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

Kenji Yasunaga Toru Fujiwara

Osaka University, Japan

Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC-17),
Indian Institute of Science, Bangalore, December 16-20, 2007

Summary of the Work

Main Result

- An explicit expression for #(correctable errors of weight $d/2+1$) for the first-order Reed-Muller codes is derived
  - d : the minimum distance of the code

Main Techniques

- Monotone error structure (Larger half)
  - Monotone error structure appeared in [Peterson, Weldon, 1972]
  - Larger half was introduced by [Helleseth, Kløve, Levenshtein, 2005]

Outline

- Correctable Errors
- First-order Reed-Muller Codes
- Previous Results
- Our Results
- Monotone Error Structure
- Proof Sketch of Our Results

Outline

- Correctable Errors
- First-order Reed-Muller Codes
- Previous Results
- Our Results
- Monotone Error Structure
- Proof Sketch of Our Results

Problem Setting

- Binary linear code $C \subseteq \{0,1\}^n$

- Error vector $\boldsymbol{e} \in \{0,1\}^n$

- If $w(\boldsymbol{e}) < d/2 \;\Rightarrow\; \boldsymbol{e}$ is always correctable
  If $w(\boldsymbol{e}) \geq d/2 \;\Rightarrow\;$?
  - $w(\boldsymbol{x})$: the Hamming weight of $\boldsymbol{x}$

In this work, we investigate

#(correctable errors of weight $\boldsymbol{i}$) for $\boldsymbol{i} \geq d/2$

Correctable/Uncorrectable Errors

- Correctable errors $E^0(C)$
  $=$ Correctable by Minimum Distance (MD) decoding
  - $E^0{}_i(C)$: Correctable errors of weight $\boldsymbol{i}$

- Uncorrectable errors $E^1(C) = \{0,1\}^n \setminus E^0(C)$
  - $E^1{}_i(C)$: Uncorrectable errors of weight $\boldsymbol{i}$
  - $|E_i^0(C)| + |E_i^1(C)| = \binom{n}{i}$

- MD decoding
  - Output a nearest (w.r.t. Hamming dist.) codeword to the input
  - Perform ML decoding for binary symmetric channels
  - Syndrome decoding is an MD decoding

Syndrome Decoding

- Coset partitioning

$$\{0,1\}^n = \bigcup_{i=1}^{2^{n-k}} C_i, \quad C_i \cap C_j = \phi \ \text{ for } \ i \neq j$$

$$C_i = \{\boldsymbol{v}_i + \boldsymbol{c} : \boldsymbol{c} \in C\}$$: Coset of C

$$\boldsymbol{v}_i = \arg\min_{v \in C_i} w(\boldsymbol{v})$$: Coset leader of C_i

- Syndrome decoding
  - Output $\boldsymbol{y} + \boldsymbol{v}_i$ if $\boldsymbol{y} \in C_i$ ($\boldsymbol{y}$ is the input)
  - Coset leaders = Correctable errors
  - Perform MD decoding

Outline

- Correctable Errors
- First-order Reed-Muller Codes
- Previous Results
- Our Results
- Monotone Error Structure
- Proof Sketch of Our Results

First-Order Reed-Muller Code

- RM_m : The first-order Reed-Muller code of length 2^m
  - Dimension $= m+1$
  - Minimum distance $d = 2^{m-1}$

- $\mathrm{RM}_m \Leftrightarrow$ Linear Boolean functions with m variables

  $|E^0{}_i(\mathrm{RM}_m)|\times 2^{m+1}$ = #(Boolean func. of nonlinearity $\boldsymbol{i}$)
  - Nonlinearity of Boolean function $\boldsymbol{f}$
    - Distance between $\boldsymbol{f}$ and linear Boolean functions
    - Important criteria for cryptographic applications [Canteaut, Carlet, Charpin, Fontaine, 2001]

Outline

- Correctable Errors
- First-order Reed-Muller Codes
- Previous Results
- Our Results
- Monotone Error Structure
- Proof Sketch of Our Results

Previous Results for $|E^0(\mathrm{RM}_m)|$

- [Berlekamp, Welch, 1972]
  - The weight distributions of all cosets of RM_5
    $\Rightarrow |E^0{}_i(\mathrm{RM}_5)|$ for all $0 \le i \le n$
  - By computer

- [Wu, 1998]
  - An explicit expression for $|E^0{}_{d/2}(\mathrm{RM}_m)|$
  - By revealing the structure of coset leaders of weight $d/2$
    1. Coset leaders of weigh $d/2$ $\Rightarrow$ 3 types
    2. Determine #(coset leaders) for each type

Outline

- Correctable Errors
- First-order Reed-Muller Codes
- Previous Results
- Our Results
- Monotone Error Structure
- Proof Sketch of Our Results

Our Results

- An explicit expression for $|E^0{}_{d/2+1}(\mathrm{RM}_m)|$
  - By using the monotone error structure (Larger half)
    - Monotone error structure appeared in [Peterson, Weldon, 1972]
    - Larger half was introduced by [Helleseth, Kløve, Levenshtein 2005]
  - Lead to #(Boolean functions of nonlinarity $d/2+1$)
  - Compared to [Wu, 1998],
    - Our approach does not fully reveal the structure of coset leaders of weight $d/2+1$
    - Our approach can give a simpler proof for $|E^0{}_{d/2}(\mathrm{RM}_m)|$

Outline

- Correctable Errors
- First-order Reed-Muller Codes
- Previous Results
- Our Results
- Monotone Error Structure
- Proof Sketch of Our Results

Monotone Error Structure

- Recall that a coset leader is a minimum weight vector in a coset
- There may be one more minimum weight vectors in the same coset
  ⇒ Any of them will do
- If we take the lexicographically smallest one for all cosets,
  ⇒ Correctable/uncorrectable errors have a monotone structure

Monotone Error Structure

- Notation
  - Support of $\boldsymbol{v}$: $S(\boldsymbol{v}) = \{ i : v_i \neq 0 \}$
  - $\boldsymbol{v}$ is covered by $\boldsymbol{u}$: $S(\boldsymbol{v}) \subseteq S(\boldsymbol{u})$

- Monotone error structure

  $\boldsymbol{v}$ is correctable

  $\Rightarrow$ all $\boldsymbol{u}$ s.t. $S(\boldsymbol{v}) \subseteq S(\boldsymbol{u})$ are correctable

  $\boldsymbol{v}$ is uncorrectable

  $\Rightarrow$ all $\boldsymbol{u}$ s.t. $S(\boldsymbol{u}) \supseteq S(\boldsymbol{v})$ are uncorrectable

- Example
  - 1100 is correctable $\Rightarrow$ 0000, 1000, 0100 are correctable
  - 0011 is uncorrectable $\Rightarrow$ 1011, 0111, 1111 are uncorrectable

Minimal uncorrectable errors

- Errors have the monotone structure (w.r.t $\subseteq$)
  $\Rightarrow E^1(C)$ is characterized by minimal vectors (w.r.t. $\subseteq$)

- Minimal uncorrectable errors $M^1(C)$
  - = Minimal vectors (w.r.t. $\subseteq$) in $E^1(C)$
  - $M^1(C)$ uniquely determines $E^1(C)$

- Larger half $LH(\boldsymbol{c})$ of $\boldsymbol{c} \in C$
  - Introduced for characterizing $M^1(C)$ in [HKL2005]
  - Combinatorial construction is given in [HKL2005]
  - $M^1(C) \subseteq LH(C \setminus \{\mathbf{0}\})$, where $LH(S) = \bigcup_{c \in S} LH(\boldsymbol{c})$

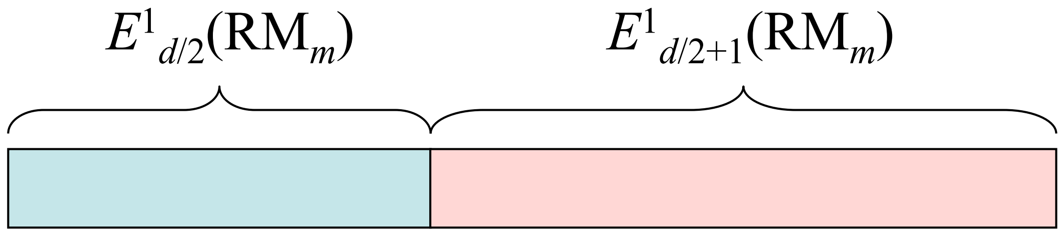
Outline

- Correctable Errors
- First-order Reed-Muller Codes
- Previous Results
- Our Results
- Monotone Error Structure
- Proof Sketch of Our Results

Proof Sketch of Our Results

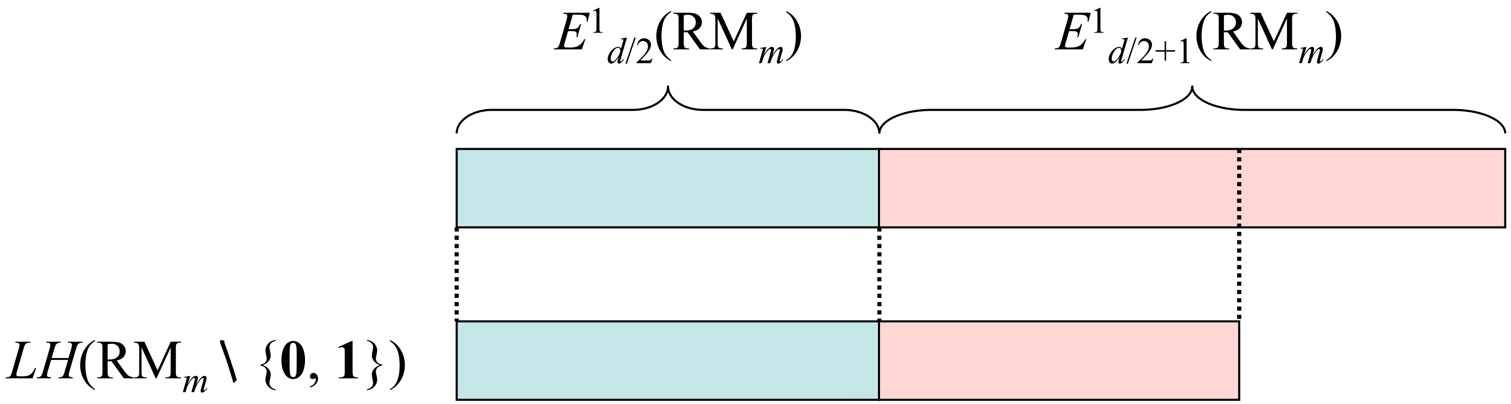
- We will determine $|E^1{}_{d/2+1}(\mathrm{RM}_m)|$

- Observe the relations between $E^1{}_{d/2}(\mathrm{RM}_m)$, $E^1{}_{d/2+1}(\mathrm{RM}_m)$, $LH(\mathrm{RM}_m \setminus \{\mathbf{0}, \mathbf{1}\})$, $M^1(\mathrm{RM}_m)$



Proof Sketch of Our Results

- We will determine $|E^1_{d/2+1}(\mathrm{RM}_m)|$
- Observe the relations between $E^1_{d/2}(\mathrm{RM}_m)$, $E^1_{d/2+1}(\mathrm{RM}_m)$, $LH(\mathrm{RM}_m \setminus \{\mathbf{0}, \mathbf{1}\})$, $M^1(\mathrm{RM}_m)$

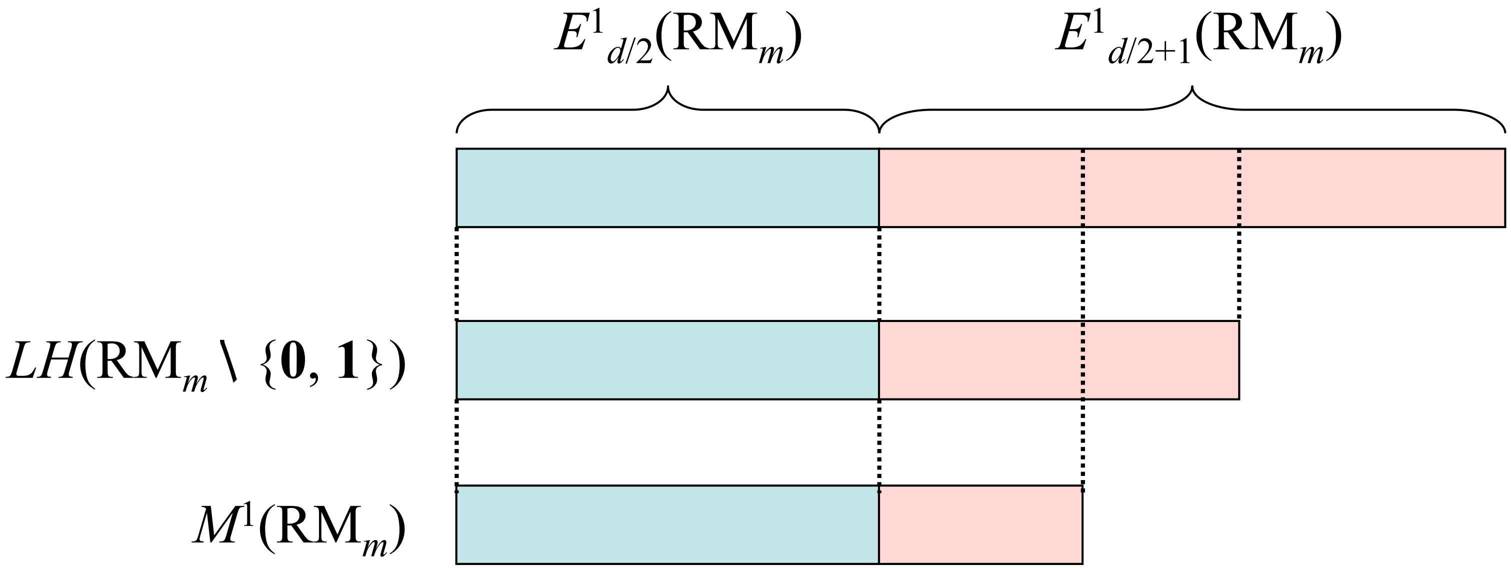


$$LH(\mathrm{RM}_m \setminus \{\mathbf{0}, \mathbf{1}\}) \subseteq E^1_{d/2}(\mathrm{RM}_m) \cup E^1_{d/2+1}(\mathrm{RM}_m)$$

Proof Sketch of Our Results

- We will determine $|E^1{}_{d/2+1}(\mathrm{RM}_m)|$

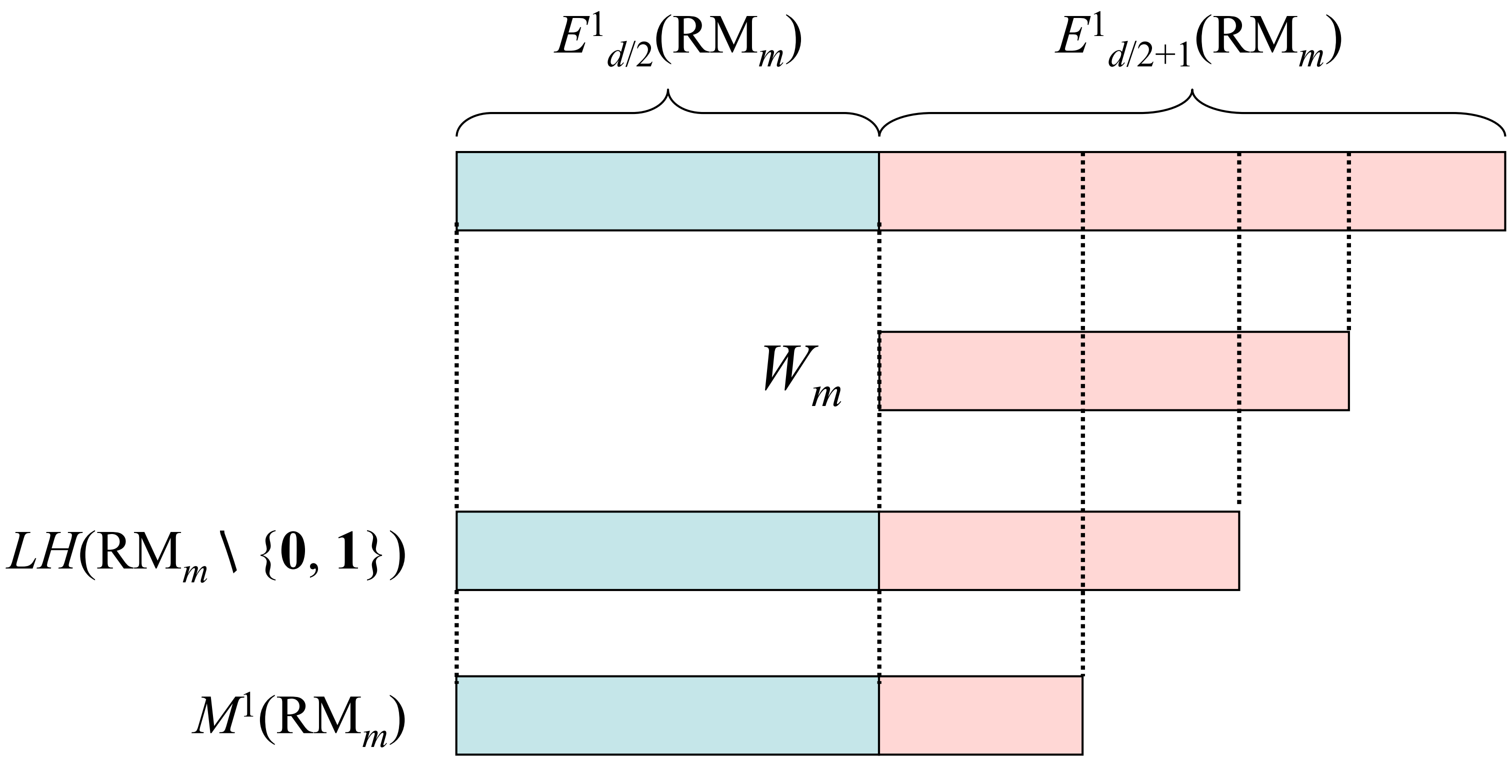
- Observe the relations between $E^1{}_{d/2}(\mathrm{RM}_m)$, $E^1{}_{d/2+1}(\mathrm{RM}_m)$, $LH(\mathrm{RM}_m \setminus \{\mathbf{0}, \mathbf{1}\})$, $M^1(\mathrm{RM}_m)$



$$M^1(\mathrm{RM}_m) \subseteq LH(\mathrm{RM}_m \setminus \{\mathbf{0}, \mathbf{1}\}) \subseteq E^1{}_{d/2}(\mathrm{RM}_m) \cup E^1{}_{d/2+1}(\mathrm{RM}_m)$$

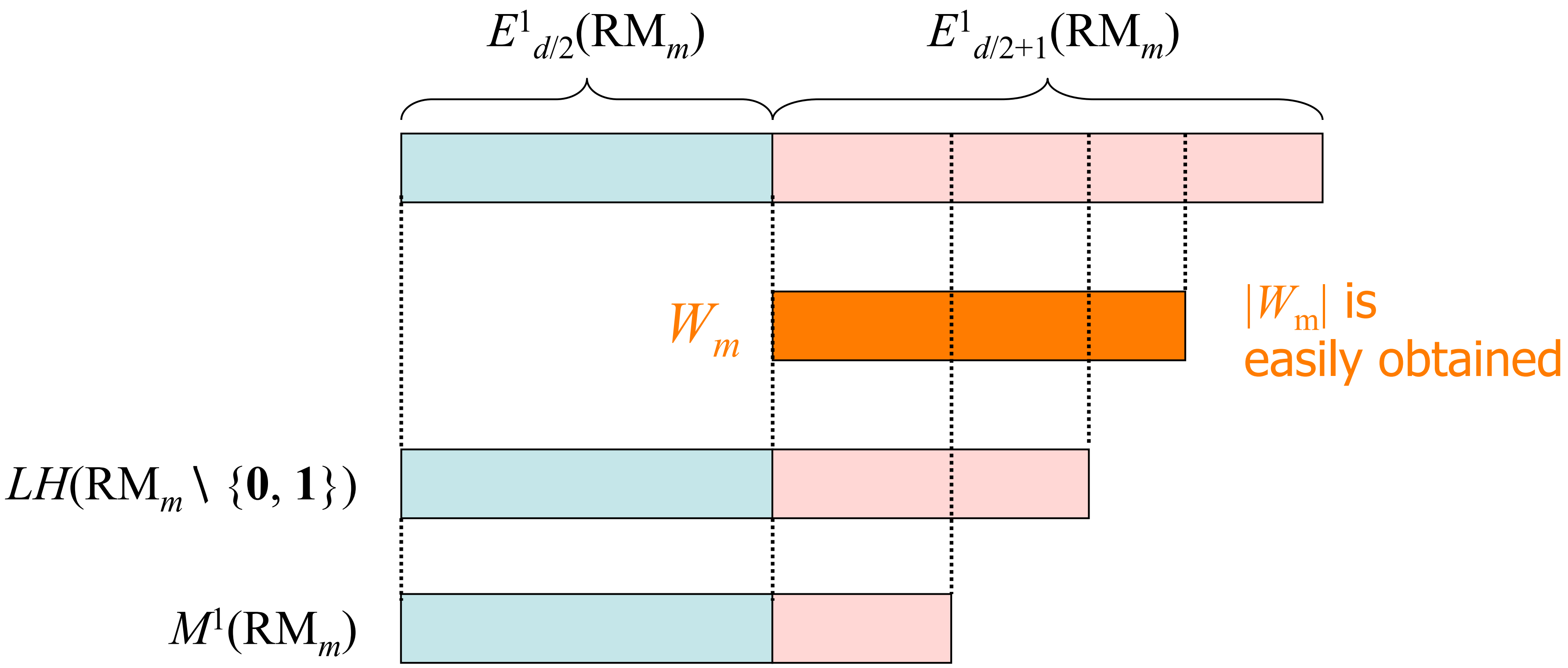
Proof Sketch of Our Results

- Consider $W_m = \{ \boldsymbol{v} : S(\boldsymbol{v}) \subseteq S(\boldsymbol{c}) \text{ for } \boldsymbol{c} \in \mathrm{RM}_m \setminus \{\mathbf{0},\mathbf{1}\}, w(\boldsymbol{v}) = d/2+1 \}$



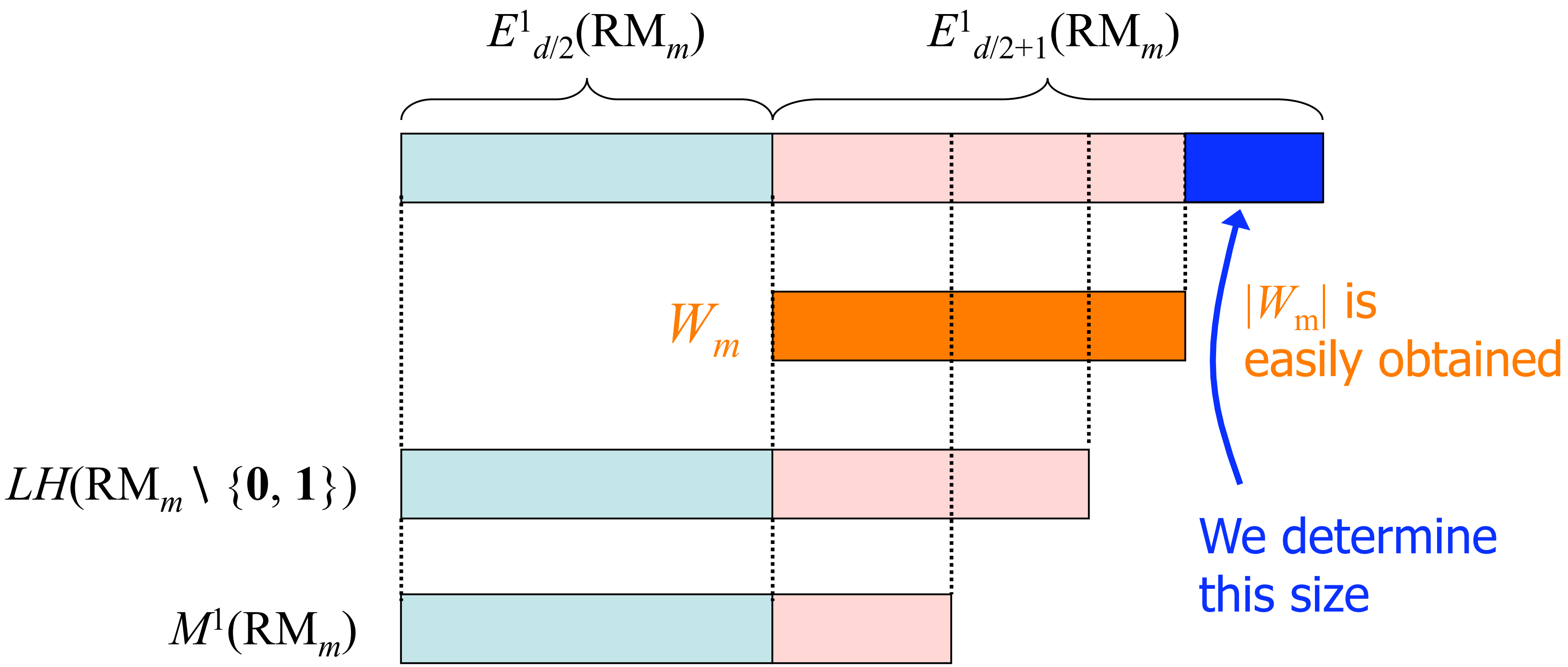
Proof Sketch of Our Results

- Consider $W_m = \{\, \boldsymbol{v} : S(\boldsymbol{v}) \subseteq S(\boldsymbol{c}) \text{ for } \boldsymbol{c} \in \mathrm{RM}_m \setminus \{\mathbf{0},\mathbf{1}\},\, w(\boldsymbol{v}) = d/2+1 \,\}$

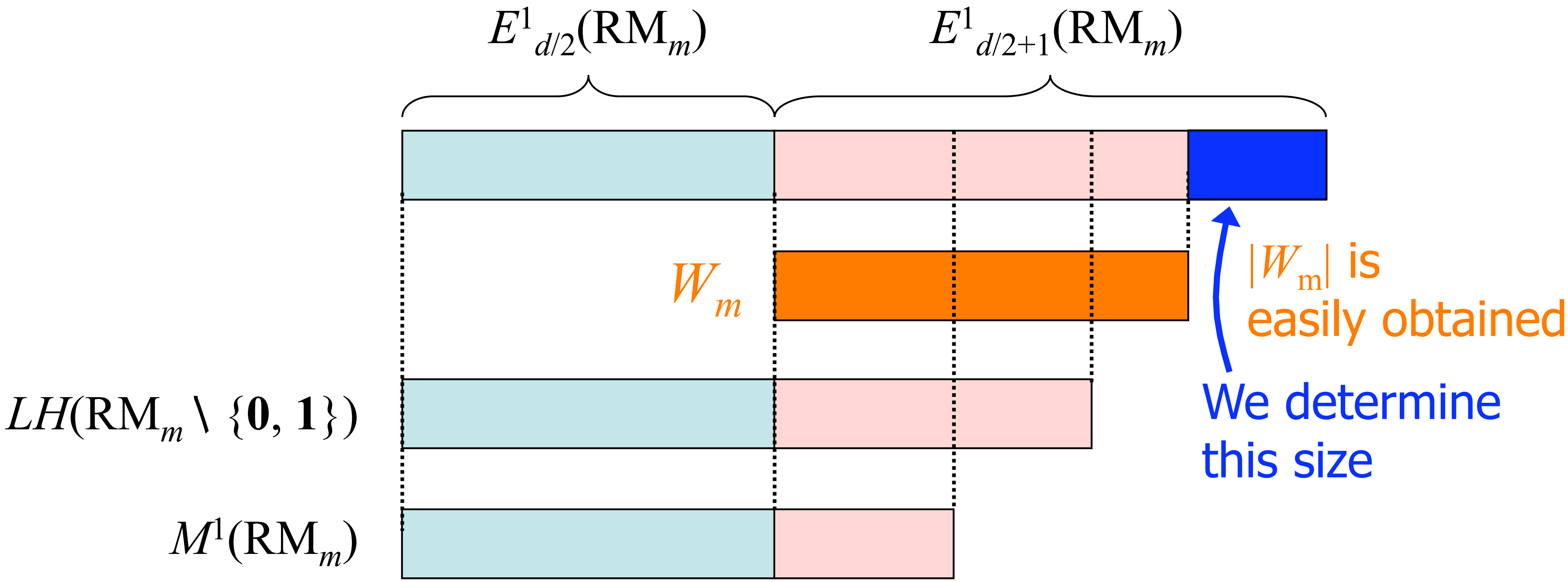


Proof Sketch of Our Results

- Consider $W_m = \{ \boldsymbol{v} : S(\boldsymbol{v}) \subseteq S(\boldsymbol{c}) \text{ for } \boldsymbol{c} \in \mathrm{RM}_m \setminus \{\mathbf{0},\mathbf{1}\}, w(\boldsymbol{v})=d/2+1 \}$



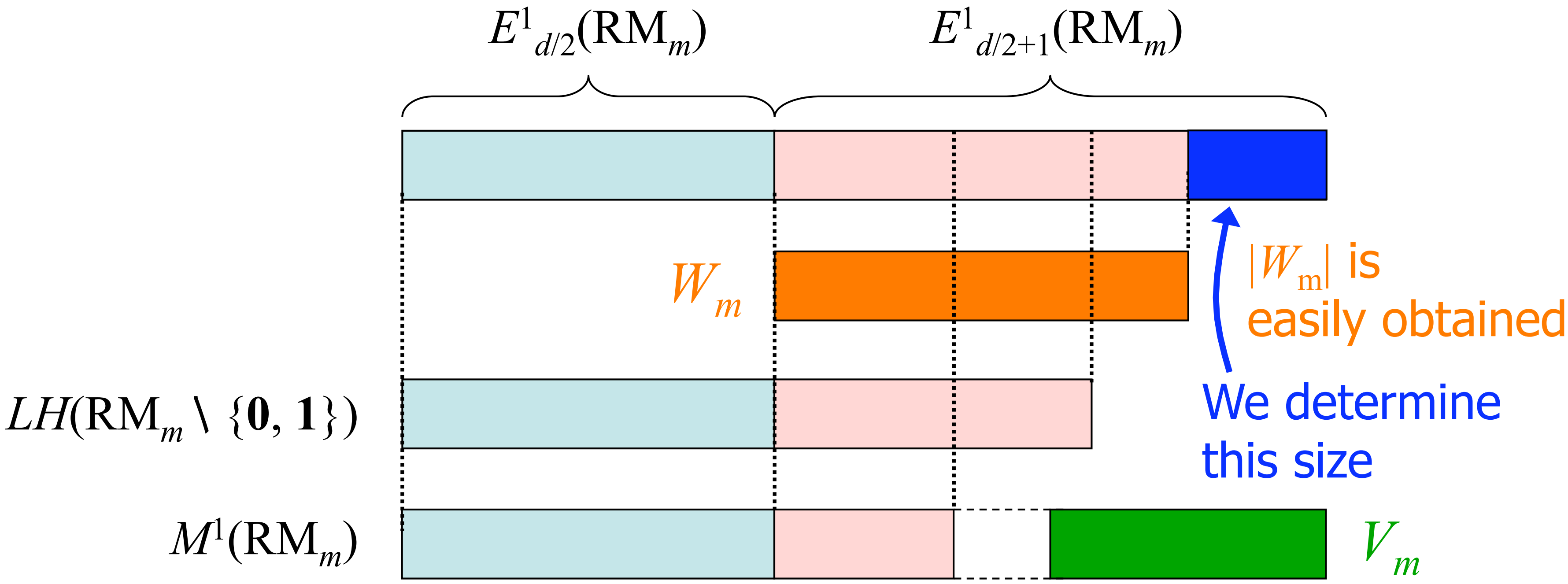
Proof Sketch of Our Results



- Observe that the vectors $\boldsymbol{v}$ in  are non-minimal

  ⇒ $\boldsymbol{v}$ is obtained by adding a weight-one vector to a minimal uncorrectable error

Proof Sketch of Our Results



- Observe that the vectors $\boldsymbol{v}$ in [blue box] are non-minimal

  ⇒ $\boldsymbol{v}$ is obtained by adding a weight-one vector to a minimal uncorrectable error

  ⇒ Construct such a set V_m [green box] and determine $|V_m \setminus W_m|$

The Results

- For $m \geq 5$,

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

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

Conclusions

- #(correctable errors of weight $d/2+1$) is derived for the first-order Reed-Muller codes
  - Monotone error stucture & larger half are main tools
  - Our approch does not reveal the structure of coset leaders of weight $d/2+1$
    - [Wu, 1998] reveals the structure of coset leaders of weight $d/2$ to derive #(correctable errors of weight $d/2$)