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

Kenji Yasunaga Toru Fujiwara
Osaka University

2007 Hawaii and SITA Joint Conference on Information Theory (HISC2007),
Hawaii, USA, May 29-31, 2007

Trial set

Trial set T for a binary linear code C

- is a subset of C that meets some property (describe later)
- introduced by [Helleseth, Kløve, Levenshtein, 2005]
- used for
  - Maximum Likelihood Decoding (MLD)
  - upper bounding #(uncorrectable errors) by MLD

- Smaller trial set is desirable

  ⇒ How large is the size of minimum trial set T_{min} ?

Main results

For binary linear codes

- Give upper/lower bounds on $|T_{min}|$

For the first-order Reed-Muller codes RM_m

- Determine $|T_{min}|$
- Determine #(minimal uncorrectable errors)

Contents

- Notations
- Background
  - Coset partitioning and Syndrome decoding
  - Monotone structure of Errors
  - Trial set, Minimal uncorrectable errors, Larger half
- Main Results
  - Upper/lower bounds on $|T_{min}|$ for linear codes
  - $|T_{min}|$ for RM_m
  - #(minimal uncorrectable errors) in RM_m

Notations

- Support set of x; $S(x) := \{ i : x_i \neq 0 \}$
- x covers y; $x \subseteq y \Leftrightarrow S(x) \subseteq S(y)$
- x is lexicographically smaller than y;

  $x \prec y \Leftrightarrow // x // < // y //$

  or $// x // = // y //$ and $v(x) < v(y)$

  - Hamming weight of x; $// x // := |S(x)|$
  - Numerical value of x; $v(x) := \Sigma x_i 2^{n-i}$
  - Example.

    $000 \prec 001 \prec 010 \prec 100 \prec 011 \prec 101 \prec 110 \prec 111$

Coset partitioning and Syndrome decoding

Coset partitioning

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

  $C_i := \{v_i + c : c \in C\}$: a coset

  $v_i \in F^n$: a coset leader

Syndrome decoding

$y \in F^n$: a received vector

- Output $y + v_i$ if $y \in C_i$
  - Coset leaders are correctable errors.
  - If v_i has minimum weight in C_i, it performs MLD.

If each coset leader is lexicographically smallest in its coset, errors have monotone structure.

Monotone structure of errors

$E^0(C)$:= the set of coset leaders (= Correctable errors)

$E^1(C)$:= $F^n \setminus E^0(C)$ (= Uncorrectable errors)

Example.

110	001
$\subseteq$	$\supseteq$
000,100,010	101,011,111
Correctable	Uncorrectable

Monotone structure of errors

- Suppose $x \in E^0(C)$, $y \in E^1(C)$.
  All $u \subseteq x$ are correctable.
  All $v \supseteq y$ are uncorrectable.
  - Monotone structure of errors is well-known.
    - e.g., Theorem 3.11 of [Peterson & Weldon, 1972]
  - However, only few research
    - Threshold behavior of error probability [Zémor, 1993]
    - Trial set and Larger half for error performance analysis [Helleseth, Kløve, Levenshtein, 2005]

Minimal uncorrectable errors and Larger half

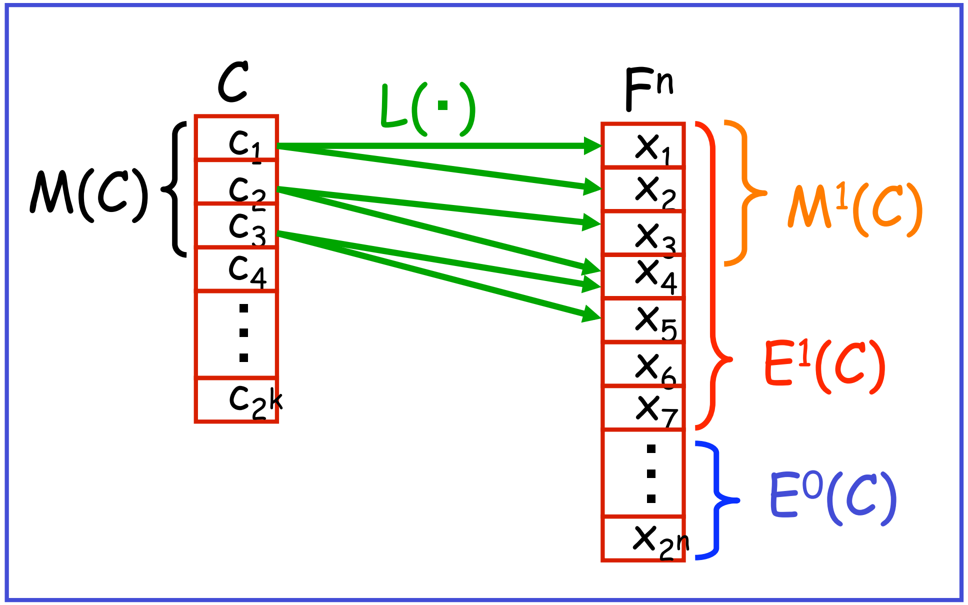
Errors have monotone structure
⇒ $E^1(C)$ is characterized by minimal vectors in $E^1(C)$

<u>Minimal uncorrectable errors</u>

- $M^1(C)$:= minimal (w.r.t covering $\subseteq$) vectors in $E^1(C)$

<u>Larger half</u> of $c \in C$

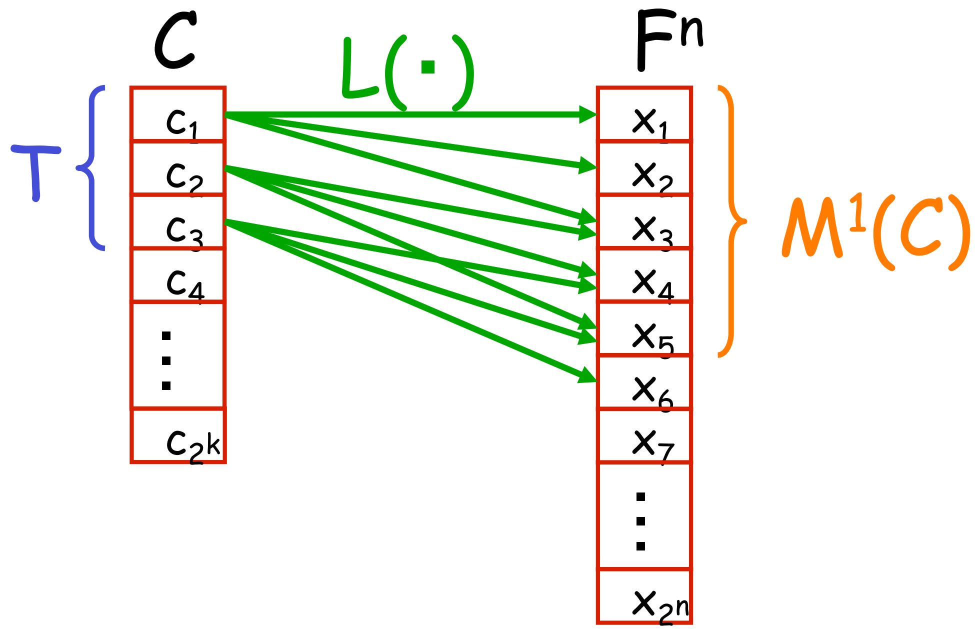
- $L(c)$:= minimal vectors in $\{ v : v+c \prec v \}$
  - $L(S) := \bigcup_{c \in S} L(c)$



- $M^1(C) \subseteq L(M(C)) \subseteq L(C)$
  - where $M(C)$:= { minimal (w.r.t. $\subseteq$) codewords in C }

Trial set

- $T \subseteq C$ is a trial set for $C \Leftrightarrow M^1(C) \subseteq L(T)$



- $C \setminus \{0\}$, $M(C)$ are examples of trial sets for C.
- Smaller trial set is desirable for its applications.
- Minimum trial set; T_{min}

$\|T_{min}\|$ is unique, though T_{min} may not be unique.

Results for linear codes

Necessary codewords for trial set

- $T_{nec} \subseteq C := \{ c : \text{for some } v \in M^1(C), v \in L(c)$ and $v \notin L(c')$ for any $c' \in C \setminus \{c\} \}$

Results

- Give 2 lower/ 2 upper bounds on $|T_{min}|$
  - For (n, k) code

$$\max \begin{Bmatrix} k \\ |T_{nec}| \end{Bmatrix} \leq |T_{min}| \leq \min \begin{Bmatrix} |C|-1 = 2^k-1, \\ |M(C)|, |M^1(C)| \\ |L(M(C)) \setminus L(C \setminus M(C))| \\ |T_{nec}| + \Sigma |D^i(C)| \end{Bmatrix}$$

$D^i(C) := \{ v \in M^1(C) \setminus L(T_{nec}) : v$ is common LH of i minimal codewords $\}$

Upper/lower bounds on $|T_{min}|$

Codes	k	$\lvert T_{nec}\rvert$	$\lvert T_{min}\rvert$	$\lvert C\rvert$-1	$\lvert M(C)\rvert$	$\lvert M^1(C)\rvert$	(1)	(2)
(15,11)BCH	11*	11 *	11~83	2047	308	105	151	83*
(15,7)BCH	7	44 *	44~87	127	108	351	2713	87*
(15,5)BCH	5	30 *	30	321	30*	945	1260	30*
(16,11)eBCH	11	16 *	16~79	2047	588	116	780	79*
(16,7)eBCH	7	45 *	45~86	127	126	434	8039	86*
(16,5)eBCH	5	30 *	30	31	30*	1260	1575	30*
(16,11)RM	11	15 *	15~79	2047	588	116	708	79*
(16,5)RM	5	30 *	30	31	30*	1260	1575	30*

(1) $|L(M(C)) \setminus L(C \setminus M(C))|$ (2) $|T_{nec}|+\Sigma|D^i(C)|$

Results for RM_m

<u>1st-order Reed-Muller codes of length 2^m</u>

- RM_m : $(2^m, m+1, 2^{m-1})$ code
  - Only three types of weights; $0, 2^{m-1}, 2^m$

Results

- Determine $|T_{min}|$
- Determine $|M^1(RM_m)|$

Proof sketch for $|T_{min}|$

Upper bound (trivial)

- $|T_{min}| \leq |M(RM_m)| = |RM_m \setminus \{\mathbf{0}, \mathbf{1}\}| = 2(2^m-1)$

Lower bound

- T_{min} is a trial set $\Rightarrow$ $M^1(RM_m) \subseteq L(T_{min})$

- Confine attention to weight 2^{m-2} vectors

  $\Rightarrow$ $E^1_{2^{m-2}}(RM_m) \subseteq L^-(T_{min})$

- $\Rightarrow$ $|E^1_{2^{m-2}}(RM_m)| \leq |L^-(T_{min})| \leq |L^-(c)| \cdot |T_{min}|$
  - $|E^1_{2^{m-2}}(RM_m)|$ is given in [Wu, 1998]
  - $|L^-(c)|$ is obtained easily

  $\Rightarrow$ $|T_{min}| \geq 2(2^m-1)$ for $m>4$

From above $|T_{min}| = 2(2^m-1)$ for $m>4$

$|T_{min}|$ for RM_m

From the proof

- For m>4 $|T_{min}| = 2(2^m-1)$

By computer search

- For m=4 $|T_{min}| = 2(2^m-1) = 30$

- For m=3 $|T_{min}| = 10$, $2(2^m-1) = 14$
- For m=2 $|T_{min}| = 3$, $2(2^m-1) = 6$

Proof sketch for $|M^1(RM_m)|$

- $M^1(RM_m) = L^-(RM_m^*) \cup (L^+(RM_m^*) \cap M^1(RM_m))$
  - where $RM_m^* = M(RM_m) = RM_m \setminus \{0, 1\}$
  - where $L^+(S) = L(S) \setminus L^-(S)$

⇩

- $|M^1(RM_m)| = |L^-(RM_m^*)| + |L^+(RM_m^*)| - |L^+(RM_m^*) \setminus M^1(RM_m)|$
  - $|L^-(RM_m^*)| = |E^1_{2m-2}(RM_m)|$ is given in [Wu, 1998]
  - $|L^+(RM_m^*)|$ is easily obtained
  - We derive $|L^+(RM_m^*) \setminus M^1(RM_m)|$ for m>3
    - By careful counting

$$|M^1(RM_m)| = 2(2^m-1)\left(\binom{2^m}{2^{m-2}} - 2^{m-3}(2^{m-1}-1)\right) \text{ for } m>3$$

Conclusions

Trial set

- used for upper bounding $E^1(C)$ and MLD

Main results

- For linear codes
  - Give upper/lower bounds on $|T_{min}|$
- For 1st-order RM codes
  - Determine $|T_{min}|$ and $|M^1(RM_m)|$

Future research

- Determine $|E^1_{2^{m-2}+1}(RM_m)|$
  - We give another proof for $|E^1_{2^{m-2}}(RM_m)|$ given in [Wu, 1998]
    - Similar argument may be applicable
  - $|E^1_{2^{m-2}+1}(RM_m)| = |M^1(RM_m)| + |\{ v+e : v \in E^1_{2^{m-2}}(RM_m),\ \| e \| = 1,\ v+e \supset v \}|$

Maximum likelihood decoding

Let $y \in F^n$: a received vector

- Output a nearest (in the Hamming distance) codeword to y
  - If several codewords are nearest, output an arbitrary one.

⇒ Syndrome decoding performs as MLD

Definition of Trial set

- A set $T \subseteq C$ is called a trial set for C if T has the following property:

$$y \in E^0(C) \quad \Leftrightarrow \quad y \prec y+c \;\; \text{for all } c \in T$$

$$(\, y \in E^1(C) \quad \Leftrightarrow \quad y+c \prec y \;\; \text{for some } c \in T \,)$$

- $C \setminus \{0\}$ is a trial set for C.
- Smaller trial set is desirable for its applications.
- Minimum trial set; T_{min}

Remark: $|T_{min}|$ is unique, though T_{min} may not be unique.

Proof sketch for $|T_{min}|$

Upper bound

- $|T_{min}| \leq |M(RM_m)| = |RM_m \setminus \{\mathbf{0}, \mathbf{1}\}| = 2(2^m-1)$

Lower bound

(1) T_{min} is a trial set $\Rightarrow$ $M^1(RM_m) \subseteq L(T_{min})$

(2) Confine attention to weight 2^{m-2} vectors

$\Rightarrow E^1_{2^{m-2}}(RM_m) \subseteq L^-(T_{min})$

From the property of $L^-(\cdot) \Rightarrow E^1_{2^{m-2}}(RM_m) \supseteq L^-(T_{min})$

$\Rightarrow E^1_{2^{m-2}}(RM_m) = L^-(T_{min})$

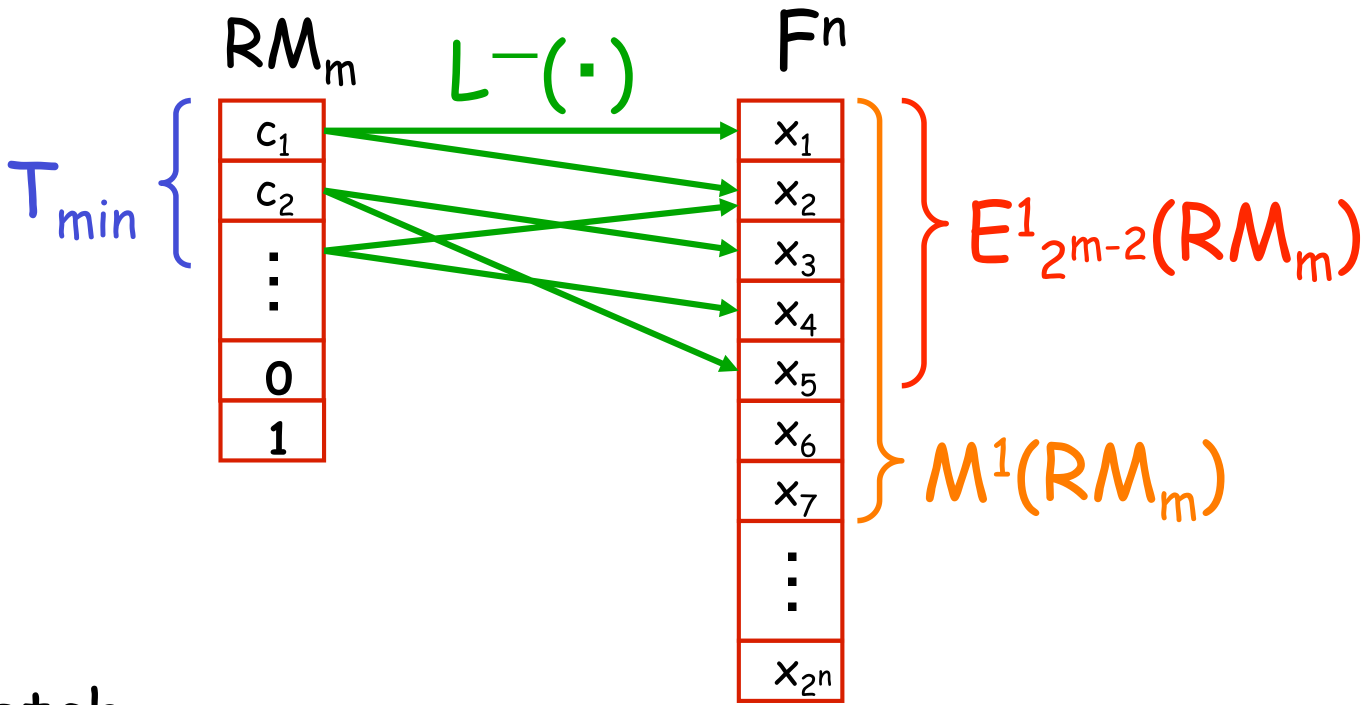
(3) $E^1_{2^{m-2}}(RM_m) = L^-(T_{min}) \Rightarrow |T_{min}| \geq 2(2^m-1)$ for $m>4$

- Describe in the next slide

From above $|T_{min}| = 2(2^m-1)$ for $m>4$

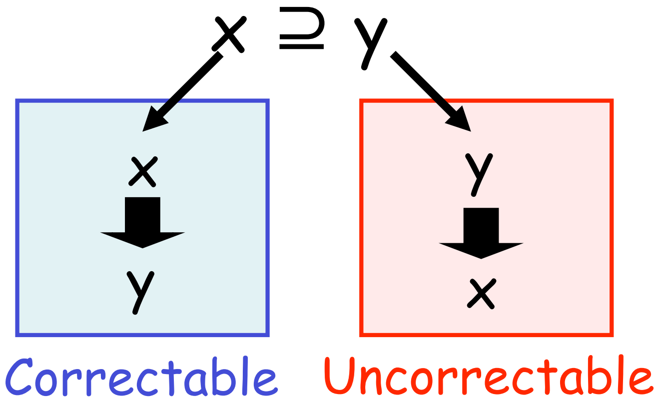
Proof sketch for $|T_{min}|$

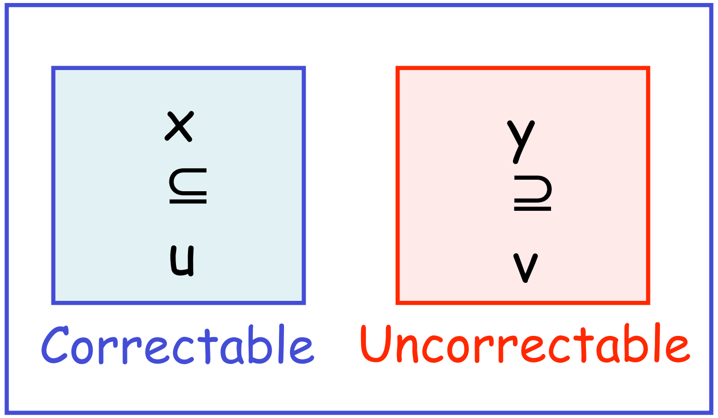
$E^1_{2m-2}(RM_m) = L^{-}(T_{min}) \Rightarrow |T_{min}| \geq 2(2^m-1)$ for $m>4$



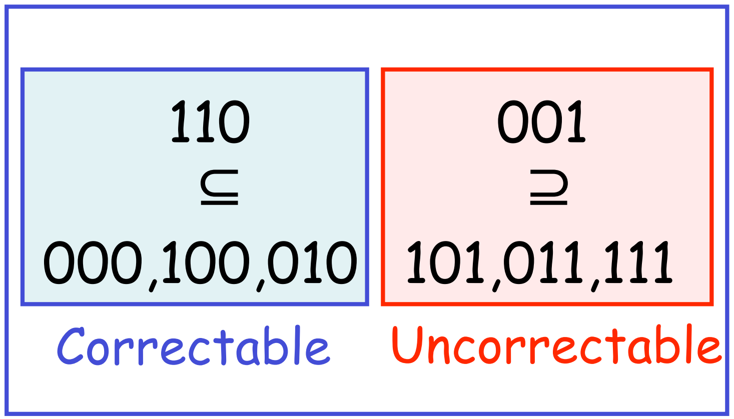
Proof sketch

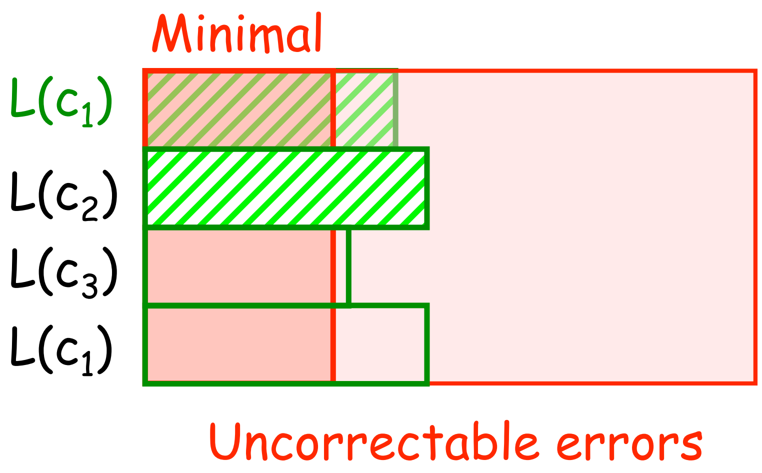
- Apply $|T_{min}| \cdot |L^{-}(c)| \geq |L^{-}(T_{min})| = |E^1_{2m-2}(RM_m)|$
  - $|L^{-}(c)|$ is easily obtained
  - $|E^1_{2m-2}(RM_m)|$ is given in [Wu, 1998]

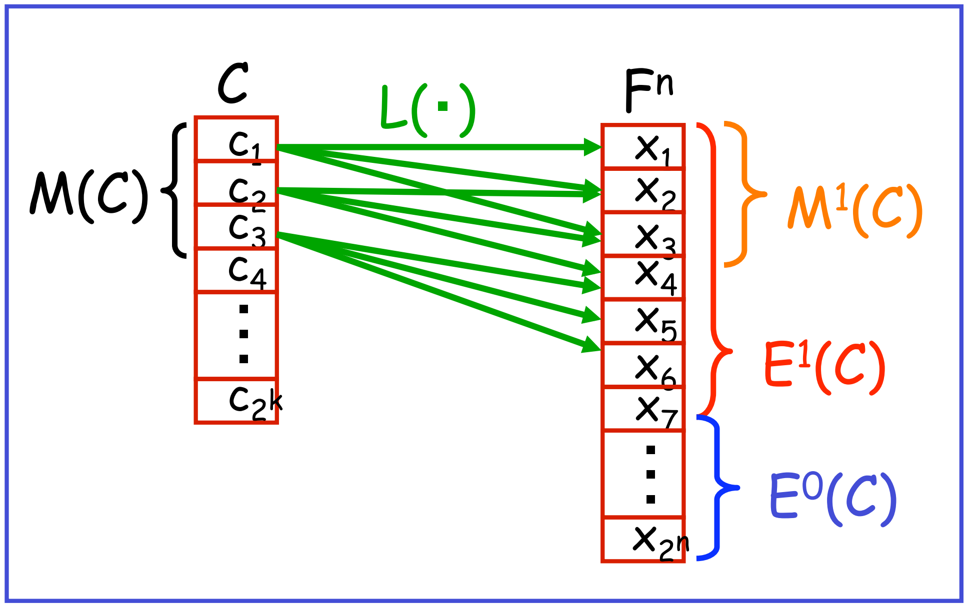




$\Rightarrow$
$\rightarrow$




Minimal
L(c1)
L(c2)
L(c3)
L(c1)
Uncorrectable errors


C
L(·)
Fn
M(C)
c1
c2
c3
c4
c2k
x1
x2
x3
x4
x5
x6
x7
x2n
M1(C)
E1(C)
E0(C)