誤り訂正符号における
誤りの単調性を利用した訂正能力分析

安永憲司

東京工業大学 大学院情報理工学研究科
数理・計算機科学専攻 GCOE特任助教

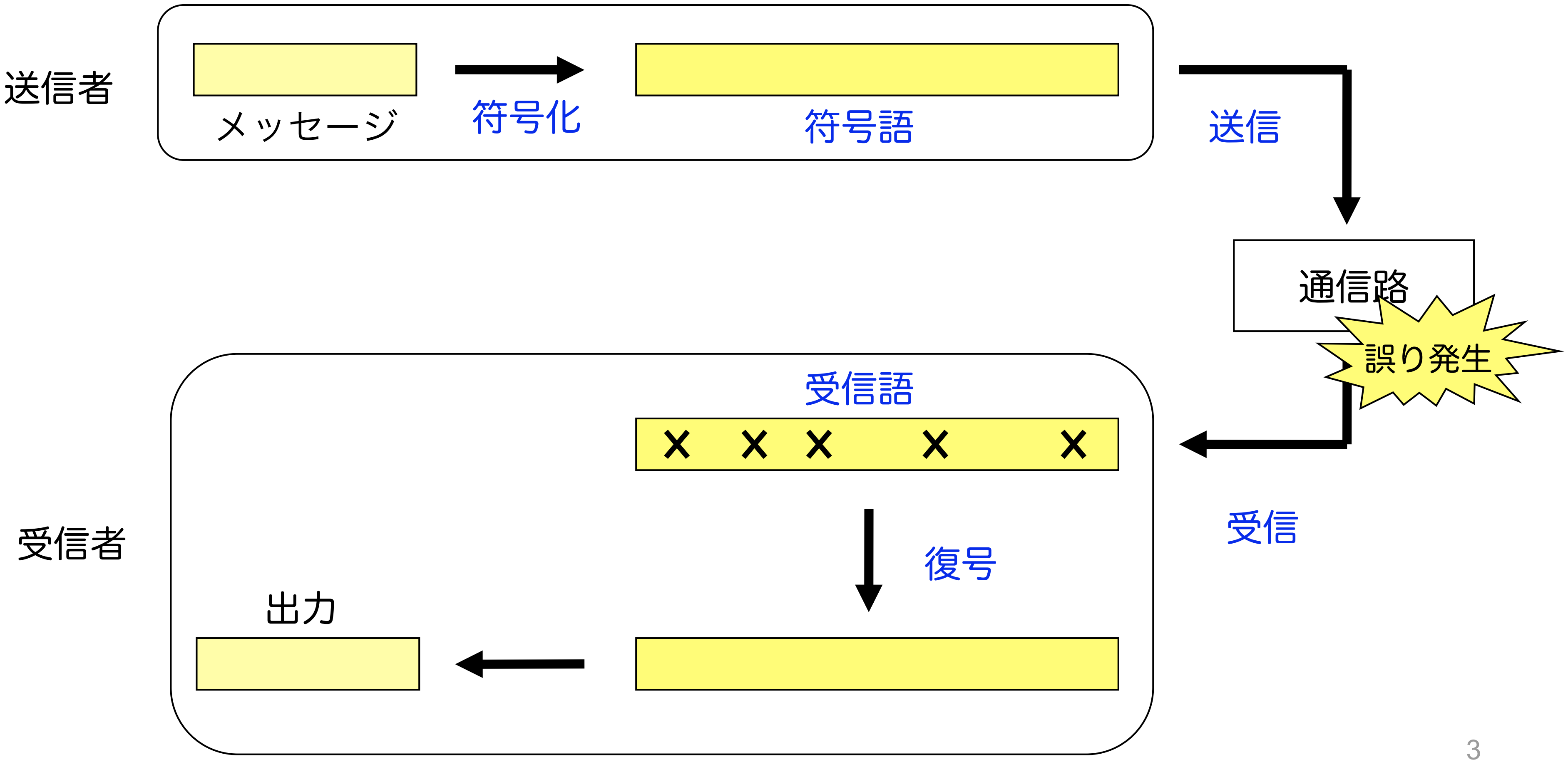
2008年10月22日

発表の流れ

- 誤り訂正符号
- 本研究で扱う問題（誤り訂正能力）
- 既存の結果・これまでの研究成果
- 扱う問題についてもう少し詳しく
- 誤りの単調性
- 研究成果の詳細
- まとめ

誤り訂正符号

- 送信メッセージに冗長性をもたせることで通信路で発生した誤りを訂正することが可能



誤り訂正符号の例

- ３回繰り返し符号
  - メッセージの各ビットを３回ずつ繰り返して送る

メッセージ		符号語
00	$\longrightarrow$	000000
01	$\longrightarrow$	000111
10	$\longrightarrow$	111000
11	$\longrightarrow$	111111

  - １ビットの誤り（０と１が反転）ならば訂正できる
    - 受信語が 010111 ならば 000111 に復号
  - ２ビット以下の誤りのとき、訂正できない場合もある
    - 受信語が 010101 ならば 000111 に復号
    - 受信語が 011111 ならば 111111 or 000111

用語の定義

- 符号：符号語の集合（線形空間をなす → 線形符号）
- (n, k) 線形符号 C ：符号長 n, メッセージ長（次元）k の線形符号
  - $C \subseteq \{0, 1\}^n$, $|C|=2^k$
- 符号の最小距離 d : 異なる符号語間の最小ハミング距離

$$d = \min_{\substack{\boldsymbol{c}_1, \boldsymbol{c}_2 \in C \\ \boldsymbol{c}_1 \neq \boldsymbol{c}_2}} d(\boldsymbol{c}_1, \boldsymbol{c}_2) = \min_{\boldsymbol{c} \in C \setminus \{0\}} w(\boldsymbol{c})$$

線形符号の場合

  - $d(\boldsymbol{x}, \boldsymbol{y})$: $\boldsymbol{x}$ と $\boldsymbol{y}$ のハミング距離
  - $w(\boldsymbol{x})$: $\boldsymbol{x}$ のハミング重み

本研究では２元線形符号を扱う

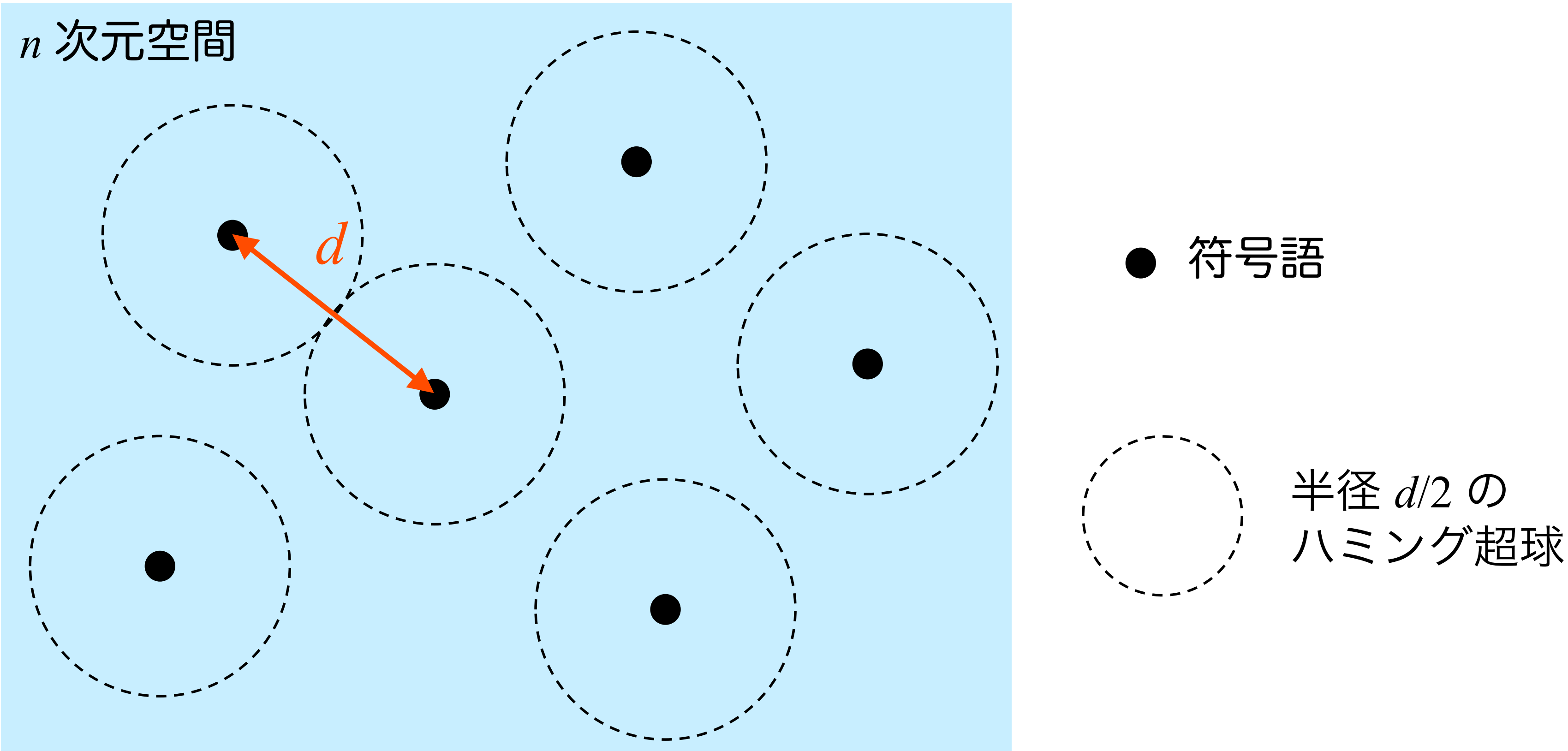
本研究で扱う問題（誤り訂正能力）

- 受信語　$\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e} \in \{0,1\}^n$
  - $\boldsymbol{c} \in C$: 送信符号語
  - $\boldsymbol{e} \in \{0,1\}^n$: 誤りベクトル
    - $w(\boldsymbol{e})$ ＝ 発生した誤りのビット数

$$
\boxed{
\begin{array}{lll}
w(\boldsymbol{e}) < d/2 & \Rightarrow & \text{必ず訂正可能} \\
w(\boldsymbol{e}) \geq d/2 & \Rightarrow & \text{？？}
\end{array}
}
$$

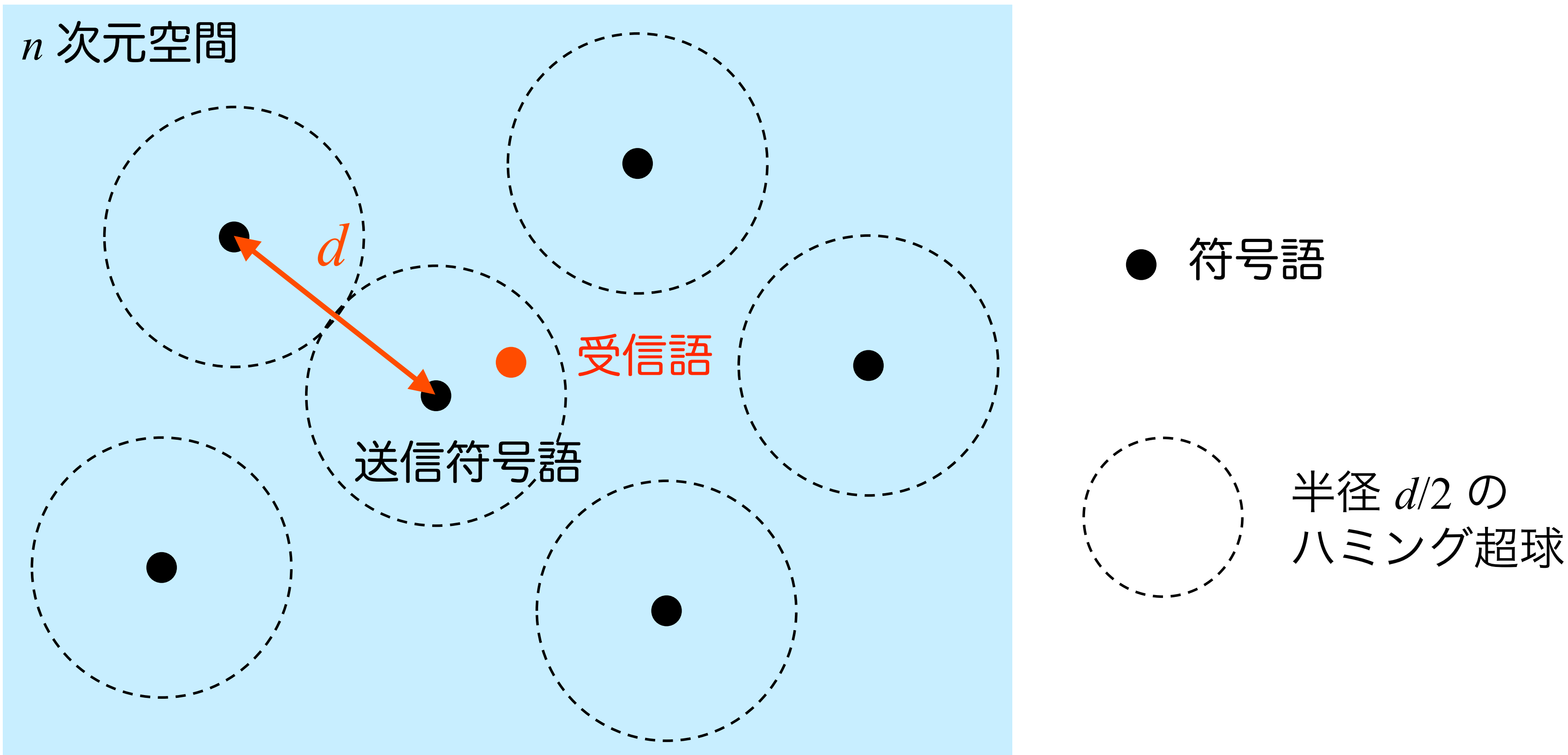
重み $d/2$ 未満の誤りが必ず訂正可能な理由

符号の最小距離 d ： すべての符号語間の最小ハミング距離



重み $d/2$ 未満の誤りが必ず訂正可能な理由

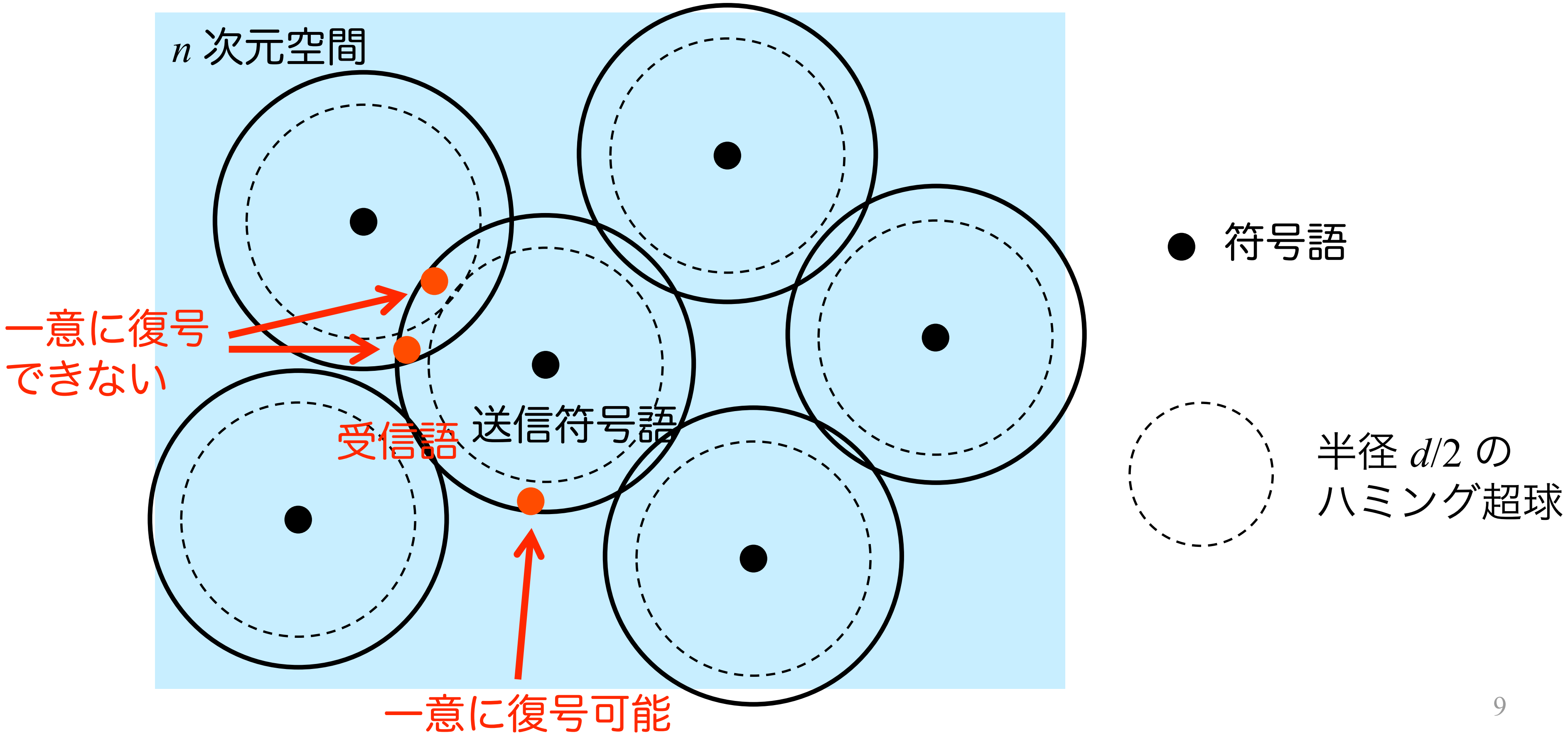
誤りの重みが $d/2$ 未満のとき、
受信語は送信符号語のハミング超球に含まれる
⇒ 一意に復号可能



重みが $d/2$ 以上の誤りが発生する場合

誤りの重みが $d/2$ より少し大きい場合（$d/2+\alpha$ 以下の場合）

半径 $d/2+\alpha$ のハミング超球が重ならない点に
受信語があれば一意に復号できる



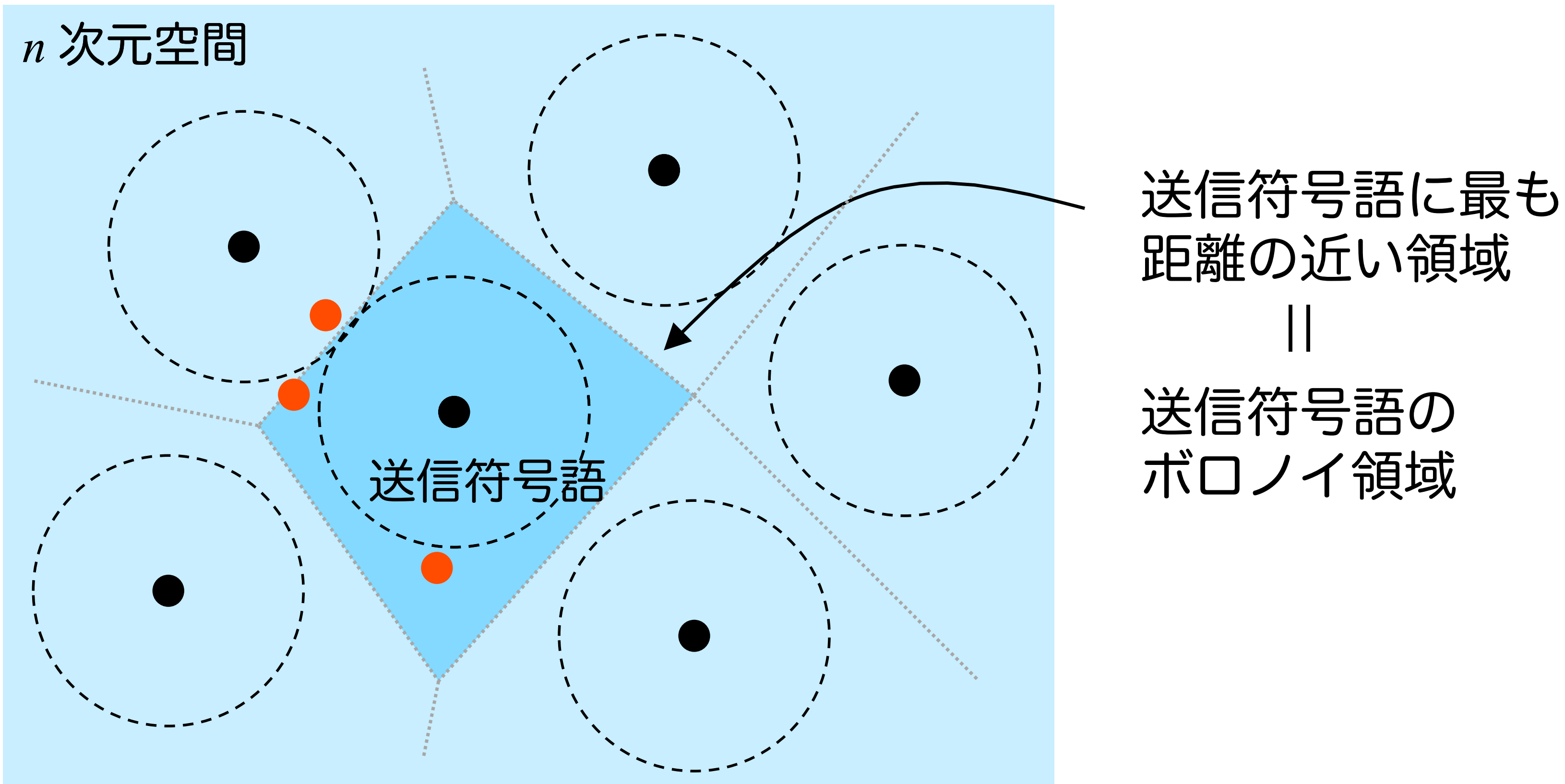
本研究で考える復号法（最小距離復号法）

- 受信語から距離が最小の符号語に復号

- ２元対称通信路で最適（＝復号誤り率を最小にする）復号法
  - ２元対称通信路
    - 各ビットごとに一定確率 $p\ (0 \leq p < 1/2)$で０と１が反転する通信路
    - 符号理論で最も研究されている通信路モデル

本研究で考える復号法（最小距離復号法）

- 受信語から距離が最小の符号語に復号
- 送信符号語に最も距離の近い領域 ＝ 訂正可能な受信語の領域



本研究で扱う問題（誤り訂正能力）

- 受信語 $\boldsymbol{y} = \boldsymbol{c} + \boldsymbol{e} \in \{0,1\}^n$
  - $\boldsymbol{c} \in C$: 送信符号語 , $\boldsymbol{e} \in \{0,1\}^n$: 誤りベクトル

最小距離復号法を行う場合

$w(\boldsymbol{e}) < d/2$	$\Rightarrow$	必ず訂正可能
$w(\boldsymbol{e}) \geq d/2$	$\Rightarrow$	受信語が送信符号語のボロノイ領域に入っていれば訂正可能

線形符号では、どの符号語のボロノイ領域も同じ形
$\rightarrow$ 訂正可能な誤りはどの送信符号語でも同じ
（$\boldsymbol{c} = \boldsymbol{0}$ を考える）

本研究では、
重み $d/2$ 以上の訂正可能な誤りベクトルの数について研究

既存の結果

- 一般の符号に対して
  - 重み i ($i \geq d/2$) の訂正不可能誤りベクトルの数の上界を導出 [Poltyrev 1994], [Helleseth, Kløve 1997], [Helleseth, Kløve, Levenshtein 2005]
- １次 Reed-Muller 符号に対して
  - $n = 32$ について、すべての重みの訂正可能誤りベクトルの数を計算 [Berlekamp, Welch 1972]
  - 重み $d/2$ の訂正可能誤りベクトルの数を導出 [Wu 1998]
- その他の符号に対して
  - ２重誤り訂正 BCH 符号 [Charpin 1994]
  - ３重誤り訂正 BCH 符号 [Charpin, Helleseth, Zinoviev 2006]
  - $n \leq 128, 29 \leq n - k \leq 42$ の Reed-Muller 符号・BCH 符号について計算 [Maeda, Fujiwara 2001]

これまでの研究成果

■ 一般の符号に対して

（成果１）重み $d/2$ の訂正不可能誤りベクトルの数の下界を導出

（成果２）重み $d/2+1$ 以上への拡張

■ １次 Reed-Muller 符号に対して

（成果３）重み $d/2$ の訂正可能誤りベクトルの数について別証明

（成果４）重み $d/2+1$ の訂正可能誤りベクトルの数を導出

いずれの結果も誤りの単調性を利用

＊上記の研究成果は大阪大学藤原融先生との共同研究であり、
まとめて論文として投稿中

以降の発表の流れ

- 扱う問題についてもう少し詳しく
  - 訂正可能・不可能な誤り
  - 扱う問題の別の見方
    - 訂正可能な誤り ＝ コセットリーダー

- 誤りの単調性
  - ベクトル間のカバー関係・極小訂正不可能誤り・Larger Half

- 研究成果の詳細
  - 結果の紹介
  - 証明概要

- まとめ

訂正可能・不可能な誤り

- 訂正可能誤り $E^0(C)$ ＝ 最小距離復号で訂正可能な誤り
  - $E_i^0(C) = \{\, \boldsymbol{v} \in E^0(C) : w(\boldsymbol{v}) = i \,\}$

- 訂正不可能誤り $E^1(C) = \{0,1\}^n \setminus E^0(C)$
  - $E_i^1(C) = \{\, \boldsymbol{v} \in E^1(C) : w(\boldsymbol{v}) = i \,\}$
  - $\left|E_i^0(C)\right| + \left|E_i^1(C)\right| = \binom{n}{i}$, $\quad |E_i^1(C)| = 0$ for $i < d/2$
  - ２元対称通信路で最適な復号をしたときの復号誤り率 P_{error}

$$P_{error} = \sum_{i=0}^{n} p^i (1-p)^{n-i} \left|E_i^1(C)\right|$$

本研究では $|E_i^1(C)|$ for $i \geq d/2$ を求めることが目標

扱う問題の別の見方

- 符号によるコセット分割
  - (n, k) 線形符号 C によって $\{0, 1\}^n$ は 2^{n-k} 個のコセットに分割

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

$$D_i = \{\boldsymbol{v}_i + \boldsymbol{c} : \boldsymbol{c} \in C\}$$: C のコセット

$$\boldsymbol{v}_i = \arg\min_{v \in C_i} w(\boldsymbol{v})$$: D_i のコセットリーダー

- シンドローム復号
  - 最小距離復号の一つ
  - $\boldsymbol{y}$ が入力されたとき, $\boldsymbol{y} \in D_i$ ならば $\boldsymbol{y} + \boldsymbol{v}_i$ を出力
  - コセットリーダー　＝　訂正可能な誤り

コセット分割の例

- (5, 2) 線形符号 $C = \{\ 00000, 11100, 00111, 11011\ \}$

$$\begin{array}{lllllll}
D_1 = \{ & 00000 & 11100 & 00111 & 11011 & \} \\
D_2 = \{ & 00001 & 11101 & 00110 & 11010 & \} \\
D_3 = \{ & 00010 & 11110 & 00101 & 11001 & \} \\
D_4 = \{ & 00100 & 11000 & 00011 & 11111 & \} \\
D_5 = \{ & 01000 & 10100 & 10111 & 10011 & \} \\
D_6 = \{ & 10000 & 01100 & 10111 & 01011 & \} \\
D_7 = \{ & 01001 & 10101 & 01110 & 10010 & \} \\
D_8 = \{ & 01010 & 10110 & 01101 & 10001 & \}
\end{array}$$

$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{\{0,\ 1\}^5}$$

コセット分割の例

- (5, 2) 線形符号 $C = \{\ 00000, 11100, 00111, 11011\ \}$

$$
\begin{array}{llllll}
D_1 = \{ & 00000 & 11100 & 00111 & 11011 & \} \\
D_2 = \{ & 00001 & 11101 & 00110 & 11010 & \} \\
D_3 = \{ & 00010 & 11110 & 00101 & 11001 & \} \\
D_4 = \{ & 00100 & 11000 & 00011 & 11111 & \} \\
D_5 = \{ & 01000 & 10100 & 10111 & 10011 & \} \\
D_6 = \{ & 10000 & 01100 & 10111 & 01011 & \} \\
D_7 = \{ & 01001 & 10101 & 01110 & 10010 & \} \\
D_8 = \{ & 01010 & 10110 & 01101 & 10001 & \}
\end{array}
$$

$E^0(C)$ $E^1(C)$

コセット分割の例

- (5, 2) 線形符号 $C = \{\ 00000, 11100, 00111, 11011\ \}$

$$
\begin{array}{l|c|ccc|l}
D_1 = \{ & 00000 & 11100 & 00111 & 11011 & \} \\
D_2 = \{ & 00001 & 11101 & 00110 & 11010 & \} \\
D_3 = \{ & 00010 & 11110 & 00101 & 11001 & \} \\
D_4 = \{ & 00100 & 11000 & 00011 & 11111 & \} \\
D_5 = \{ & 01000 & 10100 & 10111 & 10011 & \} \\
D_6 = \{ & 10000 & 01100 & 10111 & 01011 & \} \\
D_7 = \{ & \boxed{01001} & 10101 & 01110 & \boxed{10010} & \} \\
D_8 = \{ & \boxed{01010} & 10110 & 01101 & \boxed{10001} & \} \\
 & E^0(C) & & E^1(C) & &
\end{array}
$$

同じコセットに最小重みのベクトルが複数存在することもある

誤りの単調性

- 最小距離復号では訂正可能誤りに選択の余地がある
  （同じコセットに最小重みのベクトルが複数）
  （受信語の最近に複数の符号語）
  ⇒　辞書順で最小の誤りを訂正
  ⇒　誤りが単調性を持つ [Peterson, Weldon 1972]

- 誤りの単調性：

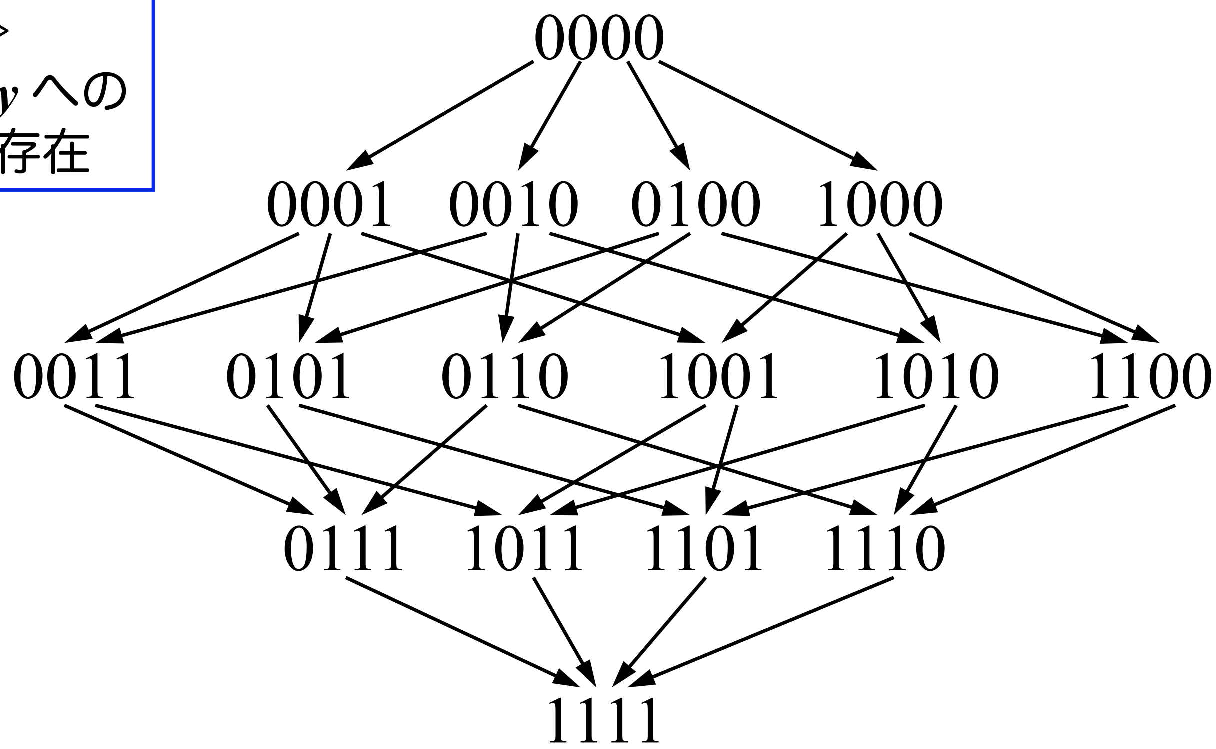
$\boldsymbol{x}$ が訂正可能	⇒	$\boldsymbol{x}$ にカバーされる誤りもすべて訂正可能
$\boldsymbol{x}$ が訂正不可能	⇒	$\boldsymbol{x}$ をカバーする誤りもすべて訂正不可能

- $\boldsymbol{x} = (x_1, \ldots, x_n)$ のサポート： $S(\boldsymbol{x}) = \{\, i : x_i \neq 0 \,\}$
- $\boldsymbol{x}$ が $\boldsymbol{y}$ にカバーされる　⇔　$S(\boldsymbol{x}) \subseteq S(\boldsymbol{y})$　⇔　$x_i \leq y_i$ for all i
  - 以降, 簡単のため $\boldsymbol{x} \subseteq \boldsymbol{y}$ と表記

誤りの単調性

x が訂正可能　⇒ $v \subseteq x$ である v もすべて訂正可能
y が訂正不可能 ⇒ $y \subseteq v$ である v もすべて訂正不可能

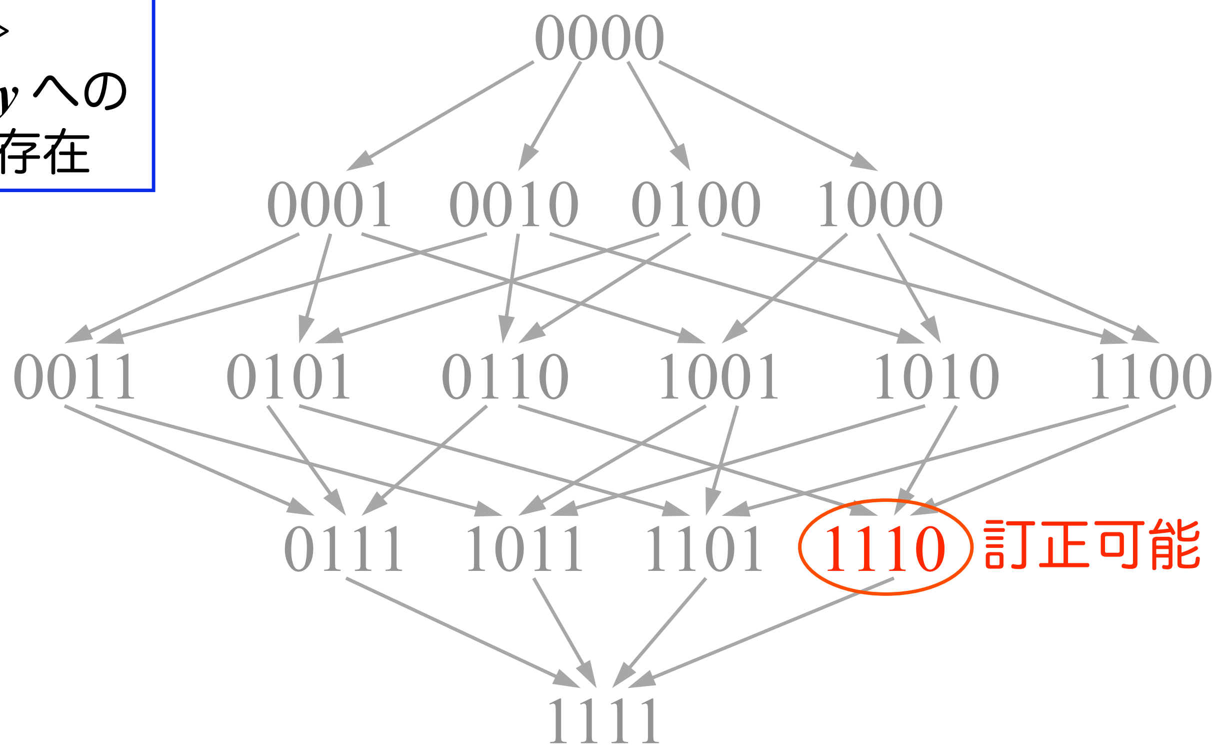
$x \subseteq y$
⇔
x から y へのパスが存在



誤りの単調性

x が訂正可能　⇒ $v \subseteq x$ である v もすべて訂正可能
y が訂正不可能 ⇒ $y \subseteq v$ である v もすべて訂正不可能

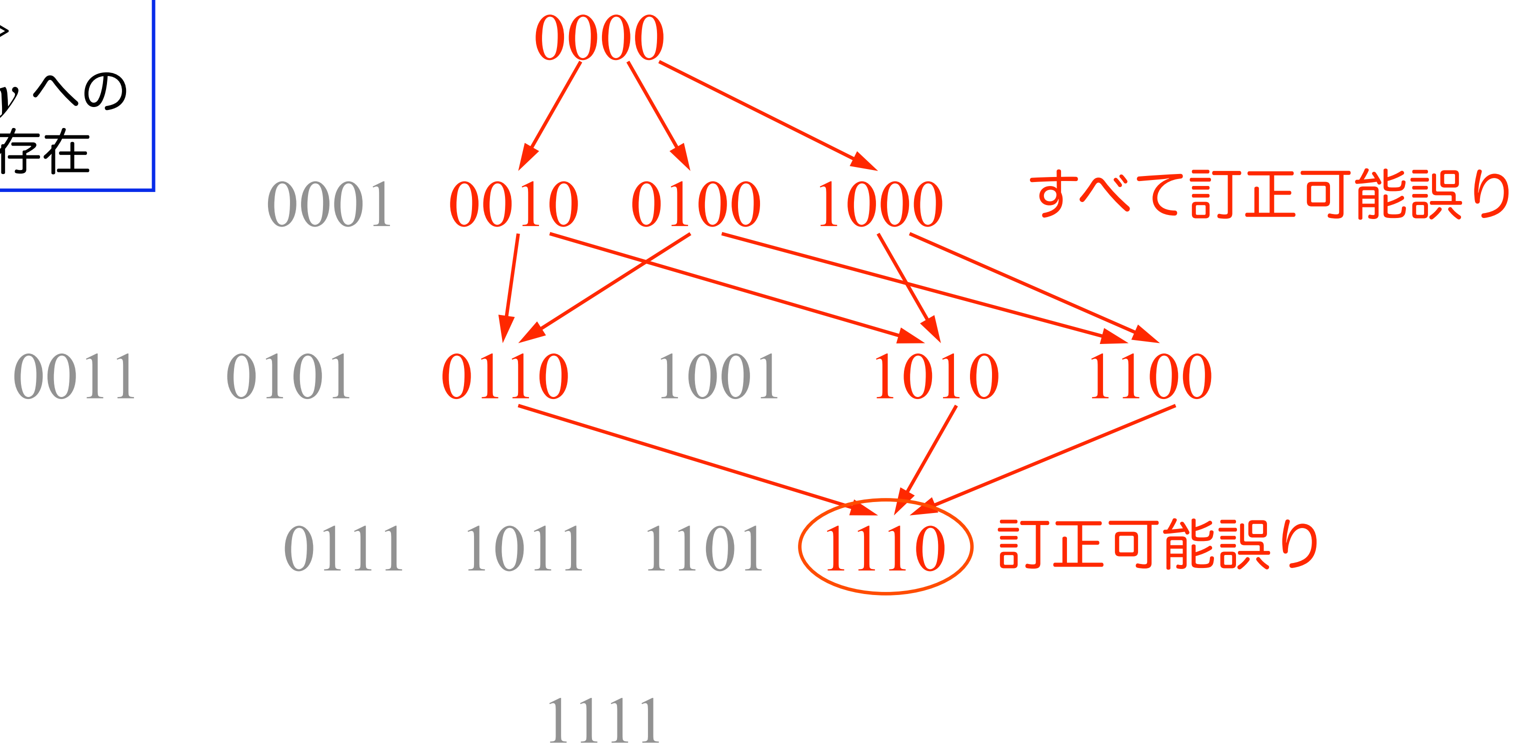
$x \subseteq y$
⇔
x から y へのパスが存在



誤りの単調性

x が訂正可能　⇒ $v \subseteq x$ である v もすべて訂正可能
y が訂正不可能 ⇒ $y \subseteq v$ である v もすべて訂正不可能

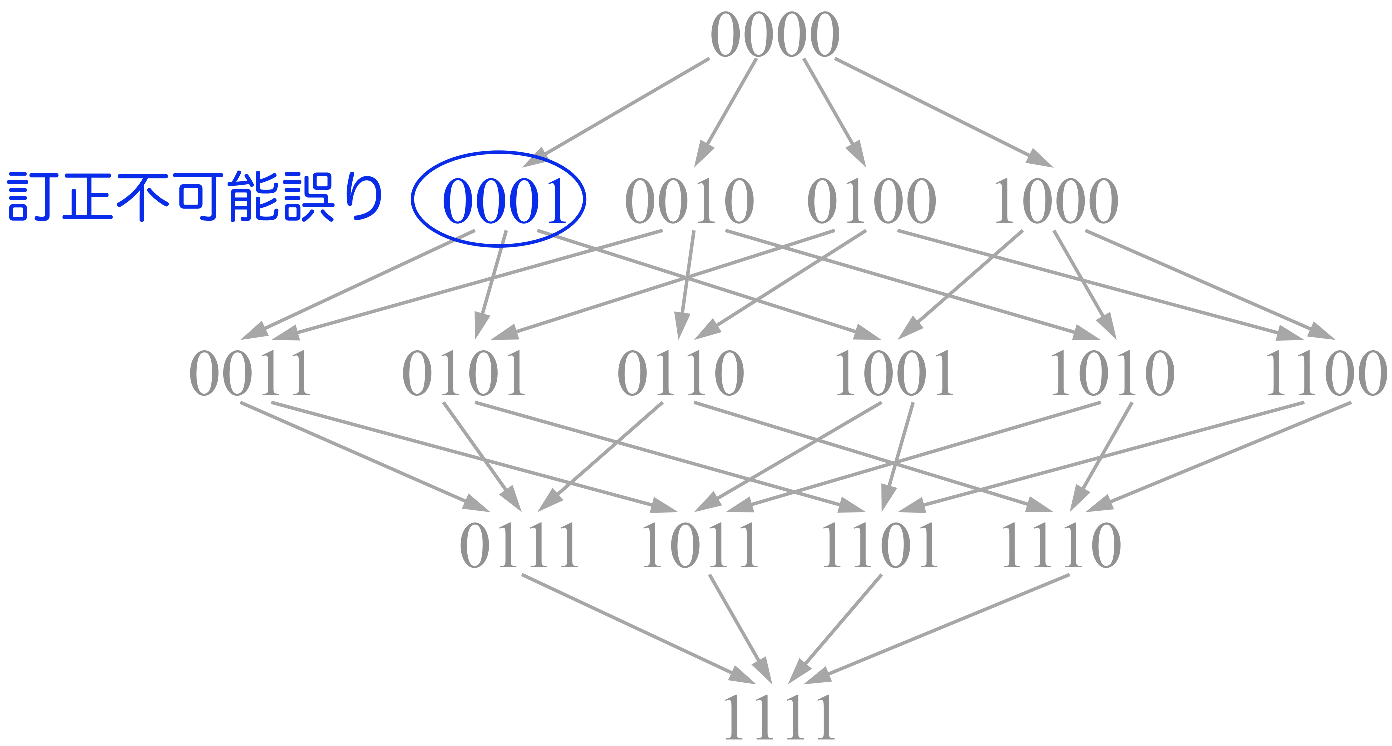
$x \subseteq y$
$\Leftrightarrow$
x から y への
パスが存在



誤りの単調性

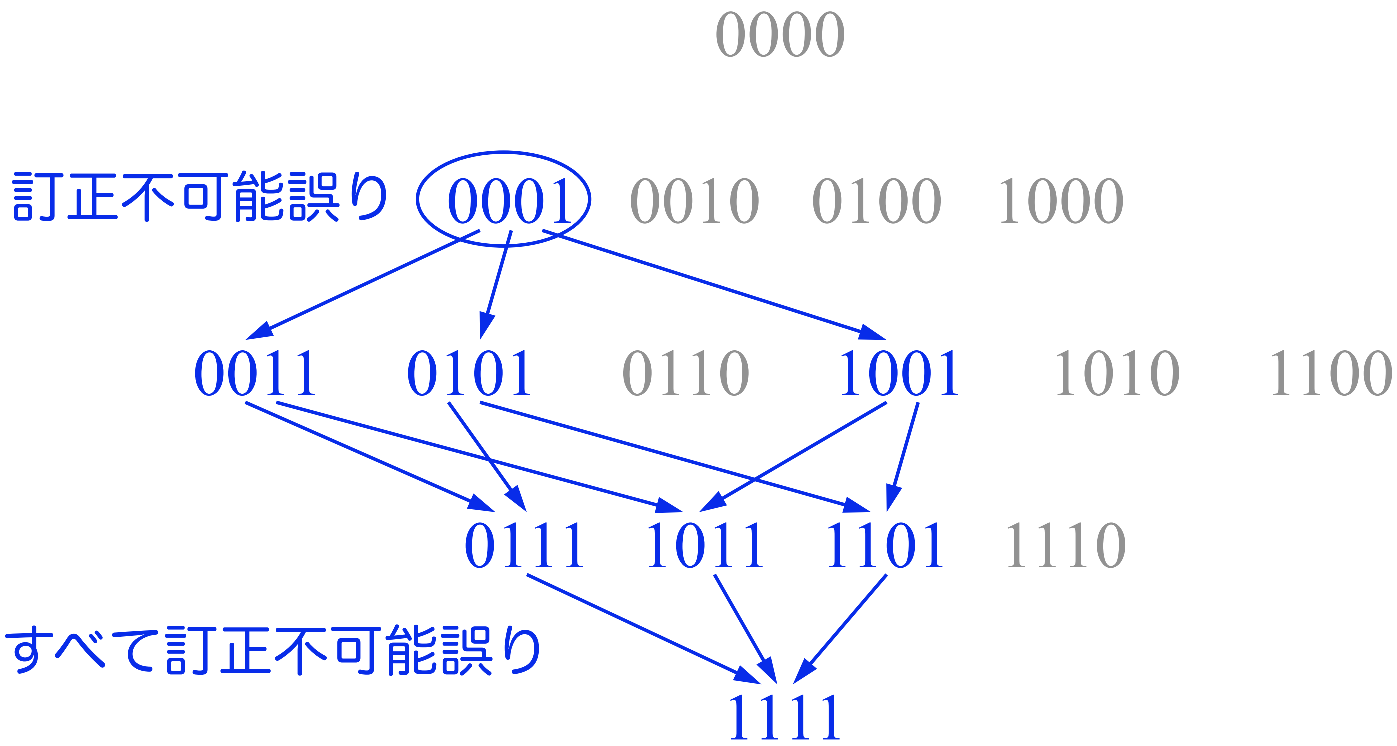
x が訂正可能　⇒ $v \subseteq x$ である v もすべて訂正可能

y が訂正不可能 ⇒ $y \subseteq v$ である v もすべて訂正不可能



誤りの単調性

x が訂正可能　$\Rightarrow$ $v \subseteq x$ である v もすべて訂正可能
y が訂正不可能 $\Rightarrow$ $y \subseteq v$ である v もすべて訂正不可能



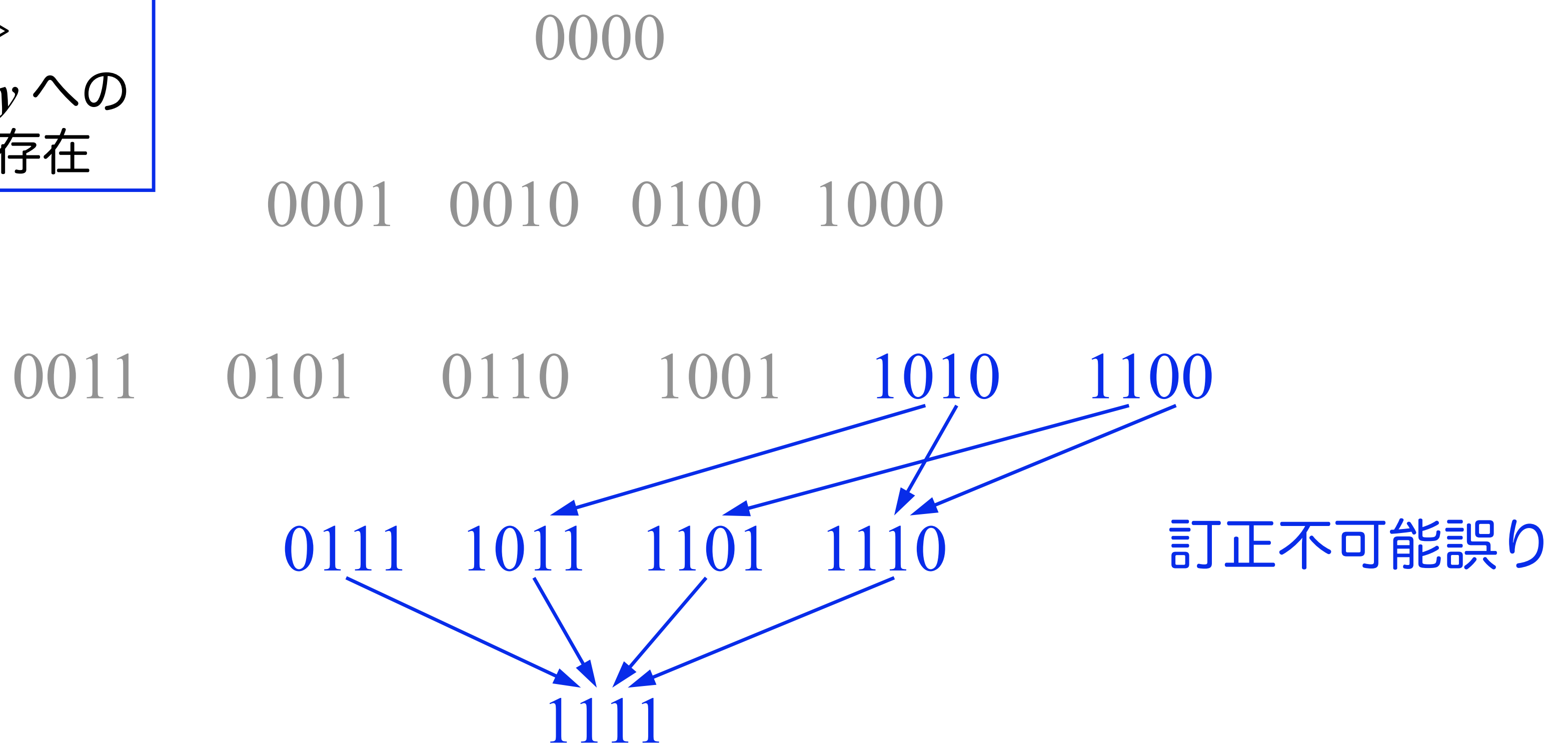
単調性があるとき

- 訂正不可能誤りは $M^1(C)$ によって特徴付けられる
  - $M^1(C)$: カバー(⊆)に関して極小な訂正不可能誤り
  - $M^1(C)$ が決まれば訂正不可能誤りは一意に決まる

$x \subseteq y$

⇔

x から y への
パスが存在



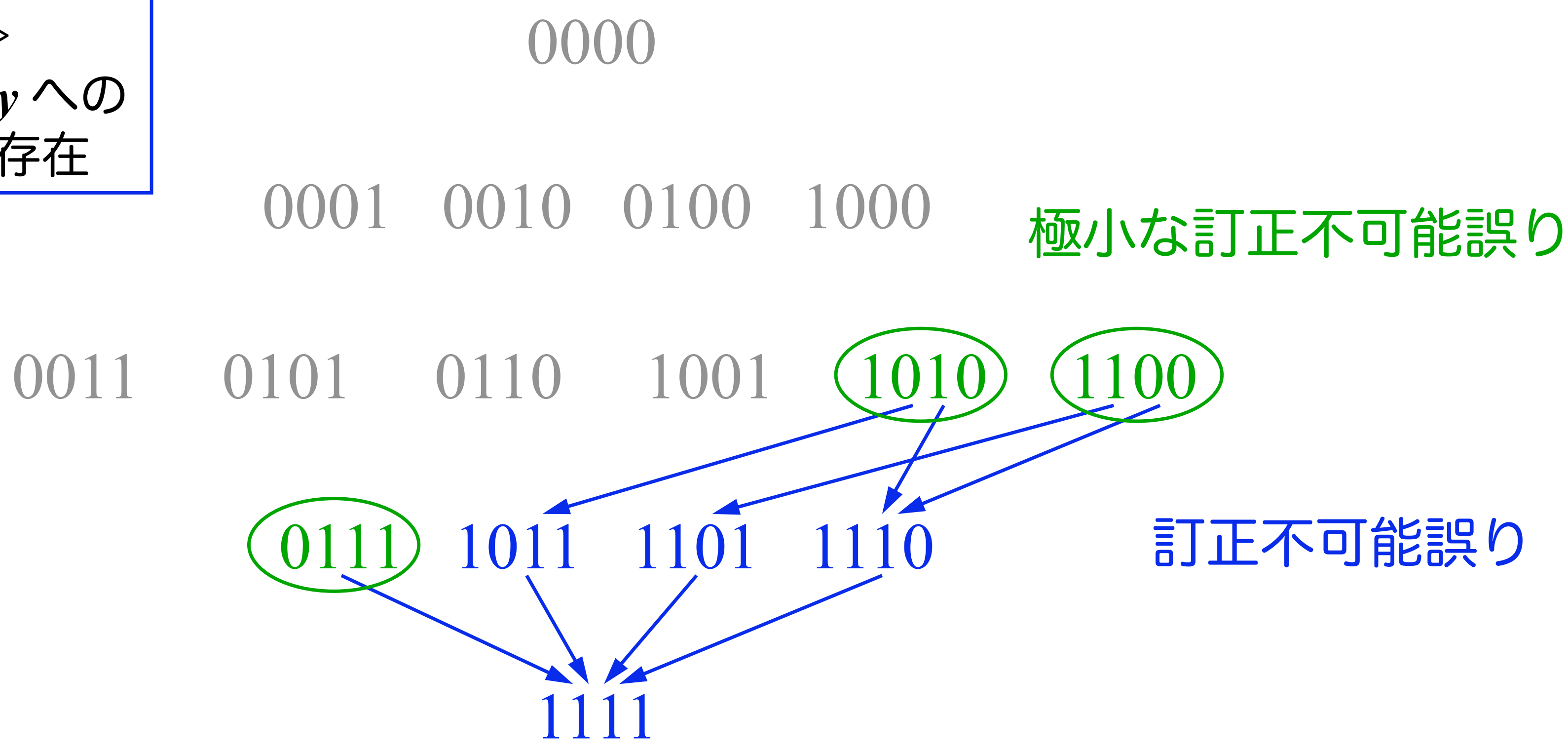
単調性があるとき

- 訂正不可能誤りは $M^1(C)$ によって特徴付けられる
  - $M^1(C)$: カバー(⊆)に関して極小な訂正不可能誤り
  - $M^1(C)$ が決まれば訂正不可能誤りは一意に決まる

$x \subseteq y$

⇔

x から y への
パスが存在



Larger Half

- 符号語 $\boldsymbol{c}$ の Larger Half; $LH(\boldsymbol{c})$
  - $M^1(C)$ を特徴付けるために導入[Helleseth et al. 2005]

  - LH の直感的定義
    $LH(\boldsymbol{c}) = \{\, \boldsymbol{v} \in \{0,1\}^n$: $\boldsymbol{c}$ によって訂正不可能誤りだとわかるベクトルの中でカバーに関して極小なもの$\}$

  - 重要な性質
    $\boxed{M^1(C) \subseteq LH(C \setminus \{\mathbf{0}\}) \subseteq E^1(C)}$ ここで $LH(U) = \bigcup_{\boldsymbol{c} \in U} LH(\boldsymbol{c})$

  - LH の組み合わせ的構成法

$$\boldsymbol{v} \in LH(\boldsymbol{c}) \Longleftrightarrow \begin{array}{l} (1)\ \boldsymbol{v} \subseteq \boldsymbol{c} \\ (2)\ w(\boldsymbol{c}) \le 2w(\boldsymbol{v}) \le w(\boldsymbol{c}) + 2 \\ (3) \begin{cases} l(\boldsymbol{v}) = l(\boldsymbol{c}) & \text{if } 2w(\boldsymbol{v}) = w(\boldsymbol{c}) \\ l(\boldsymbol{v}) > l(\boldsymbol{c}) & \text{if } 2w(\boldsymbol{v}) = w(\boldsymbol{c}) + 2 \end{cases} \end{array}$$

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

これまでの研究成果

- 一般の符号に対して

（成果１）重み $d/2$ の訂正不可能誤りベクトルの数の下界を導出
（成果２）重み $d/2+1$ 以上への拡張

- １次 Reed-Muller 符号に対して

（成果３）重み $d/2$ の訂正可能誤りベクトルの数について別証明
（成果４）重み $d/2+1$ の訂正可能誤りベクトルの数を導出

成果１・２・４について以降で紹介

（成果１）： 結果（d が偶数の場合）

d が偶数であり $\frac{1}{2}\binom{d}{d/2} > \left\lceil \frac{|C_d|-1}{2} \right\rceil$ であるとき

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

$C_w = \{$ C で重み w の符号語 $\}$

上界は [Helleseth et al .2005] から

- $n \to \infty$ で $|C_d| \Big/ \binom{d}{d/2} \to 0$ なら上界・下界が漸近的に一致
  - Reed-Muller 符号やランダム線形符号では漸近的に一致

（成果１）： 結果（d が奇数の場合）

d が奇数であり $\frac{1}{2}\binom{d}{(d+1)/2} > \left\lceil \frac{|C_d|}{2} \right\rceil + \left\lceil \frac{|C_{d+1}|-1}{2} \right\rceil$ であるとき

$$\frac{1}{2}\binom{d}{(d+1)/2}\left(|C_d| + |C_{d+1}|\right) - \left(\left\lceil \frac{|C_d|}{2} \right\rceil + \left\lceil \frac{|C_{d+1}|-1}{2} \right\rceil\right)|C_{d+1}|$$

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

$C_w = \{\, C$ で重み w の符号語 $\}$

上界は [Helleseth et al .2005] から

- $n \to \infty$ で $|C_{d+1}| \Big/ \binom{d}{(d+1)/2} \to 0$ なら上界・下界が漸近的に一致
  - ランダム線形符号では漸近的に一致

（成果１）：証明概要

- $\left|E^1_{\lceil d/2 \rceil}(C)\right|$ を求めたい

- 次の関係が成立

$$M^1_{\lceil d/2 \rceil}(C) = LH_{\lceil d/2 \rceil}(C \setminus \{\mathbf{0}\}) = E^1_{\lceil d/2 \rceil}(C)$$

［証明］

- $M^1(C) \subseteq LH(C \setminus \{\mathbf{0}\}) \subseteq E^1(C)$
- 重み $\lceil d/2 \rceil$ は $E^1(C)$ の中で最小の重みであり、その重みをもつ誤りはその他の訂正不可能誤りにカバーされない

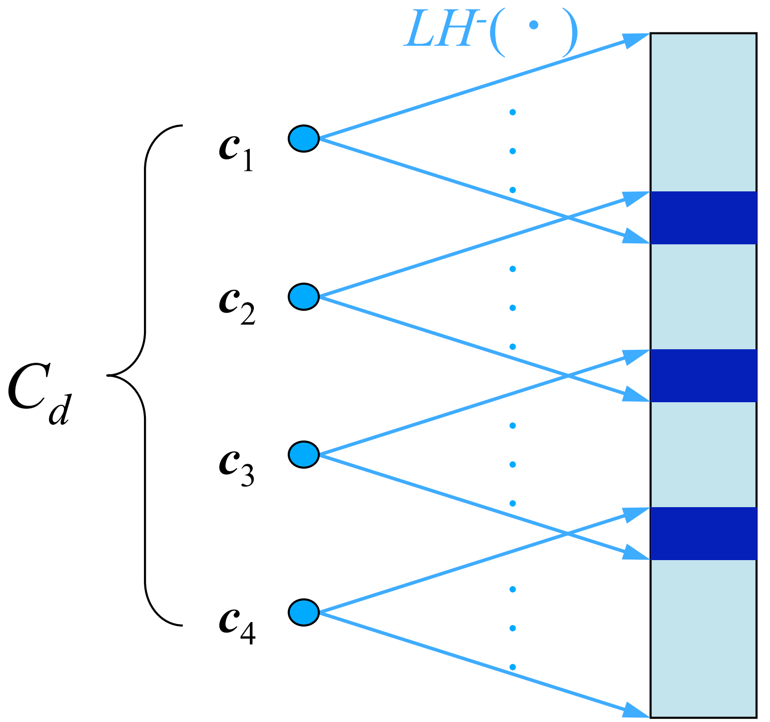
$\Rightarrow \quad M^1_{\lceil d/2 \rceil}(C) = E^1_{\lceil d/2 \rceil}(C)$

- $\left|LH_{\lceil d/2 \rceil}(C \setminus \{\mathbf{0}\})\right|$ の下界を考えることで $\left|E^1_{\lceil d/2 \rceil}(C)\right|$ の下界を導出

（成果１）： 証明概要（d が偶数の場合）

- $\left|LH_{d/2}(C\setminus\{\mathbf{0}\})\right|$ の下界を求める

$$LH_{d/2}(C\setminus\{0\}) = LH^{-}(C_d)$$



$|LH^{-}(\boldsymbol{c}_i)| = \frac{1}{2}\binom{d}{d/2}$

$(|C_d|-1)/2$ 以下

各 $\boldsymbol{c}_i \in C_d$ について
重複は $(|C_d|-1)/2$ 個以下

したがって

$$(|LH(\boldsymbol{c}_i)| - (|C_d|-1)/2)\,|C_d| \le |LH_{d/2}(C\setminus\{\mathbf{0}\})|$$

Reed-Muller 符号への適用

- 符号長 2^m の r 次 Reed-Muller 符号
  - $d = 2^{m-r}$
  - $|C_d| \le (2^{m+1} - 2)^r$

- 条件 $\frac{1}{2}\binom{d}{d/2} > \left\lceil \frac{|C_d| - 1}{2} \right\rceil$ は r 固定・ $m \to \infty$ で満たされる

条件を満たす r, m

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

- また、$m \to \infty$ のとき

$$|C_d| \Big/ \binom{d}{d/2} \le \frac{(2^{m+1} - 2)^r}{2^{2^{m-r}}} \le 2^{(m+1)r - 2^{m-r}} \to 0$$

なので上界・下界は漸近的に一致

ランダム線形符号への適用

- 生成行列（nk ビット）を確率 2^{-nk} でとってくるランダム線形符号（のアンサンブル）
  - レート $R = k/n$ をあらかじめ決める
  - $n \to \infty$ としたときの平均を考える

- d は Gilbert-Varshamov bound 上にある

$$d \approx \delta_{\mathrm{GV}} n \qquad \text{ここで} \quad 1 - H(\delta_{\mathrm{GV}}) = R$$

$$H(x) = -x \log x - (1-x) \log x$$

- 重み分布は２項分布にしたがう

$$|C_d| \approx (2^k - 1)\binom{n}{d} 2^{-n} \approx 2^{n(H(\delta)-1+R)} \approx 1, \quad |C_{d+1}| \approx |C_d|$$

ランダム線形符号への適用

- 条件は
  d が偶数のとき $\frac{1}{2}\binom{d}{d/2} > \left\lceil \frac{|C_d|-1}{2} \right\rceil \approx 0$

  d が奇数のとき $\frac{1}{2}\binom{d}{(d+1)/2} > \left\lceil \frac{|C_d|}{2} \right\rceil + \left\lceil \frac{|C_{d+1}|-1}{2} \right\rceil \approx 1$

  であり、$d \approx \delta_{\mathrm{GV}} n$ なので満たされる

- $n \to \infty$で

  $$|C_d| \Big/ \binom{d}{d/2} \to 0, \quad |C_{d+1}| \Big/ \binom{d}{(d+1)/2} \to 0$$

  なので上界・下界は漸近的に一致

（成果２）：結果

成果１と同様の議論から

$\lceil d/2 \rceil \le i \le \lceil n/2 \rceil$ である i に対して、$\binom{2i-3}{i} > \binom{2i-\lceil d/2 \rceil}{i} B_i$ であるとき

$$\binom{2i-3}{i} B_i - \binom{2i-\lceil d/2 \rceil}{i} \left(B_i^2 - \hat{B}_i\right) \le |LH_i(C)| \le \binom{2i-1}{i} B_i$$

ここで $B_i = |C_{2i-2}| + |C_{2i-1}| + |C_{2i}|,\ \hat{B}_i = |C_{2i-2}||C_{2i-1}| + |C_{2i-1}||C_{2i}| + |C_{2i}||C_{2i-2}|$

- $|LH_i(C)| \le |E_i^1(C)|$ であるため下界を与えている

大きな i に対して

- 下界のための条件が厳しい
- 弱い下界である
  - あくまで $|LH_i(C)|$ に対する下界であり、i が大きいと $|LH_i(C)|$ と $|E_i^1(C)|$ の差が広がる

1次 Reed-Muller 符号 RM_m

- $(2^m, m+1)$ 符号で最小距離 $d = 2^{m-1} = n/2$
  - 次元 $k = m+1$ は小さいが、最小距離が $n/2$ と非常に大きい
  - non-trivial な符号の中では構造が非常にシンプル
    - ある論文では、RM_m は符号理論で最も研究されてきた符号と紹介

- 各符号語は m 変数の線形ブール関数と一対一に対応
  - r 次 Reed-Muller 符号の符号語は r 次ブール関数に対応

- RM_m の重み i の訂正可能誤りの数
  ⇔ 非線形性が i のブール関数の数
  - 関数 f の非線形性 : f が線形関数からどのくらい離れているか
    - 関数の非線形性は、暗号システム（対称鍵暗号、ストリーム暗号）の安全性指標として重要

（成果４）：結果

$m \geq 5$ の１次 Reed-Muller 符号 $(n = 2^m)$ に対し

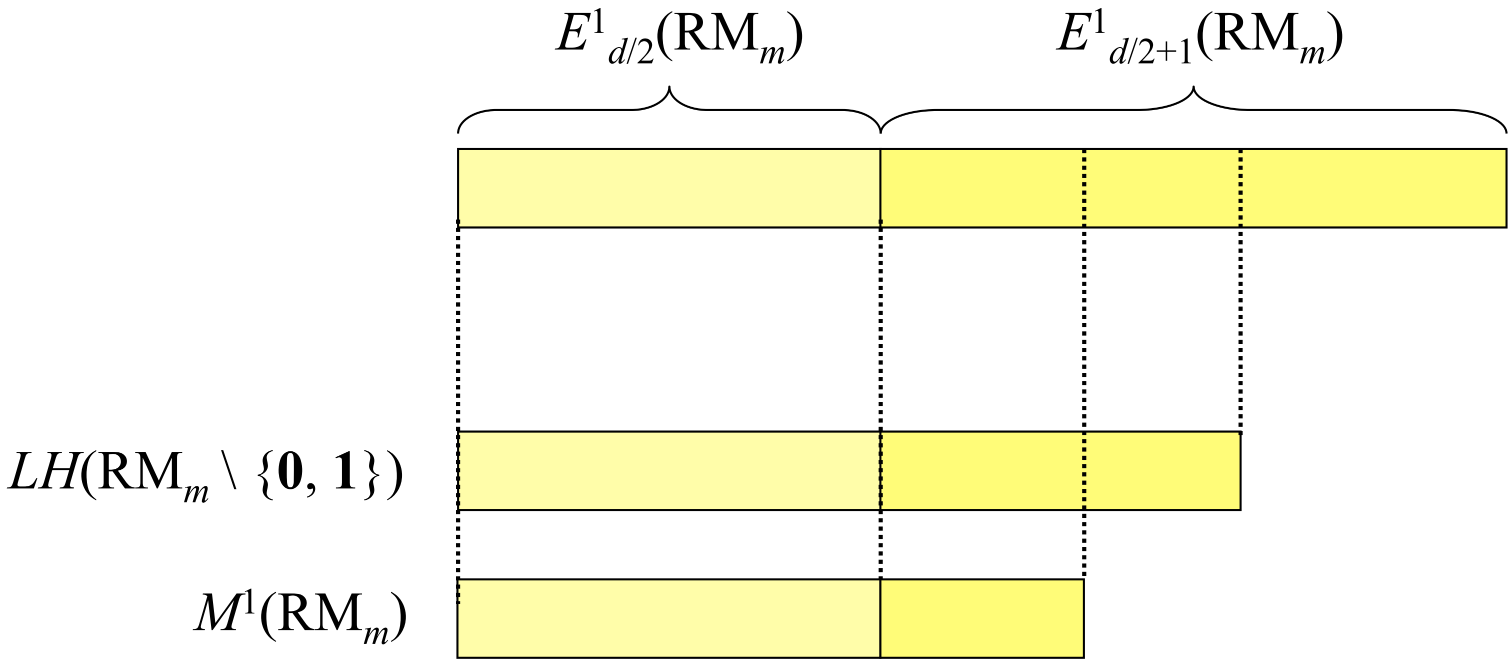
$$\left|E^1_{d/2+1}(\mathrm{RM}_m)\right| = 4(2^m - 1)(2^{m-3} + 1)\binom{2^{m-1}}{2^{m-2}+1} - (4^{m-2} + 3)\binom{2^m}{3}$$

- 重み $d/2+1$ の訂正可能な誤りベクトルの数は

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

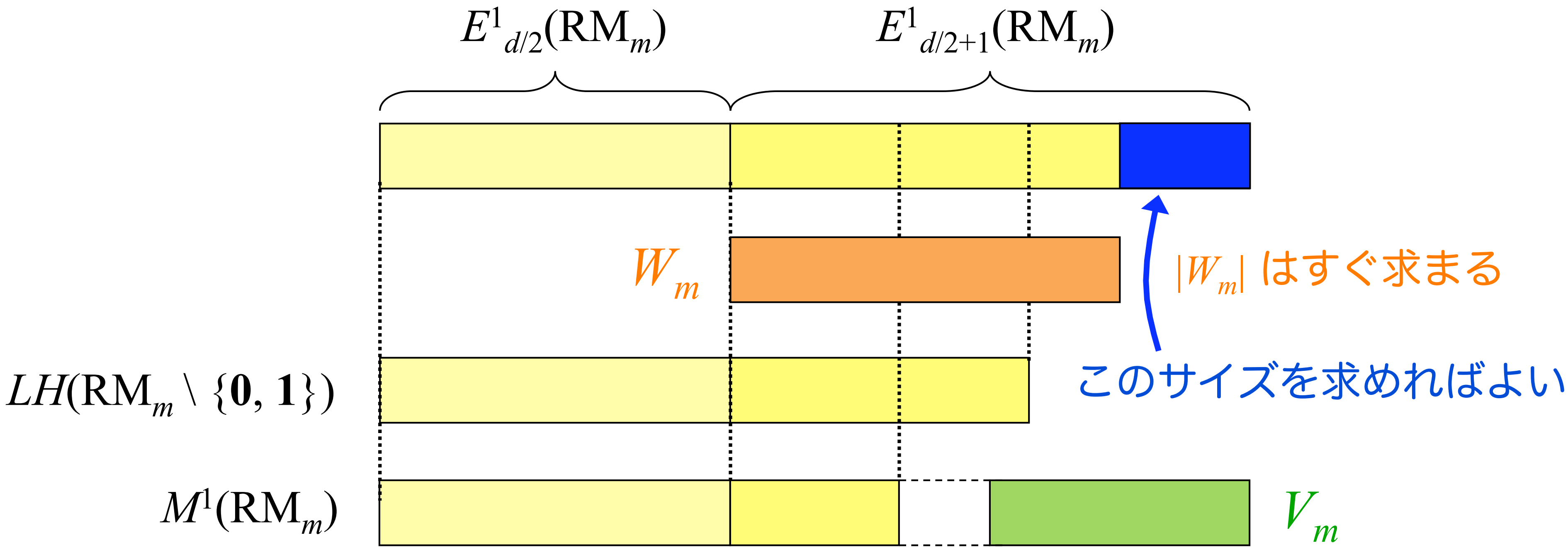
から導出可能

（成果４）： 証明概要



- $M^1(C) \subseteq LH(C \setminus \{\mathbf{0}\}) \subseteq E^1(C)$ の関係を RM_m について調べると上記の関係が成立

（成果４）：証明概要



- $W_m = \{\, \boldsymbol{v} \in \{0, 1\}^n : \boldsymbol{v} \subseteq \boldsymbol{c} \text{ for } \boldsymbol{c} \in \mathrm{RM}_m \setminus \{\mathbf{0},\mathbf{1}\}, w(\boldsymbol{v}) = d/2+1 \}$ を考える
- （青色の部分）に含まれる訂正不可能誤りは極小でない

  ⇒ 重み $d/2$ の訂正不可能誤りに重み 1 のベクトルを足した形

  ⇒ そのようなベクトル集合 V_m を構成し $|V_m \setminus W_m|$ を求める

成果４の結果の考察

（成果４）訂正可能な重み $d/2+1$ の誤りベクトルの数

- 数値例（符号長 2^m）

m	n	k	訂正可能誤り数	訂正不可能誤り数
5	32	6	21,288,320	6,760,480
6	64	7	1.378×10^{15}	1.238×10^{12}
7	128	8	4.299×10^{30}	1.535×10^{22}
8	256	9	5.625×10^{61}	7.938×10^{41}
9	512	10	1.329×10^{124}	7.605×10^{80}

- $m = 9$ のとき、
  訂正不可能な誤りは 10^{44} 個に １ 個の割合

まとめ

- 誤り訂正符号の誤りの単調性を利用した訂正能力分析
  - 重み d/2 以上の訂正可能な誤りベクトルの数について研究
  - 誤りの単調性（Larger Half）を利用

- 研究成果
  - 一般の符号に対して
    （成果１）重み $d/2$ の訂正不可能誤りベクトルの数の下界を導出
    （成果２）重み $d/2+1$ 以上への拡張
  - １次 Reed-Muller 符号に対して
    （成果３）重み $d/2$ の訂正可能誤りベクトルの数について別証明
    （成果４）重み $d/2+1$ の訂正可能誤りベクトルの数を導出

- 今後の研究の方向
  - 一般の符号における $d/2+1$ 以上の場合の下界の改善
  - その他の符号（２次以上 Reed-Muller 符号・BCH符号）への適用

参考文献（1/2）

[Berlekamp, Welch 1972]
E.R. Berlekamp, L.R. Welch, "Weight distributions of the cosets of the (32,6) Reed-Muller code," *IEEE Trans. Inf. Theory*, 1972.

[Charpin 1994]
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.

[Charpin, Helleseth, Zinoviev 2006]
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.

[Helleseth, Klove 1997]
T. Helleseth, T. Kløve, "The Newton radius of codes," *IEEE Trans. Inf. Theory,* 1997.

[Helleseth, Kove, Levenshtein 2005]
T. Helleseth, T. Kløve, and V. Levenshtein, "Error-correction capability of binary linear codes," *IEEE Trans. Inf. Theory,* 2005.

参考文献（2/2）

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

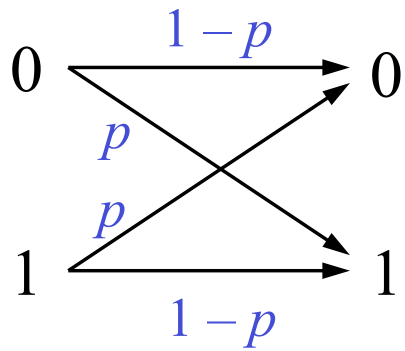
[Poltyrev 1994]
G. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra," *IEEE Trans. Inf. Theory,* 1994.

[Wu 1998]
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.

通信路モデル

２元対称通信路

- 各ビット毎に 0 と 1 を一定確率で反転
- 離散通信路
  - 受信語　$\boldsymbol{y} \in \{0,1\}^n$



加法的白色ガウス雑音(AWGN)通信路

- 各ビット毎に白色ガウス雑音を付加
- 連続通信路
  - 受信語　$\boldsymbol{y} \in \boldsymbol{R}^n$