}$ has at most one common larger half for every codeword in $C_d \cup \{C_{d+1} \setminus \{\boldsymbol{c}\}\}$. If $\boldsymbol{c}$ and $\boldsymbol{c}' \in C_d$ have the common larger half $\boldsymbol{c} \cap \boldsymbol{c}'$, then $l(\boldsymbol{v}) = l(\boldsymbol{c})$ from (3) and the codeword $\boldsymbol{c} + \boldsymbol{c}'$ is in C_d. Since $l(\boldsymbol{c}) \notin S(\boldsymbol{c} + \boldsymbol{c}')$, $\boldsymbol{c} + \boldsymbol{c}'$ has no common larger half with $\boldsymbol{c}$. Likewise, if $\boldsymbol{c}$ and $\boldsymbol{c}'' \in C_{d+1}$ have the common larger half $\boldsymbol{c} \cap \boldsymbol{c}''$, then $l(\boldsymbol{c}) = l(\boldsymbol{c}')$ from (3) and the codeword $\boldsymbol{c} + \boldsymbol{c}''$ is in C_{d+1}. Since $l(\boldsymbol{c}) \neq l(\boldsymbol{c} + \boldsymbol{c}')$, $\boldsymbol{c}$ and $\boldsymbol{c} + \boldsymbol{c}''$ have no common larger half of weight $(d+1)/2$. Therefore, at least $|LH^-(\boldsymbol{c})| - \lceil |C_d|/2 \rceil - \lceil (|C_{d+1}| - 1)/2 \rceil$ vectors in $LH^-(\boldsymbol{c})$ are not in $LH^-(C_{d+1} \setminus \{\boldsymbol{c}\}) \setminus LH(C_d)$. Hence we have the lower bound $\binom{d}{(d+1)/2}(|C_d| + |C_{d+1}|) - (\lceil |C_d|/2 \rceil + \lceil (|C_{d+1}| - 1)/2 \rceil)|C_{d+1}|$.

An upper bound is given by (6) as $|E^1_{(d+1)/2}(C)| \leq \binom{d}{(d+1)/2}(|T_d| + |T_{d+1}|)$. However, as in the even case, the condition (9) leads to the fact that $T_d = C_d$ and $T_{d+1} = C_{d+1}$. □

TABLE I

THE r-TH ORDER REED-MULLER CODE OF LENGTH 2^m SATISFYING (8).

r	m
1	≥ 4
2	≥ 6
3	≥ 8
4	≥ 10
5	≥ 11
6	≥ 13

The difference between the upper and lower bounds is at most $(|C_d| + |C_{d+1}|)|C_{d+1}|$. If the fraction $|C_{d+1}|/\binom{d}{(d+1)/2}$ tends to zero as the code length becomes large, the lower bound asymptotically coincides with the upper one.

In what follows, we see that some BCH codes, Reed-Muller codes, and random linear codes satisfy the conditions (8) or (9).

a) Primitive BCH codes: By using the weight distribution [8], we can verify that the (n, k) primitive BCH codes satisfy the condition (9) for $n = 127, k \leq 64$ and $n = 63, k \leq 24$.

b) Extended Primitive BCH codes: By using the weight distribution [8], we can verify that the (n, k) extended primitive BCH codes satisfy the condition (8) for $n = 128, k \leq 64$ and $n = 64, k \leq 24$.

c) Reed-Muller codes: For the r-th 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 [12, Chapter 13], which is upper bounded by $(2^{m+1} - 2)^r$. Then, for a fixed r, the condition (8) is satisfied except for small m. Table I shows which parameters meet the condition (8).

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

$$\frac{|C_d|}{\binom{d}{d/2}} \leq \frac{(2^{m+1} - 2)^r}{2^{2^{m-r}}} \leq 2^{(m+1)r - 2^{m-r}}.$$

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

d) Random Linear Codes: A random linear code is a code whose generator matrix has equiprobable entries. That is, first we set a parameter (n, k), and then we choose a generator

matrix from all the 2^{nk} possible generator matrices with probability 2^{-nk}. It is known that with high probability the minimum distance equals to $n\delta_{\rm GV}$, where $1-H(\delta_{\rm GV})=k/n$ and $H(x)$ is the binary entropy function of x [9], [16]. Also it is known that the weight distribution equals the binomial distribution. Then, $|C_d| \approx (2^k-1)\binom{n}{d}2^{-n} \approx \binom{n}{n\delta_{\rm GV}}2^{k-n} \approx 2^{n(H(\delta_{\rm GV})+k/n-1)} \approx 1$, where we use the approximation $\binom{n}{n\lambda} \approx 2^{H(\lambda)}$, and $|C_{d+1}| \approx (2^k-1)\binom{n}{d+1}2^{-n} \approx 1$. Since $\binom{d}{d/2} \approx \sqrt{2/\pi d}2^d \approx 2^{n\delta}$ for even d and $\binom{d}{(d+1)/2} \approx 1/\sqrt{2\pi(d+1)}2^{d+1} \approx 2^{n\delta}$ for odd d, where $d=n\delta$, the conditions (8) and (9) are satisfied. Since the fractions $|C_{d+1}|/\binom{d}{(d+1)/2}$ and $|C_d|/\binom{d}{d/2}$ tend to zero, the upper and lower bounds in Theorems 1 and 2 asymptotically coincide.

B. Correctable Errors of Weight Beyond Half the Minimum Distance

By generalizing the results in the previous section, we give a lower bound on the size of $LH_i(C \setminus \{\mathbf{0}\})$ for each i. We have the relation $M_i^1(C) \subseteq LH_i(T) \subseteq E_i^1(C)$ for a trial set T for C. Thus the following lower bound is also a lower bound on the number of uncorrectable errors.

Theorem 3: Let C be a linear code with minimum distance d and T be a trial set for C. Define $B_i = |T_{2i-2}| + |T_{2i-1}| + |T_{2i}|$ and $\hat{B}_i = |T_{2i-2}||T_{2i-1}| + |T_{2i-1}||T_{2i}| + |T_{2i}||T_{2i-2}|$. For an integer i with $\lceil d/2 \rceil \le i \le \lfloor n/2 \rfloor$, if

$$\binom{2i-3}{i} > \binom{2i-\lceil \frac{d}{2} \rceil}{i} B_i$$

holds, then

$$\binom{2i-3}{i}B_i - \binom{2i-\lceil \frac{d}{2} \rceil}{i}(B_i^2 - \hat{B}_i) \le |LH_i(T)| \le \binom{2i-1}{i}B_i.$$

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 $\boldsymbol{c}, \boldsymbol{c}'$ be codewords in $T_{2i-2} \cup T_{2i-1} \cup T_{2i}$. Then $w(\boldsymbol{c} \cap \boldsymbol{c}') = (w(\boldsymbol{c}) + w(\boldsymbol{c}') - w(\boldsymbol{c}+\boldsymbol{c}'))/2 \le (2i + 2i - d)/2 = 2i - \lceil d/2 \rceil$. 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 size 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 $|LH_i(T)| \leq |LH^+(T_{2i-2})| + |LH(T_{2i-1})| + |LH^-(T_{2i})| \leq \binom{2i-3}{i}|T_{2i-2}| + \binom{2i-1}{i}|T_{2i-1}| + \binom{2i-1}{i}|T_{2i}| \leq \binom{2i-1}{i}B_i$. □

The lower bound in the above theorem is based on the fact that the set of the larger halves of trial sets is contained in the set of uncorrectable errors. From the fact that larger half is introduced to characterize minimal uncorrectable errors and that the size of the minimal uncorrectable errors is small for large weight, the bound in Theorem 3 is weak for large i. In addition, then 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 nonlinearity of Boolean functions, and provide some properties of RM_m used in the later.

The binary r-th order Reed-Muller code of length 2^m corresponds to the Boolean functions of m variables with degree at most r. Thus RM_m corresponds to the set of affine functions of m variables. The *nonlinearity* of a Boolean function f of m variables 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 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. There has been much study of nonlinearity of Boolean functions in cryptography. For further details, see [4], [5] and references therein.

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

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

where $\boldsymbol{u} \circ \boldsymbol{v}$ denotes the concatenation of $\boldsymbol{u}$ and $\boldsymbol{v}$, and $\overline{\boldsymbol{v}} = \boldsymbol{1} + \boldsymbol{v}$. 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 $\boldsymbol{c} \in \mathrm{RM}_m^*$.

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 $S_m = \{s_1, s_2, \ldots, s_{m+1}\}$ with $s_1 < s_2 < \cdots < s_{m+1}$. We define the set $C_m(s_i) \subseteq \mathrm{RM}_m^*$ for $1 \le i \le m+1$ 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 have

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

Let $\boldsymbol{c}_1, \boldsymbol{c}_2, \ldots, \boldsymbol{c}_l$ be codewords in RM_m^*. We say $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_l$, and $\mathbf{1}$ are linearly independent if $a_1\boldsymbol{c}_1 + a_2\boldsymbol{c}_2 + \cdots + a_l\boldsymbol{c}_l + a_{l+1}\mathbf{1} = \mathbf{0}$ for $a_i \in \{0,1\}$, $1 \le i \le l+1$ implies $a_1 = a_2 = \cdots = a_{l+1} = 0$. That is, if $l+1$ codewords $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_l$, and $\mathbf{1}$ are linearly independent, then every $\boldsymbol{c}_i$ with $1 \le i \le l$ cannot be represented as a sum of other l codewords.

Lemma 3: For $2 \le l \le m$, 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 $\mathbf{1}$ are linearly independent. Then $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \cdots \cap \boldsymbol{c}_l) = 2^{m-l}$.

Proof: We prove the statement by induction on l. For the case $l = 2$, the statement follows from the fact that $w(\boldsymbol{c}_1 + \boldsymbol{c}_2) = w(\boldsymbol{c}_1) + w(\boldsymbol{c}_2) - 2w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2)$ and that $w(\boldsymbol{c}_1 + \boldsymbol{c}_2) = w(\boldsymbol{c}_1) = w(\boldsymbol{c}_2) = 2^{m-1}$. For the induction step, assume that if l codewords in RM_m^* and $\mathbf{1}$ are linearly independent, then the weight of their intersection vector is 2^{m-l}. Let $\boldsymbol{c}_i \in \mathrm{RM}_m^*$ with $1 \le i \le l+1$ and $\mathbf{1}$ be linearly independent codewords. Let $\boldsymbol{x} = \boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \cdots \cap \boldsymbol{c}_{l-1} \cap \boldsymbol{c}_l$ and $\boldsymbol{y} = \boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \cdots \cap \boldsymbol{c}_{l-1} \cap \boldsymbol{c}_{l+1}$. From the assumption, $w(\boldsymbol{x}) = w(\boldsymbol{y}) = 2^{m-l}$, and $w(\boldsymbol{x} + \boldsymbol{y}) =$

$\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \cdots \cap \boldsymbol{c}_{l-1} \cap (\boldsymbol{c}_l + \boldsymbol{c}_{l+1}) = 2^{m-l}$ because $\boldsymbol{c}_i$ with $1 \le i \le l-1$, $\boldsymbol{c}_l + \boldsymbol{c}_{l+1}$, and $\mathbf{1}$ are linearly independent. From the relation $w(\boldsymbol{x} \cap \boldsymbol{y}) = (w(\boldsymbol{x}) + w(\boldsymbol{y}) - w(\boldsymbol{x} + \boldsymbol{y}))/2$ we have $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \cdots \cap \boldsymbol{c}_l \cap \boldsymbol{c}_{l+1}) = w(\boldsymbol{x} \cap \boldsymbol{y}) = (2^{m-l} + 2^{m-l} - 2^{m-l})/2 = 2^{m-(l+1)}$. □

Lemma 4: Let $\boldsymbol{c}_1, \boldsymbol{c}_2$ be distinct codewords in $C_m(s_i)$ with $1 \le i \le m$. For $m \ge 2$,

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

Proof: Since $\boldsymbol{c}_1, \boldsymbol{c}_2 \in C_m(s_i)$, $\boldsymbol{c}_1 \ne \overline{\boldsymbol{c}_2}$. Hence $\boldsymbol{c}_1$, $\boldsymbol{c}_2$, and $\mathbf{1}$ are linearly independent. Thus from Lemma 3 we have the statement. □

Lemma 5: Let $\boldsymbol{c}_1, \boldsymbol{c}_2, \boldsymbol{c}_3$ be distinct codewords in RM_m^*. For $m \ge 3$,

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

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 of Weight Half the Minimum Distance

In this section, we determine the number of correctable errors of weight half the minimum distance for RM_m. The proof was already given in [17], but here we give a slightly simpler proof.

In the proof of [17], 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, first we observe that uncorrectable errors of weight 2^{m-2} are equivalent to the set of larger halves of weight 2^{m-2} of codewords except the all-zero and the all-one codewords. Then counting the number of larger halves that are common among more than one codeword leads to the result. Our approach does not make clear 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 [17].

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

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

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

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

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

Lemma 6: $D_m^i = \emptyset$ for $m \geq 2$ and $i \geq 4$.

Proof: For $\boldsymbol{v} \in E_{2^{m-2}}^1(\mathrm{RM}_m)$, assume that there are four codewords $\boldsymbol{c}_i \in \mathrm{RM}_m^*$ with $1 \leq i \leq 4$ such that $\boldsymbol{v} \in LH^-(\boldsymbol{c}_i)$. It holds from the condition (1) that $\boldsymbol{v} \subseteq \bigcap_{i=1}^4 \boldsymbol{c}_i$. Since $w(\boldsymbol{c}_i \cap \boldsymbol{c}_j) = 2^{m-2}$ for different i and j, $\bigcap_{i=1}^4 \{S(\boldsymbol{c}_i) \setminus S(\boldsymbol{v})\} = \emptyset$. Then, $|S(\boldsymbol{v})| + \sum_{i=1}^4 |S(\boldsymbol{c}_i) \setminus S(\boldsymbol{v})| = 5 \cdot 2^{m-2} > 2^m$, a contradiction.

□

Corollary 1: For $m \geq 2$,

$$|E_{2^{m-2}}^1(\mathrm{RM}_m)| = |D_m^1| + |D_m^2| + |D_m^3|, \tag{12}$$

$$(2^m - 1)\binom{2^{m-1}}{2^{m-2}} = |D_m^1| + 2|D_m^2| + 3|D_m^3|. \tag{13}$$

Proof: (12) is from (11) and Lemma 6. The left-hand side of (13) is the product of $|\mathrm{RM}_m^*| = 2^{m+1} - 2$ and $|LH^-(\boldsymbol{c})|$ for $\boldsymbol{c} \in \mathrm{RM}_m^*$. This value is equal to the right-hand side from Lemma 6.

□

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 from Corollary 1.

Lemma 7: For $m \geq 2$,

$$D_m^2 = \bigcup_{s_i \in S_m \setminus \{s_1, s_{m+1}\}} \{\boldsymbol{c}_1 \cap \boldsymbol{c}_2 : \boldsymbol{c}_1, \boldsymbol{c}_2 \in C_m(s_i), \boldsymbol{c}_1 \neq \boldsymbol{c}_2\}, \tag{14}$$

$$D_m^3 = \{\boldsymbol{c}_1 \cap \boldsymbol{c}_2 : \boldsymbol{c}_1, \boldsymbol{c}_2 \in C_m(s_1), \boldsymbol{c}_1 \neq \boldsymbol{c}_2\}. \tag{15}$$

Proof: From Lemma 1, if two distinct codewords $\boldsymbol{c}_1, \boldsymbol{c}_2$ have a common larger half, then the larger half is $\boldsymbol{c}_1 \cap \boldsymbol{c}_2$. Since then $l(\boldsymbol{c}_1) = l(\boldsymbol{c}_2)$ from (3), it must be that $\boldsymbol{c}_1, \boldsymbol{c}_2 \in C_m(s_i)$ for some i. For $i = 1$, $\boldsymbol{c}_1 \cap \boldsymbol{c}_2$ is also a larger half of the codeword of $\overline{\boldsymbol{c}_1 + \boldsymbol{c}_2}$ since $\overline{\boldsymbol{c}_1 + \boldsymbol{c}_2} \in C_m(s_1)$ and

$S(\boldsymbol{c}_1 \cap \boldsymbol{c}_2) \subset S(\overline{\boldsymbol{c}_1 + \boldsymbol{c}_2})$. For $2 \le i \le m$, there is no other codeword $\boldsymbol{c} \in C_m(s_i) \setminus \{\boldsymbol{c}_1, \boldsymbol{c}_2\}$ such that $\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \in LH^-(\boldsymbol{c})$. This can be shown by a similar argument of the proof of Lemma 6. For $i = m + 1$, there is only one codeword in $C_m(s_i)$. □

Corollary 2: For $m \ge 2$,

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

Proof: From Lemma 7, 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 $C_m(s_i)$ for $2 \le i \le m$, there is another codeword such that those two have the common larger half. Therefore, we have

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

and

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

from (10). □

The number of uncorrectable errors of weight half the minimum distance is determined by Corollaries 1 and 2.

Theorem 4 ([17]): For $m \ge 2$,

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

The number of correctable errors are obtained by the equation $|E^0_{2^{m-2}}(\mathrm{RM}_m)| + |E^1_{2^{m-2}}(\mathrm{RM}_m)| = \binom{2^m}{2^{m-2}}$. These expressions can be approximated by Stirling's approximation, $n! \approx \sqrt{2\pi n}(n/e)^n$, and thus we have

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

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

We determine the number of correctable errors of weight half the minimum distance plus one for the first-order Reed-Muller codes.

The set $E^1_{2^{m-2}+1}(\mathrm{RM}_m)$ contains $LH^+(\mathrm{RM}^*_m)$, and $LH^+(\mathrm{RM}^*_m)$ contains all minimal uncorrectable errors of weight $2^{m-2}+1$ from (4). Therefore, the remaining uncorrectable errors in $E^1_{2^{m-2}+1}(\mathrm{RM}_m)$ are non-minimal ones.

We will determine the size of $E^1_{2^{m-2}+1}(\mathrm{RM}_m)$ by partitioning the set into two subsets. The first one is the set of vectors of weight $2^{m-2}+1$ that are covered by codewords in RM^*_m. More precisely, it is

$$W_m = \{\boldsymbol{v} \in \mathbb{F}^n_{2^{m-2}+1} : \boldsymbol{v} \subseteq \boldsymbol{c} \text{ for some } \boldsymbol{c} \in \mathrm{RM}^*_m\}, \tag{16}$$

where

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

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, $E^1_{2^{m-2}+1}(\mathrm{RM}_m)\backslash W_m$. Here note that W_m contains $LH^+(\mathrm{RM}^*_m)$ and $LH^+(\mathrm{RM}^*_m)$ contains all minimal uncorrectable errors. Hence a vector in the second set is a non-minimal 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. Define

$$\mathbb{F}^n_1(\boldsymbol{c}) = \{\boldsymbol{e} \in \mathbb{F}^n_1 : \boldsymbol{e} \cap \boldsymbol{c} = \boldsymbol{0}\}$$

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

$$\mathrm{X}_m = \bigcup_{\boldsymbol{c}\in\mathrm{RM}^*_m} \{\boldsymbol{v}+\boldsymbol{e} : \boldsymbol{v} \in LH^-(\boldsymbol{c}), \boldsymbol{e} \in \mathbb{F}^n_1(\boldsymbol{c})\},$$

$$\mathrm{Y}_m = \{\boldsymbol{u} \in \mathrm{X}_m : \boldsymbol{u} \subseteq \boldsymbol{c} \text{ for some } \boldsymbol{c} \in \mathrm{RM}^*_m\},$$

and thus we have

$$|E^1_{2^{m-2}+1}(\mathrm{RM}_m)| = |W_m| + |X_m \setminus Y_m|. \tag{17}$$

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

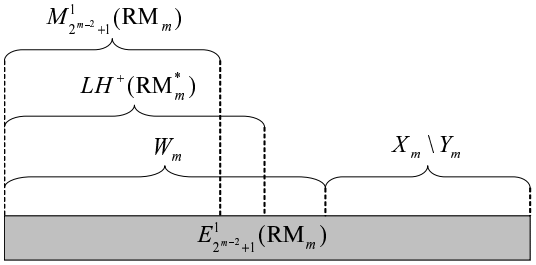

Fig. 1. The structure of $E^1_{2^{m-2}+1}(\mathrm{RM}_m)$.

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 because of the following lemma.

Lemma 8: Let $\boldsymbol{c}$ be a codeword in RM^*_m and $\boldsymbol{v}$ be 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 $\boldsymbol{c}' \neq \overline{\boldsymbol{c}}$ 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 vector 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

$$\begin{aligned} |\tilde{\mathrm{X}}_m| &= |\mathrm{RM}^*_m| \cdot \binom{2^{m-1}-1}{2^{m-2}-1} \cdot 2^{m-1} \\ &= 2^{m-1}(2^m - 1)\binom{2^{m-1}}{2^{m-2}} \end{aligned} \tag{18}$$

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 $\tilde{\mathrm{X}}_m \setminus \tilde{\mathrm{Y}}_m$ is not greater than two.

Lemma 9: The multiplicity of a vector in $\tilde{\mathrm{X}}_m \setminus \tilde{\mathrm{Y}}_m$ is less than or equal to two for $m \geq 5$.

Proof: Let $\boldsymbol{c}_1$, $\boldsymbol{c}_2$, $\boldsymbol{c}_3$ be distinct codewords in RM_m^*. For $1 \le i \le 3$, suppose there exist $\boldsymbol{v}_i, \boldsymbol{e}_i, \boldsymbol{u}$ such that $\boldsymbol{v}_i \in LH^-(\boldsymbol{c}_i)$, $\boldsymbol{e}_i \in \mathbb{F}_1^n(\boldsymbol{c}_i)$, $\boldsymbol{u} = \boldsymbol{v}_i + \boldsymbol{e}_i$, and there exists no $\boldsymbol{c}_4 \in \mathrm{RM}_m^*$ satisfying $\boldsymbol{u} \subseteq \boldsymbol{c}_4$.

First we show that $\boldsymbol{c}_1$, $\boldsymbol{c}_2$, $\boldsymbol{c}_3$, and $\mathbf{1}$ are linearly independent. Since $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \boldsymbol{c}_3) \neq 0$ for $m \ge 4$ from the assumption, we have $\boldsymbol{c}_2 \neq \overline{\boldsymbol{c}_1}$ and $\boldsymbol{c}_3 \neq \overline{\boldsymbol{c}_1}$. If $\boldsymbol{c}_3 = \boldsymbol{c}_1 + \boldsymbol{c}_2$ then $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \boldsymbol{c}_3) = 0$, leading to the contradiction. Suppose $\boldsymbol{c}_3 = \overline{\boldsymbol{c}_1 + \boldsymbol{c}_2}$. If $S(\boldsymbol{e}_1) \in S(\boldsymbol{c}_2) \setminus S(\boldsymbol{c}_1)$ then $\boldsymbol{e}_1 = \boldsymbol{e}_3$ because $\{S(\boldsymbol{c}_2) \setminus S(\boldsymbol{c}_1)\} \cap S(\boldsymbol{c}_3) = \emptyset$. In this case we cannot choose $\boldsymbol{e}_2$ such that $\boldsymbol{e}_2 \in \mathbb{F}_1^n(\boldsymbol{c}_2)$ and $\boldsymbol{e}_2 \subseteq \boldsymbol{c}_1 \cap \boldsymbol{c}_3$. The same thing occurs if $S(\boldsymbol{e}_1) \in S(\boldsymbol{c}_3) \setminus S(\boldsymbol{c}_1)$. Thus the contradiction arises, and $\boldsymbol{c}_1$, $\boldsymbol{c}_2$, $\boldsymbol{c}_3$, and $\mathbf{1}$ are linearly independent.

If $\boldsymbol{v}_1 = \boldsymbol{v}_2$, then $\boldsymbol{v}_1 \in LH^-(\boldsymbol{c}_1) \cap LH^-(\boldsymbol{c}_2)$ and thus $\boldsymbol{v}_1 = \boldsymbol{c}_1 \cap \boldsymbol{c}_2$ from Lemma 4. Since $\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \subseteq \overline{\boldsymbol{c}_1 + \boldsymbol{c}_2}$ and $\boldsymbol{e}_1 \subseteq \overline{\boldsymbol{c}_1 + \boldsymbol{c}_2}$, we have $\boldsymbol{v}_1 + \boldsymbol{e}_1 \subseteq \overline{\boldsymbol{c}_1 + \boldsymbol{c}_2}$, leading to the contradiction. Therefore $\boldsymbol{v}_1$, $\boldsymbol{v}_2$, $\boldsymbol{v}_3$ are distinct, and so are $\boldsymbol{e}_1$, $\boldsymbol{e}_2$, $\boldsymbol{e}_3$. Then $w(\boldsymbol{v}_1 \cap \boldsymbol{v}_2 \cap \boldsymbol{v}_3) = 2^{m-2} - 2$, and thus $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \boldsymbol{c}_3) \ge w(\boldsymbol{v}_1 \cap \boldsymbol{v}_2 \cap \boldsymbol{v}_3) = 2^{m-2} - 2$. On the other hand, $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \boldsymbol{c}_3) = 2^{m-3}$ from Lemma 3. Thus we have $2^{m-3} \ge 2^{m-2} - 2$. The contradiction arises for the case $m \ge 5$. □

Thus the size of $\mathrm{X}_m \setminus \mathrm{Y}_m$ is represented as follows.

$$|\mathrm{X}_m \setminus \mathrm{Y}_m| = |\tilde{\mathrm{X}}_m| - |\tilde{\mathrm{Y}}_m| - \frac{|\tilde{\mathrm{Z}}_m|}{2}, \tag{19}$$

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

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

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

Lemma 10: Let $\boldsymbol{c}_1, \boldsymbol{c}_2 \in \mathrm{RM}_m^*$. Then

1) there exist $\boldsymbol{v} \in LH^-(\boldsymbol{c}_1)$, $\boldsymbol{e} \in \mathbb{F}_1^n(\boldsymbol{c}_1)$ satisfying $\boldsymbol{v} + \boldsymbol{e} \subseteq \boldsymbol{c}_2$ if and only if

$$\boldsymbol{c}_1 \neq \boldsymbol{c}_2 \text{ and } l(\boldsymbol{c}_1) \in S(\boldsymbol{c}_2); \tag{20}$$

2) if (20) holds, then

$$\{(\boldsymbol{v}, \boldsymbol{e}) : \boldsymbol{v} \in LH^-(\boldsymbol{c}_1), \boldsymbol{e} \in \mathbb{F}_1^n(\boldsymbol{c}_1), \boldsymbol{v} + \boldsymbol{e} \subseteq \boldsymbol{c}_2\}$$
$$= \{(\boldsymbol{c}_1 \cap \boldsymbol{c}_2, \boldsymbol{e}) : \boldsymbol{e} \in \mathbb{F}_1^n, S(\boldsymbol{e}) \subseteq S(\boldsymbol{c}_2) \setminus S(\boldsymbol{c}_1)\}. \tag{21}$$

Proof: (First part) The only if part is obvious. We prove the if part. Let $\boldsymbol{v} = \boldsymbol{c}_1 \cap \boldsymbol{c}_2$. Since $\boldsymbol{c}_1 \neq \boldsymbol{c}_2$ and $\boldsymbol{c}_1 + \boldsymbol{c}_2 \neq \mathbf{1}$ from (20), we have $w(\boldsymbol{v}) = 2^{m-2}$ from Lemma 3. We have $l(\boldsymbol{v}) = l(\boldsymbol{c}_1)$ from $l(\boldsymbol{c}_1) \in S(\boldsymbol{c}_2)$. Thus $\boldsymbol{v} \in LH^-(\boldsymbol{c}_1)$. If we take $\boldsymbol{e} \in \mathbb{F}_1^n(\boldsymbol{c}_1)$ such that $S(\boldsymbol{e}) \subseteq S(\boldsymbol{c}_2) \setminus S(\boldsymbol{c}_1)$, then $\boldsymbol{v} + \boldsymbol{e} \subseteq \boldsymbol{c}_2$.

(Second part) The $\supseteq$ part is obvious, so we show the $\subseteq$ part. Since $\boldsymbol{v} \subseteq \boldsymbol{c}_1$ and $\boldsymbol{v} \subseteq \boldsymbol{c}_2$, it holds that $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2) \geq w(\boldsymbol{v}) = 2^{m-2}$. We also have $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2) = 2^{m-2}$. Therefore we have $\boldsymbol{v} = \boldsymbol{c}_1 \cap \boldsymbol{c}_2$. It immediately follows that $S(\boldsymbol{e}) \subseteq S(\boldsymbol{c}_2) \setminus S(\boldsymbol{c}_1)$ from $\boldsymbol{c}_1 \cap \boldsymbol{e} = \mathbf{0}$ and $\boldsymbol{v} + \boldsymbol{e} \subseteq \boldsymbol{c}_2$. □

From Lemma 10, $\boldsymbol{v} + \boldsymbol{e} \in \tilde{\mathrm{X}}_m$ is covered by every $\boldsymbol{c}_2 \in \mathrm{RM}_m^*$ satisfying (20). The number of codewords $\boldsymbol{c}_2$ satisfying (20) is $|\mathrm{RM}_m|/2 - 2 = 2^m - 2$. There are $|S(\boldsymbol{c}_2) \setminus S(\boldsymbol{c}_1)| = 2^{m-2}$ choices of $\boldsymbol{e}$ from (21). Thus we have

$$\begin{aligned} |\tilde{\mathrm{Y}}_m| &= |\mathrm{RM}_m^*| \cdot (2^m - 2) \cdot 2^{m-2} \\ &= 2^m(2^m - 1)(2^{m-1} - 1). \end{aligned} \tag{22}$$

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

Lemma 11: 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 $m \geq 5$, 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: First note that $\boldsymbol{c}_1 + \boldsymbol{c}_2 \neq \mathbf{1}$ since $\boldsymbol{v}_1 + \boldsymbol{e}_1 = \boldsymbol{v}_2 + \boldsymbol{e}_2$ cannot hold for $m \geq 3$ if $\boldsymbol{c}_1 + \boldsymbol{c}_2 = \mathbf{1}$. (Only if part) We have $\boldsymbol{c}_1 \neq \boldsymbol{c}_3$ 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 $\boldsymbol{v}_1 = \boldsymbol{c}_1 \cap \boldsymbol{c}_3$. 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 $w(\boldsymbol{v}_1 \cap \boldsymbol{v}_2) = w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \boldsymbol{c}_3)$. Since $\boldsymbol{c}_1$, $\boldsymbol{c}_2$, $\boldsymbol{c}_3$ are distinct, $w(\boldsymbol{c}_1 \cap \boldsymbol{c}_2 \cap \boldsymbol{c}_3)$ is either 2^{m-2}, 2^{m-3}, or 0 from Lemma 5. We have $w(\boldsymbol{v}_1 \cap \boldsymbol{v}_2)$ is 2^{m-2} if $\boldsymbol{v}_1 = \boldsymbol{v}_2$, and is $2^{m-2} - 2$ 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 $m \geq 5$ from the fact $2^{m-3} \neq 2^{m-2} - 2$. Hence $\boldsymbol{v}_1 = \boldsymbol{v}_2$, and thus $\boldsymbol{e}_1 = \boldsymbol{e}_2$.

(If part) Since $\boldsymbol{e}_1 = \boldsymbol{e}_2$ and $\boldsymbol{c}_1 \neq \boldsymbol{c}_2$, we have $\boldsymbol{v}_1 = \boldsymbol{v}_2 = \boldsymbol{c}_1 \cap \boldsymbol{c}_2 \subseteq \overline{\boldsymbol{c}_1 + \boldsymbol{c}_2}$. Since $\boldsymbol{e}_1 \cap \boldsymbol{c}_1 = \boldsymbol{e}_2 \cap \boldsymbol{c}_2 = \boldsymbol{e}_1 \cap \boldsymbol{c}_2 = \mathbf{0}$, we have $\boldsymbol{e}_1 \subseteq \overline{\boldsymbol{c}_1 + \boldsymbol{c}_2}$. By taking $\boldsymbol{c}_3 = \overline{\boldsymbol{c}_1 + \boldsymbol{c}_2}$ we have $\boldsymbol{u} = \boldsymbol{v}_1 + \boldsymbol{e}_1 \subseteq \boldsymbol{c}_3$. □

From Lemma 11, for each $\boldsymbol{c}_1 \in \mathrm{RM}_m^*$, $|\tilde{\mathrm{Z}}_m|$ is obtained by counting all patterns in $\{\boldsymbol{v}_1 + \boldsymbol{e}_1 : \boldsymbol{v}_1 \in LH^-(\boldsymbol{c}_1), \boldsymbol{e}_1 \in \mathbb{F}_1^n(\boldsymbol{c}_1)\}$ such that $\boldsymbol{v}_1 + \boldsymbol{e}_1 = \boldsymbol{v}_2 + \boldsymbol{e}_2$ for some $\boldsymbol{v}_2, \boldsymbol{e}_2$ with $\boldsymbol{v}_2 \in$

$LH^-(\boldsymbol{c}_2), \boldsymbol{c}_2 \in \mathrm{RM}_m^* \setminus \{\boldsymbol{c}_1\}, \boldsymbol{e}_2 \in \mathbb{F}_1^n(\boldsymbol{c}_2)$ and $\boldsymbol{e}_1 \neq \boldsymbol{e}_2$. We will count such $\boldsymbol{v}_1 + \boldsymbol{e}_1$ for each $\boldsymbol{c}_1 \in \mathrm{RM}_m^*$.

There are three cases to be considered:

1) The case that $l(\boldsymbol{c}_1) = l(\boldsymbol{c}_2)$; we choose $\boldsymbol{w}$ such that $\boldsymbol{w} \subseteq \boldsymbol{c}_1 \cap \boldsymbol{c}_2, w(\boldsymbol{w}) = 2^{m-2} - 1$, and $l(\boldsymbol{w}) = l(\boldsymbol{c}_1 \cap \boldsymbol{c}_2)$. We choose $\boldsymbol{e}_2$ so that $S(\boldsymbol{e}_2) \subseteq S(\boldsymbol{c}_1) \setminus S(\boldsymbol{c}_2)$, and choose $\boldsymbol{e}_1$ so that $S(\boldsymbol{e}_1) \subseteq S(\boldsymbol{c}_2) \setminus S(\boldsymbol{c}_1)$. Then letting $\boldsymbol{v}_1 = \boldsymbol{w} + \boldsymbol{e}_2$ and $\boldsymbol{v}_2 = \boldsymbol{w} + \boldsymbol{e}_1$ gives vectors as $\boldsymbol{v}_1 + \boldsymbol{e}_1 = \boldsymbol{v}_2 + \boldsymbol{e}_2$. There are $(2^{m-2} - 1) \cdot 2^{m-2} \cdot 2^{m-2}$ such $\boldsymbol{v}_1 + \boldsymbol{e}_1$.
   For each codeword $\boldsymbol{c}_1$ in $C_m(s_i)$ there are $|C_m(s_i)| - 1$ codewords $\boldsymbol{c}_2$ in RM_m^* satisfying $l(\boldsymbol{c}_1) = l(\boldsymbol{c}_2)$.
2) The case that $l(\boldsymbol{c}_1) > l(\boldsymbol{c}_2)$; since $\boldsymbol{v}_1 \in LH^-(\boldsymbol{c}_1)$ and $\boldsymbol{v}_2 \in LH^-(\boldsymbol{c}_2)$, the $l(\boldsymbol{c}_2)$-th bit of $\boldsymbol{e}_1$ is one.

   a) If the $l(\boldsymbol{c}_1)$-th bit of $\boldsymbol{c}_2$ is one; we choose $\boldsymbol{w}$ such that $\boldsymbol{w} \subseteq \boldsymbol{c}_1 \cap \boldsymbol{c}_2, w(\boldsymbol{w}) = 2^{m-2} - 1$, and $l(\boldsymbol{w}) = l(\boldsymbol{c}_1 \cap \boldsymbol{c}_2)$. We choose $\boldsymbol{e}_2$ so that $S(\boldsymbol{e}_2) \subseteq S(\boldsymbol{c}_1) \setminus S(\boldsymbol{c}_2)$. Then letting $\boldsymbol{v}_1 = \boldsymbol{w} + \boldsymbol{e}_2$ and $\boldsymbol{v}_2 = \boldsymbol{w} + \boldsymbol{e}_1$ gives vectors as $\boldsymbol{v}_1 + \boldsymbol{e}_1 = \boldsymbol{v}_2 + \boldsymbol{e}_2$. There are $(2^{m-2} - 1) \cdot 2^{m-2}$ such $\boldsymbol{v}_1 + \boldsymbol{e}_1$.
      For each codeword $\boldsymbol{c}_1$ in $C_m(s_i)$ with $i \geq 2$, there are $\left(\left(\sum_{j<i} |C_m(s_j)| + 1\right)/2 - 1\right)$ codewords $\boldsymbol{c}_2$ in RM_m^* satisfying $l(\boldsymbol{c}_1) \in S(\boldsymbol{c}_2)$.
   b) If the $l(\boldsymbol{c}_1)$-th bit of $\boldsymbol{c}_2$ is zero; then $\boldsymbol{e}_2$ must be the vector having one in the $l(\boldsymbol{c}_1)$-th bit. We choose $\boldsymbol{w}$ such that $\boldsymbol{w} \subseteq \boldsymbol{c}_1 \cap \boldsymbol{c}_2$ and $w(\boldsymbol{w}) = 2^{m-2} - 1$. Then letting $\boldsymbol{v}_1 = \boldsymbol{w} + \boldsymbol{e}_2$ and $\boldsymbol{v}_2 = \boldsymbol{w} + \boldsymbol{e}_1$ gives vectors as $\boldsymbol{v}_1 + \boldsymbol{e}_1 = \boldsymbol{v}_2 + \boldsymbol{e}_2$. There are 2^{m-2} such $\boldsymbol{v}_1 + \boldsymbol{e}_1$.
      For each codeword $\boldsymbol{c}_1$ in $C_m(s_i)$ with $i \geq 2$, there are $\left(\left(\sum_{j<i} |C_m(s_j)| + 1\right)/2 - 1\right)$ codewords $\boldsymbol{c}_2$ in RM_m^* satisfying $l(\boldsymbol{c}_1) \notin S(\boldsymbol{c}_2)$ and $\boldsymbol{c}_1 + \boldsymbol{c}_2 \neq \mathbf{1}$.

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

From the above analysis we have

$$\begin{aligned}|\tilde{\mathrm{Z}}_m| &= \sum_{i=1}^{m+1} |C_m(s_i)|(|C_m(s_i)|-1)(2^{m-2}-1)(2^{m-2})^2 \\ &\quad + 2\sum_{i=2}^{m+1} |C_m(s_i)| \left(\frac{1}{2}\left(\sum_{j=1}^{i-1}|C_m(s_j)|+1\right)-1\right)(2^{m-2}-1)2^{m-2} \\ &\quad + 2\sum_{i=2}^{m+1} |C_m(s_i)| \left(\frac{1}{2}\left(\sum_{j=1}^{i-1}|C_m(s_j)|+1\right)-1\right)2^{m-2} \\ &= 2^{2m-3}\binom{2^m}{3}. \end{aligned} \tag{23}$$

From (17), (18), (19), (22), and (23), we can determine the number of uncorrectable errors of weight $2^{m-2}+1$ for RM_m.

Theorem 5: For $m \geq 5$,

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

The number of correctable errors of weight $2^{m-2}+1$ is obtained from the equation,

$$|E^0_{2^{m-2}+1}(\mathrm{RM}_m)| + |E^1_{2^{m-2}+1}(\mathrm{RM}_m)| = \binom{2^m}{2^{m-2}+1}.$$

The expressions for $|E^0_{2^{m-2}+1}(\mathrm{RM}_m)|$ and $|E^1_{2^{m-2}+1}(\mathrm{RM}_m)|$ are approximated as

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

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 gives a better upper bound on the numbers of uncorrectable errors than (6) by using the bound of [11, 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

$$|M^1_i(\mathrm{RM}_m)| = \begin{cases} 0 & \text{for } \ 0 \leq i \leq 2^{m-2}-1, 2^{m-2}+2 \leq i \leq n, \\ |E^1_{2^{m-2}}(\mathrm{RM}_m)| & \text{for } \ i = 2^{m-2}. \end{cases} \tag{24}$$

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

$$|M^1_{2^{m-2}+1}(\mathrm{RM}_m)| = |LH^+(\mathrm{RM}^*_m)| - |LH^+(\mathrm{RM}^*_m) \setminus M^1(\mathrm{RM}_m)|. \tag{25}$$

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 8 there is no common larger half of weight $2^{m-2}+1$ of more than one codeword in RM^*_m. Therefore

$$\begin{aligned} |LH^+(\mathrm{RM}^*_m)| &= \binom{2^{m-1}-1}{2^{m-2}+1} \cdot |\mathrm{RM}^*_m| \\ &= 2(2^m-1)\binom{2^{m-1}-1}{2^{m-2}+1}. \end{aligned} \tag{26}$$

Next we will determine $|LH^+(\mathrm{RM}^*_m) \setminus M^1(\mathrm{RM}_m)|$. For $\boldsymbol{v} \in LH^+(\mathrm{RM}^*_m)$, $\boldsymbol{v} \notin M^1(\mathrm{RM}_m)$ if and only if $\boldsymbol{v} \supseteq \boldsymbol{v}'$ for some $\boldsymbol{v}' \in LH^-(\mathrm{RM}^*_m)$. Then the following lemma holds.

Lemma 12: Let $\boldsymbol{c}, \boldsymbol{c}'$ be codewords in RM^*_m. Then

1) there exist $\boldsymbol{v} \in LH^+(\boldsymbol{c}), \boldsymbol{v}' \in LH^-(\boldsymbol{c}')$ satisfying $\boldsymbol{v} \supseteq \boldsymbol{v}'$ if and only if

$$l(\boldsymbol{c}) < l(\boldsymbol{c}') \text{ and } l(\boldsymbol{c}') \in S(\boldsymbol{c}); \tag{27}$$

2) if (27) holds, then

$$\begin{aligned} &\{(\boldsymbol{v}, \boldsymbol{v}') : \boldsymbol{v} \in LH^+(\boldsymbol{c}), \boldsymbol{v}' \in LH^-(\boldsymbol{c}'), \boldsymbol{v}' \subseteq \boldsymbol{v}\} \\ &\qquad = \{(\boldsymbol{c} \cap \boldsymbol{c}' + \boldsymbol{e}, \boldsymbol{c} \cap \boldsymbol{c}') : \boldsymbol{e} \in \mathbb{F}^n_1, S(\boldsymbol{e}) \subseteq S(\boldsymbol{c}) \setminus \{S(\boldsymbol{c}') \cup \{l(\boldsymbol{c})\}\}. \end{aligned} \tag{28}$$

Proof: (First part) We first show the if part. From (27), we have $\boldsymbol{c} + \boldsymbol{c}' \neq \boldsymbol{0}, \boldsymbol{1}$ and thus $w(\boldsymbol{c} \cap \boldsymbol{c}') = 2^{m-2}$ from Lemma 3. If we take $\boldsymbol{v}' = \boldsymbol{c} \cap \boldsymbol{c}'$ then $\boldsymbol{v}' \in LH^-(\boldsymbol{c}')$. Since $\boldsymbol{v}' \subseteq \boldsymbol{c}$ and $l(\boldsymbol{v}') = l(\boldsymbol{c}') > l(\boldsymbol{c})$, there exists $\boldsymbol{v} \in LH^+(\boldsymbol{c})$ satisfying $\boldsymbol{v}' \subseteq \boldsymbol{v}$. Next we show the only if part. The inequality $l(\boldsymbol{c}) < l(\boldsymbol{c}')$ comes from $l(\boldsymbol{c}) < l(\boldsymbol{v}) \leq l(\boldsymbol{v}') = l(\boldsymbol{c}')$, and $l(\boldsymbol{c}') \in S(\boldsymbol{c})$ comes from $l(\boldsymbol{c}') = l(\boldsymbol{v}') \in S(\boldsymbol{v}') \subseteq S(\boldsymbol{v}) \subseteq S(\boldsymbol{c})$.

(Second part) From the discussion on the first part of the proof, $\boldsymbol{v}' = \boldsymbol{c} \cap \boldsymbol{c}'$. Then $\boldsymbol{v} \in LH^+(\boldsymbol{c})$ if and only if $\boldsymbol{v} = \boldsymbol{v} + \boldsymbol{e}, \boldsymbol{e} \in \mathbb{F}^n_1, S(\boldsymbol{c}) \setminus \{S(\boldsymbol{c}') \cup \{l(\boldsymbol{c})\}\}$. □

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

Lemma 13: For $\boldsymbol{v} \in LH^+(\mathrm{RM}^*_m)$, there is at most one $\boldsymbol{v}' \in LH^-(\mathrm{RM}^*_m)$ such that $\boldsymbol{v}' \subseteq \boldsymbol{v}$ for $m \geq 4$.

Proof: Suppose there are two distinct vectors $\boldsymbol{v}' \in LH^-(\boldsymbol{c}')$ and $\boldsymbol{v}'' \in LH^-(\boldsymbol{c}'')$ such that $\boldsymbol{v}' \subseteq \boldsymbol{v}$ and $\boldsymbol{v}'' \subseteq \boldsymbol{v}$ for some $\boldsymbol{c}', \boldsymbol{c}'' \in \mathrm{RM}_m^*$. Then we have $\boldsymbol{v}' = \boldsymbol{c} \cap \boldsymbol{c}'$ and $\boldsymbol{v}'' = \boldsymbol{c} \cap \boldsymbol{c}''$ from Lemma 12. The vector $\boldsymbol{v}$ is represented as $\boldsymbol{v}' + \boldsymbol{e}_1$ and $\boldsymbol{v}'' + \boldsymbol{e}_2$ for vectors $\boldsymbol{e}_1, \boldsymbol{e}_2 \in \mathbb{F}_1^n$. Then $d(\boldsymbol{v}', \boldsymbol{v}'') = d(\boldsymbol{v} + \boldsymbol{e}_1, \boldsymbol{v} + \boldsymbol{e}_2) = 2$, where $d(\boldsymbol{x}, \boldsymbol{y})$ is the Hamming distance between $\boldsymbol{x}$ and $\boldsymbol{y}$. However, $d(\boldsymbol{v}', \boldsymbol{v}'') = d(\boldsymbol{c} \cap \boldsymbol{c}', \boldsymbol{c} \cap \boldsymbol{c}'') \geq 2^{m-2}$ because $\boldsymbol{v}'$ and $\boldsymbol{v}''$ 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 $\boldsymbol{v} \in LH^+(\boldsymbol{c})$ covers $\boldsymbol{v}' \in LH^-(\boldsymbol{c}')$ for $\boldsymbol{c}' \in \mathrm{RM}_m^*$, then $\boldsymbol{v}'$ is unique for $\boldsymbol{v}$ from Lemma 13. Then the number of $\boldsymbol{v}$ in $LH^+(\boldsymbol{c})$ that covers $\boldsymbol{v}'$ is the size of $S(\boldsymbol{c}) \setminus \{S(\boldsymbol{c}') \cup \{l(\boldsymbol{c})\}\}$ from (28), which is equal to $2^{m-2} - 1$. If we know the number of codewords whose larger halves cover $\boldsymbol{v}'$ for each $\boldsymbol{v}' \in LH^-(\mathrm{RM}_m^*)$, 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 $\boldsymbol{v}' \in LH^-(\mathrm{RM}_m^*)$ such that $\boldsymbol{v}' \subseteq \boldsymbol{v}$ for some $\boldsymbol{v} \in LH^+(\mathrm{RM}_m^*)$. Suppose $\boldsymbol{v}' \in LH^-(\boldsymbol{c}')$ and $\boldsymbol{c}' \in C_m(s_i)$. Note from (27) that $i \neq 1$ because if $i = 1$ there is no $\boldsymbol{c}$ such that $l(\boldsymbol{c}) < s_i$. For $\boldsymbol{c}' \in C_m(s_i)$ with $i \leq 2$, the number of $\boldsymbol{c} \in \mathrm{RM}_m^*$ satisfying (27) 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 (28) we have $\boldsymbol{v}' = \boldsymbol{c} \cap \boldsymbol{c}'$. Then there may be other codeword $\boldsymbol{c}'' \in \mathrm{RM}_m^*$ such that $\boldsymbol{v}' = \boldsymbol{c} \cap \boldsymbol{c}''$. 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 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 is because, as in the proof of Lemma 7, 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 $\boldsymbol{v}' \in LH^-(\mathrm{RM}_m^*)$ such that $\boldsymbol{v}' \subseteq \boldsymbol{v}$ for some $\boldsymbol{v} \in LH^+(\mathrm{RM}_m^*)$ is

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

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 14: 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 $0 \leq i \leq n$,

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

Proof: The statement follows from Theorem 4, (24), (25), (26), and Lemma 14. □

By Stirling's approximation, we have $|M^1_{2^{m-2}+1}(\mathrm{RM}_m)| \approx |LH^+(\mathrm{RM}_m^*)| \approx \sqrt{\frac{2^m}{\pi}} 2^{2^{m-1}+1}$.

V. Trial Sets

In this section, the size of trial sets for general linear codes and the first-order Reed-Muller codes is studied. 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 a minimum distance decoding. The algorithm is described in [11]. 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 $T_{\min}$. Note that $T_{\min}$ 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 $|T_{\min}| \leq |C^*|$. Let us define T_{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 $\boldsymbol{c} \in C^*$,

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

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

TABLE II

BOUNDS OF THE SIZE OF MINIMUM TRIAL SETS FOR SOME BCH, EXTENDED BCH, AND REED-MULLER CODES.

(n,k) code C	Lower bounds		$\lvert T_{\min}\rvert$	Upper bounds	
	New			[11]	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*
(16,5) RM	5	30*	30	30*	30*

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

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

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

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

From the definition of $T_{\rm nec}$, $T_{\min}$ contains $T_{\rm nec}$. We show that the number of remaining codewords that should be in $T_{\min}$, that is $|T_{\min} \setminus T_{\rm nec}|$, is upper bounded by $|M^1(C) \setminus LH(T_{\rm nec})|$. Since the larger halves of $T_{\min}$ contain $M^1(C)$ from the definition of trial sets, the larger halves of the set $T_{\min} \setminus T_{\rm nec}$ should contain the set $M^1(C) \setminus LH(T_{\rm nec})$. Therefore, $|T_{\min} \setminus T_{\rm nec}| \leq |M^1(C) \setminus LH(T_{\rm nec})|$, and thus $|T_{\min}| \leq |T_{\rm nec}| + |M^1(C) \setminus LH(T_{\rm nec})|$. □

While a naive algorithm for computing $|T_{\min}|$ 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, above bounds are useful to estimate $|T_{\min}|$.

We compute the bounds in Theorem 7 and the upper bound $|C^*|$ for some codes. The results are shown in Table II. The new upper bound is tight for all codes compared to the known bound.

The upper and lower bounds coincide for three codes, the $(15, 5)$ BCH code, the $(16, 5)$ extended BCH code, and the $(16, 5)$ Reed-Muller code.

B. First-Order Reed-Muller Codes

We determine the minimum trial set $T_{\min}$ 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_{nec} for $m \geq 4$.

Lemma 15: Let $\boldsymbol{c} \in \mathrm{RM}_m^*$ with $m \geq 4$. 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 4. 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 $LH^-(\boldsymbol{c})$ which 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 $m \geq 4$. □

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

Proof: From Lemma 15, 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 $\mathrm{RM}_m^* \subseteq T_{\mathrm{nec}} \subseteq T_{\min}$. From (5) we have $T_{\min} \subseteq \mathrm{RM}_m^*$. □

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

VI. Conclusion and Future Work

In this paper, we have studied 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 codes satisfying some conditions. 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 is 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 larger half is introduced for characterizing minimal uncorrectable errors, our lower bound cannot be a good bound for the size of uncorrectable errors.

To apply the analysis using the monotone error structure for other specific codes, such as the second-order Reed-Muller codes and BCH codes, is another avenue. Even the number of uncorrectable errors of weight $\lceil d/2 \rceil$ is not known for them.

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 size of minimum trial sets for longer codes or random linear codes will be important for the applications of trial sets. In this connection, estimating the time-complexity of the trial set decoding is another future work.

REFERENCES

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

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

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

[4] 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.

[5] C. Carlet, "Boolean functions for cryptography and error correcting codes," to appear in Y. Crama and P. Hammer, Eds. *Boolean Methods and Models*, Cambridge University Press.

[6] 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, Sept. 1994.

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

[8] Y. Desaki, T. Fujiwara, and T. Kasami, "The weight distributions of extended binary primitive BCH codes of length 128," *IEEE Trans. Inf. Theory*, vol. 43, no. 4, July, 1997.

[9] E.N. Gilbert, "A comparison of signalling alphabets," *Bell System Technical Journal*, vol. 31, pp. 504–522, 1952.

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

[11] 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.

[12] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland, 1977.

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

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

[15] 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, July 1994.

[16] R.R. Varshamov, "Estimate of the number of signals in error correcting codes," *Doklady Akadamii Nauk SSSR*, vol. 117, pp. 739–741, 1957.

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

[18] G. Zémor, "Threshold effects in codes," in *Proc. Algebraic Coding*, Paris, France, 1993, *Lecture Notes in Computer Science*, vol. 781, Springer, pp. 278–286, 1994.