誤り訂正符号の訂正能力分析

東京工業大学　数理・計算科学専攻
GCOE”計算世界観の深化と展開” 特任助教
安永憲司

コンピュテーション研究会　2009.3.2

発表概要

- 誤り訂正符号
  - 線形符号
  - 通信路モデル（adversarial・確率的）
- 訂正能力分析
  - adversarial モデルにおける分析
  - 確率的モデルにおける分析
- まとめ

誤り訂正符号化

- 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受信側で訂正可能にすること

符号の例（３回繰り返し符号）

メッセージ		符号語
00	→	000000
01	→	000111
10	→	111000
11	→	111111

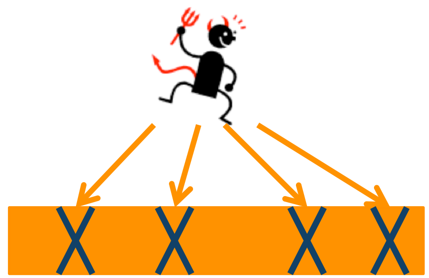
- １ビット以下の誤り（０と１が反転）は訂正可能
- ２ビット以下の誤りは、訂正できない場合もある
  - 受信語が 010101 → 000111
  - 受信語が 011111 → 111111 or 000111

線形符号

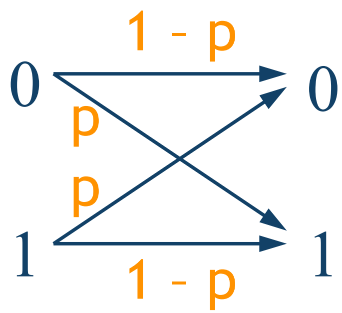
- 符号：符号語の集合
  - 線形空間をなす → 線形符号
- (n,k) 線形符号 C：符号長 n, 次元 k の線形符号
  - $C \subseteq \{0,1\}^n$, $|C|=2^k$
- 符号の最小距離 d：符号語間の最小ハミング距離
  - $d := \min \{ d_H(x, y) : x, y(\neq x) \in C \}$
    - $d_H(x, y) := |\{ i : x_i \neq y_i \}|$
  - 線形符号の場合、最小ハミング重みに等しい
    - $w_H(x) := |\{ i : x_i \neq 0 \}|$

通信路モデル

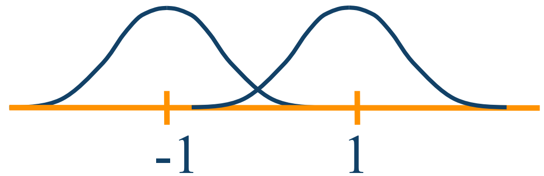
- adversarial モデル
  - t-bit 誤り通信路
    任意の t-bit 以下の誤りが発生



- 確率的モデル
  - ２元対称通信路
    各 bit 毎に確率 p で誤り発生



  - 加法的白色ガウス雑音通信路
    各 bit 毎にガウス雑音が加法的に付加



符号の性能評価

ある復号法を用いたとき、

- adversarial モデル

- 確率的モデル

符号の性能評価

ある復号法を用いたとき、

- adversarial モデル
  → 任意の t-bit 誤りが訂正可能か？
  or t-bit 誤りのうちどのくらいが訂正可能か？
- 確率的モデル

符号の性能評価

ある復号法を用いたとき、

- adversarial モデル
  → 任意の t-bit 誤りが訂正可能か？
  or t-bit 誤りのうちどのくらいが訂正可能か？
- 確率的モデル
  → 復号誤り率

今回考える復号法

- 最小距離復号法
  - 受信語から最小の距離にある符号語に復号

  - ２元対称通信路・加法的白色ガウス雑音通信路に対して最適復号
    - 最適復号 ＝ 復号誤り率を最小にする復号

発表概要

- 誤り訂正符号
  - 線形符号
  - 通信路モデル（adversarial・確率的）
- 訂正能力分析
  - adversarial モデルにおける分析
  - 確率的モデルにおける分析
- まとめ

adversarial モデルにおける訂正能力分析

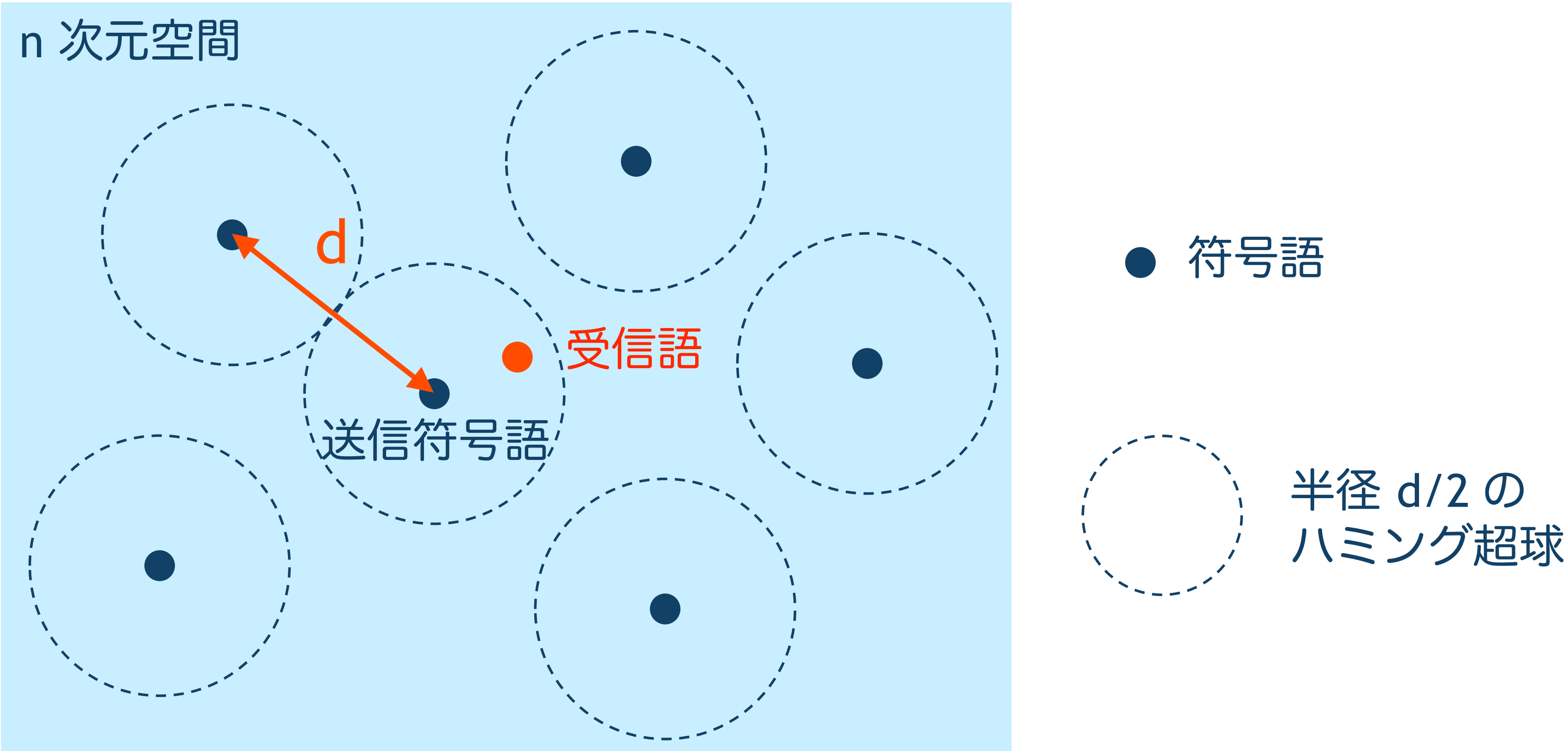
- 問題
  - t-bit 誤り通信路で最小距離復号を行ったときの訂正能力は？

adversarial モデルにおける訂正能力分析

- 問題
  - t-bit 誤り通信路で最小距離復号を行ったときの訂正能力は？
- 回答
  - $t < d/2$ → 必ず誤り訂正可能
  - $t \geq d/2$ → ？？

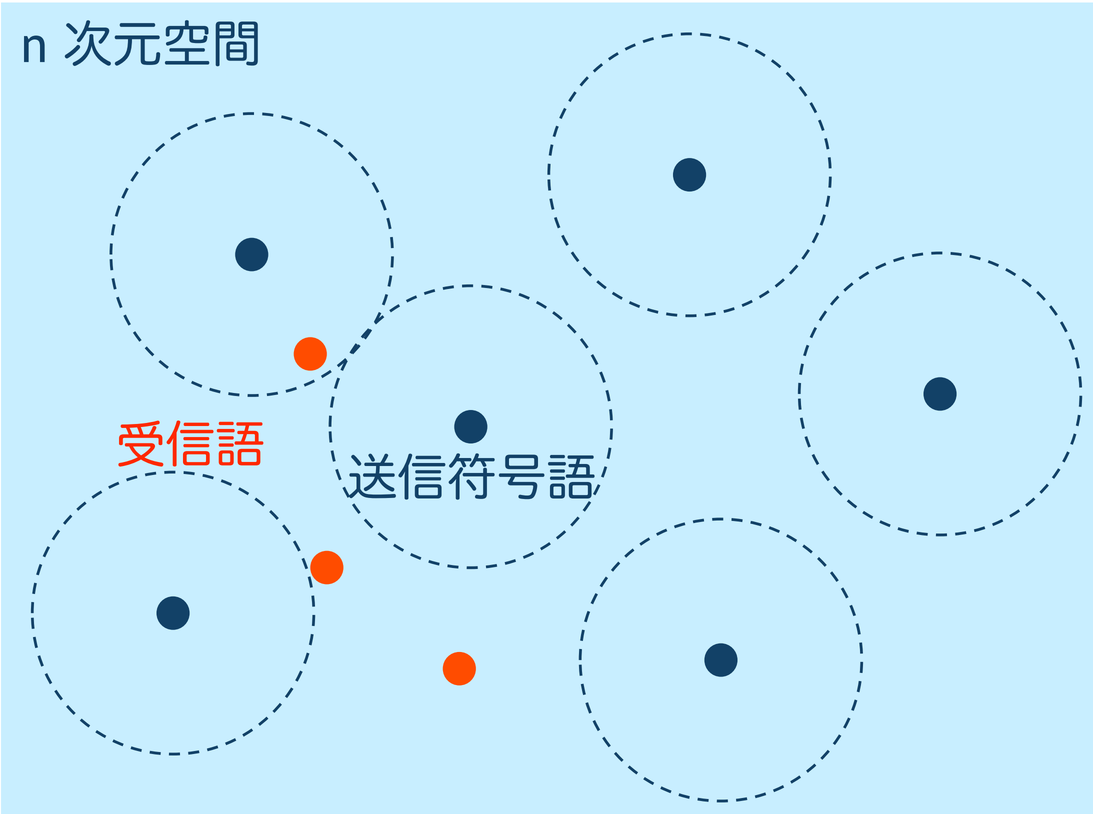
t < d/2 のとき必ず訂正可能な理由

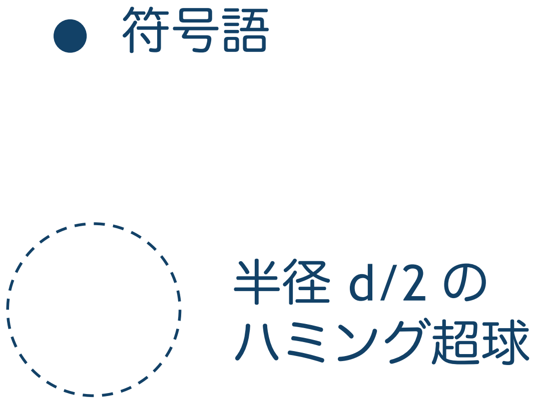
- t < d/2 → 受信語はハミング超球の内側



t ≥ d/2 のとき

+ 訂正可能？





$t \geq d/2$ のとき

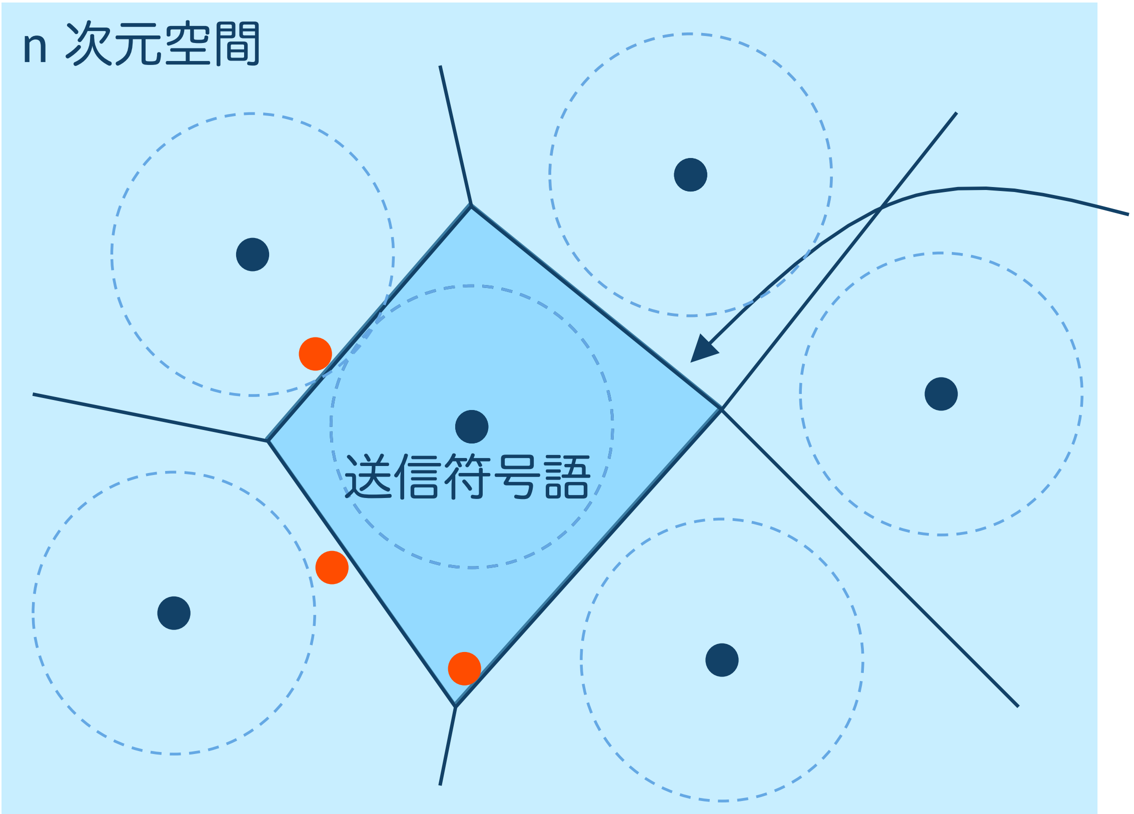
- 最小距離復号 ＝ 距離が最小の符号語に復号

⇓

- 受信語が、他の符号語よりも送信符号語に近い領域にあれば、訂正可能

t ≥ d/2 のとき

- 訂正可能？



送信符号語に最も距離の近い領域

||

送信符号語のボロノイ領域

adversarial モデルにおける訂正能力分析

- 問題
  - t-bit 誤り通信路で最小距離復号を行ったときの訂正能力は？
- 回答
  - $t < d/2$ → 必ず誤り訂正可能
  - $t \geq d/2$ → 受信語が送信符号語のボロノイ領域内なら訂正可能

本研究では、$t \geq d/2$ の場合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
  + t ≥ d/2 の、訂正不可能誤りベクトル数の上界 [Poltyrev 1994], [Helleseth, Kløve 1997], [Helleseth, Kløve, Levenshtein 2005]
+ １次 Reed-Muller 符号に対して
  + n = 32、すべての t について訂正可能誤りベクトル数を計算 [Berlekamp, Welch 1972]
  + t = d/2 の訂正可能誤りベクトルの数 [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 ≤ 128, 29 ≤ n - k ≤ 42 の Reed-Muller 符号・BCH 符号について計算 [Maeda, Fujiwara 2001]

研究成果 [Yasunaga, Fujiwara 2008]

- 一般の符号に対して
  （成果１） $t = d/2$ の訂正不可能誤りベクトルの数の下界
  （成果２） $t \geq d/2+1$ への拡張
- １次 Reed-Muller 符号に対して
  （成果３） $t = d/2$ の訂正可能誤りベクトルの数の別証明
  （成果４） $t = d/2+1$ の訂正可能誤りベクトルの数

いずれの結果も誤りの単調性を利用

訂正可能・不可能な誤り

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

- 訂正可能誤り $E^0(C)$:= 最小距離復号で訂正可能な誤り
- 訂正不可能誤り $E^1(C) := \{0,1\}^n \setminus E^0(C)$
  - $E_i^b(C) := \{ v \in E^b(C) : w_H(v) = i \}, b = 0,1$
  - $|E_i^0(C)|+|E_i^1(C)| = (n \text{ choose } i)$
  - $|E_i^1(C)| = 0$ for $i < d/2$

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

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（受信語と距離最小の符号語が複数）
  ⇒　辞書順で最小の誤りを訂正
  ⇒　誤りが単調性を持つ [Peterson, Weldon 1972]

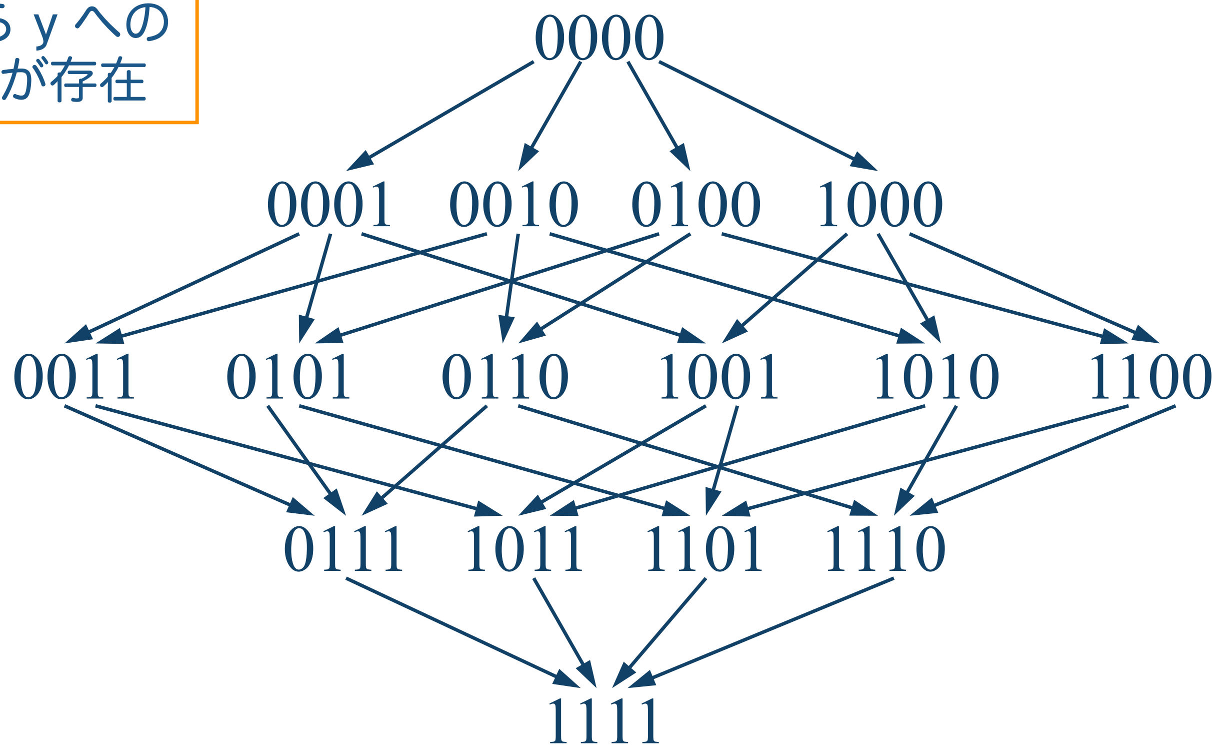
+ 誤りの単調性：

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

+ x が y にカバーされる ⇔ $x_i \leq y_i$ for all i

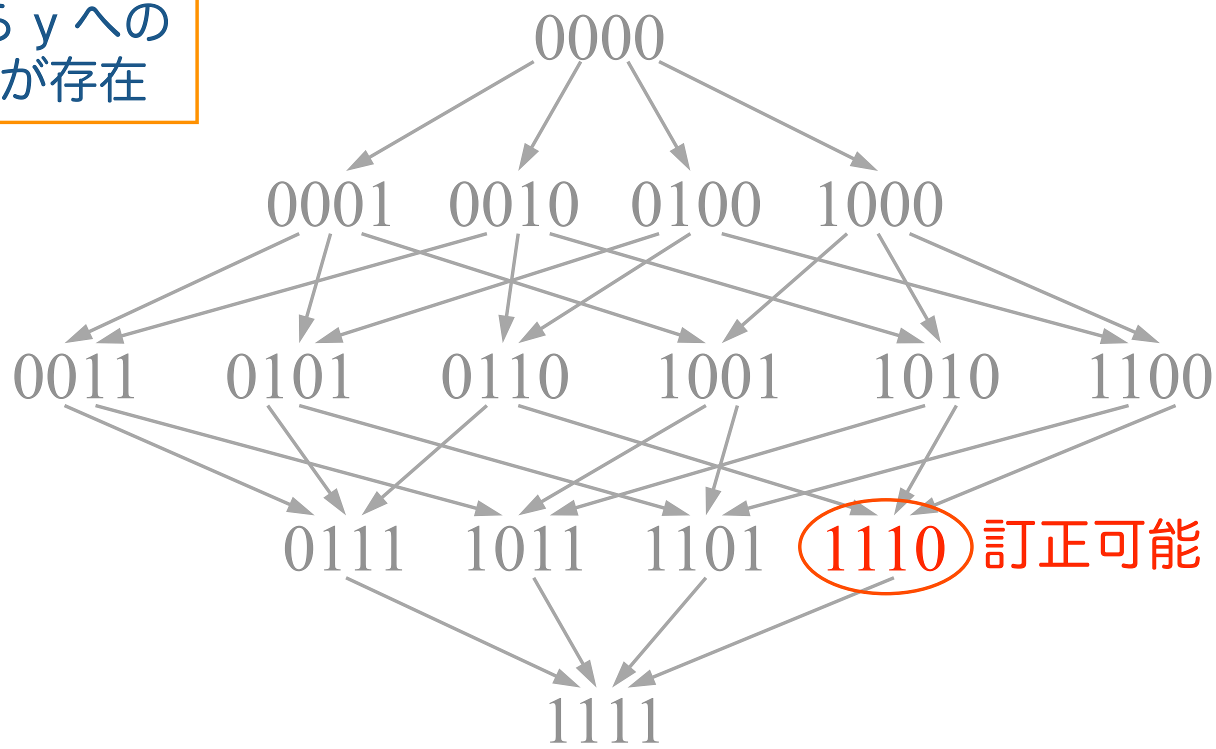
x が訂正可能　⇒ x にカバーされる誤りもすべて訂正可能
x が訂正不可能 ⇒ x をカバーする誤りもすべて訂正不可能

x が y に
カバーされる
⇔
x から y への
パスが存在



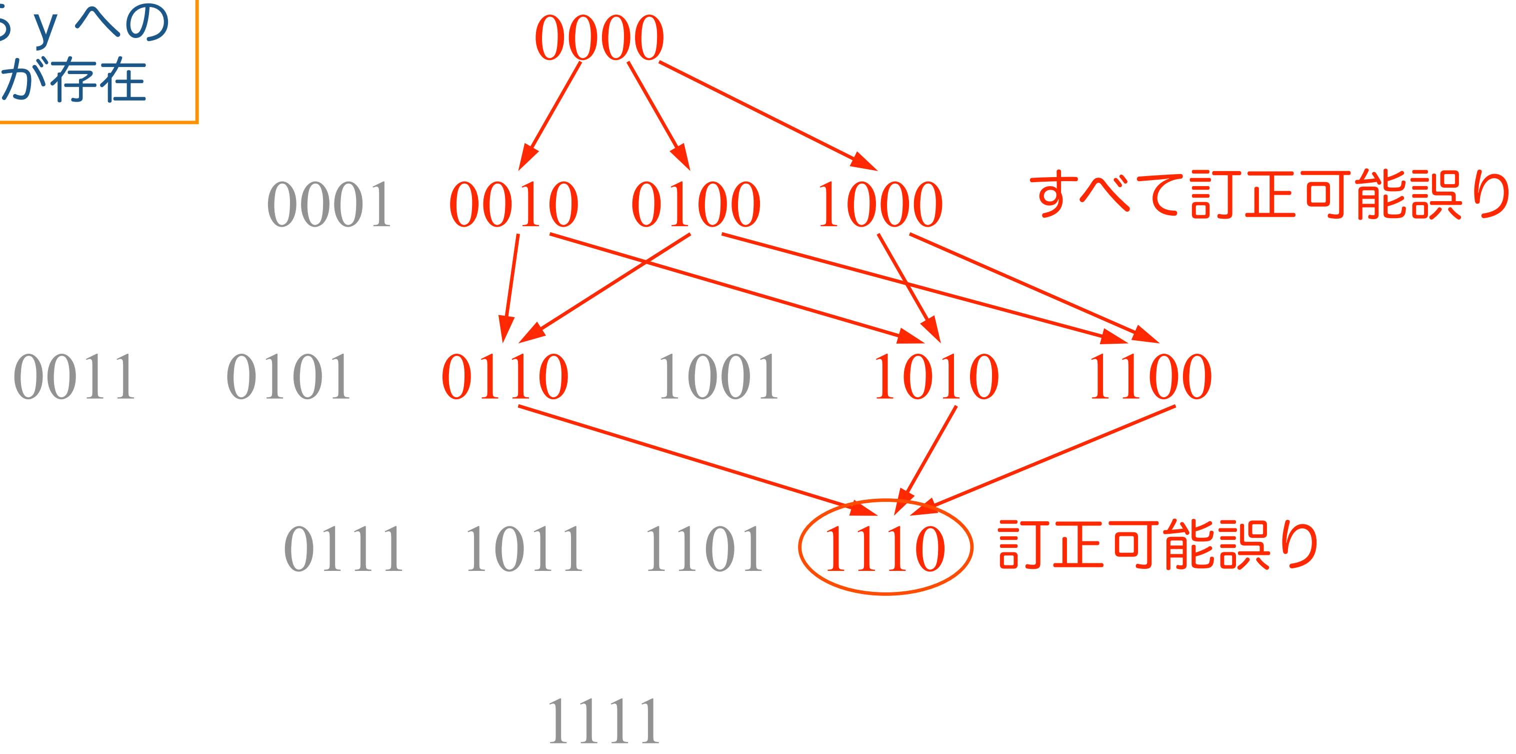
x が訂正可能　⇒ x にカバーされる誤りもすべて訂正可能
x が訂正不可能 ⇒ x をカバーする誤りもすべて訂正不可能

x が y に
カバーされる
⇔
x から y への
パスが存在



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

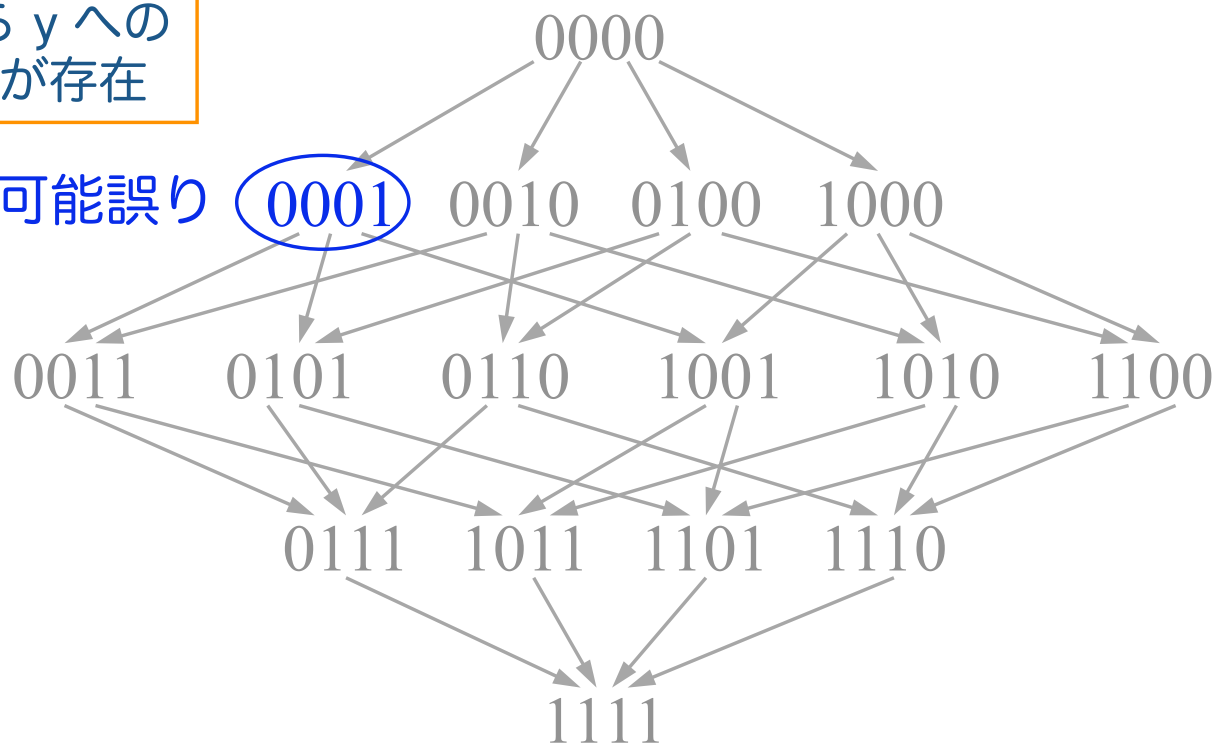
x が y に
カバーされる
⇔
x から y への
パスが存在



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

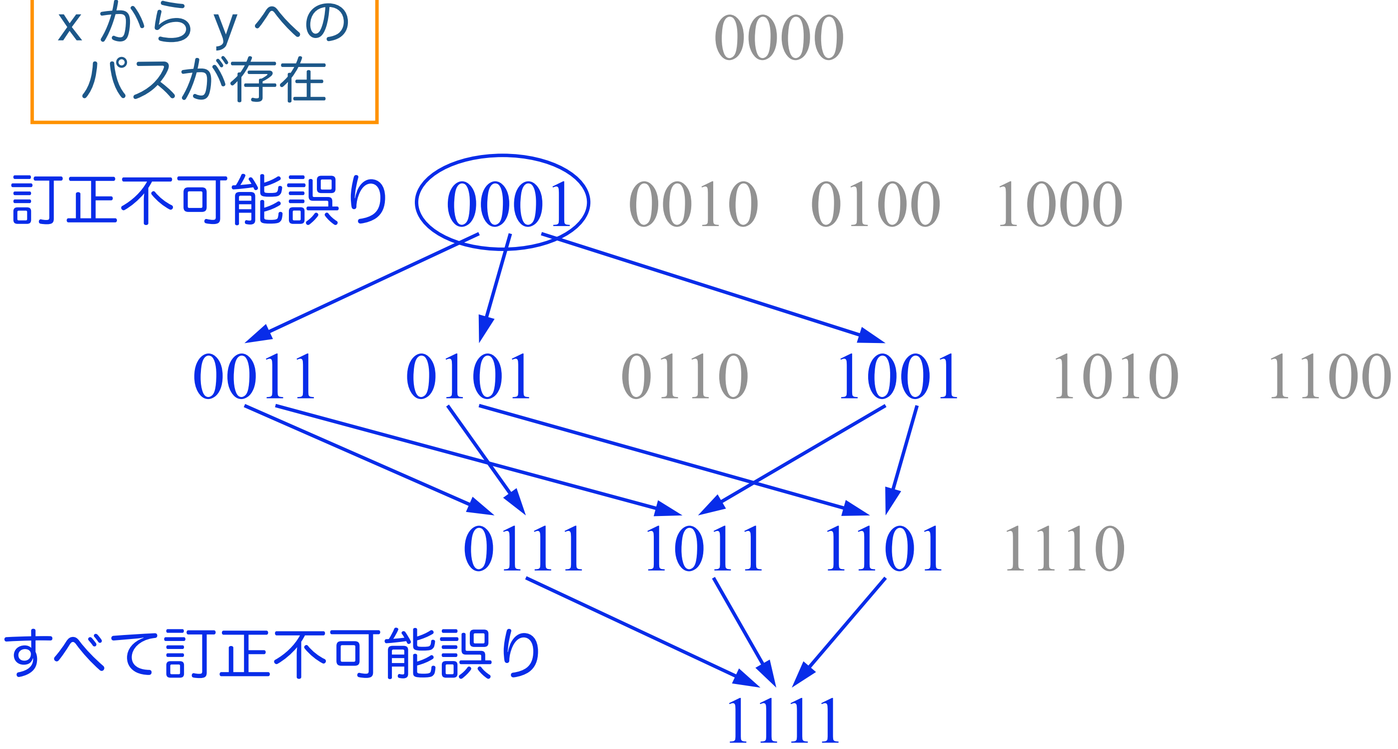
x が y に
カバーされる
⇔
x から y への
パスが存在

訂正不可能誤り



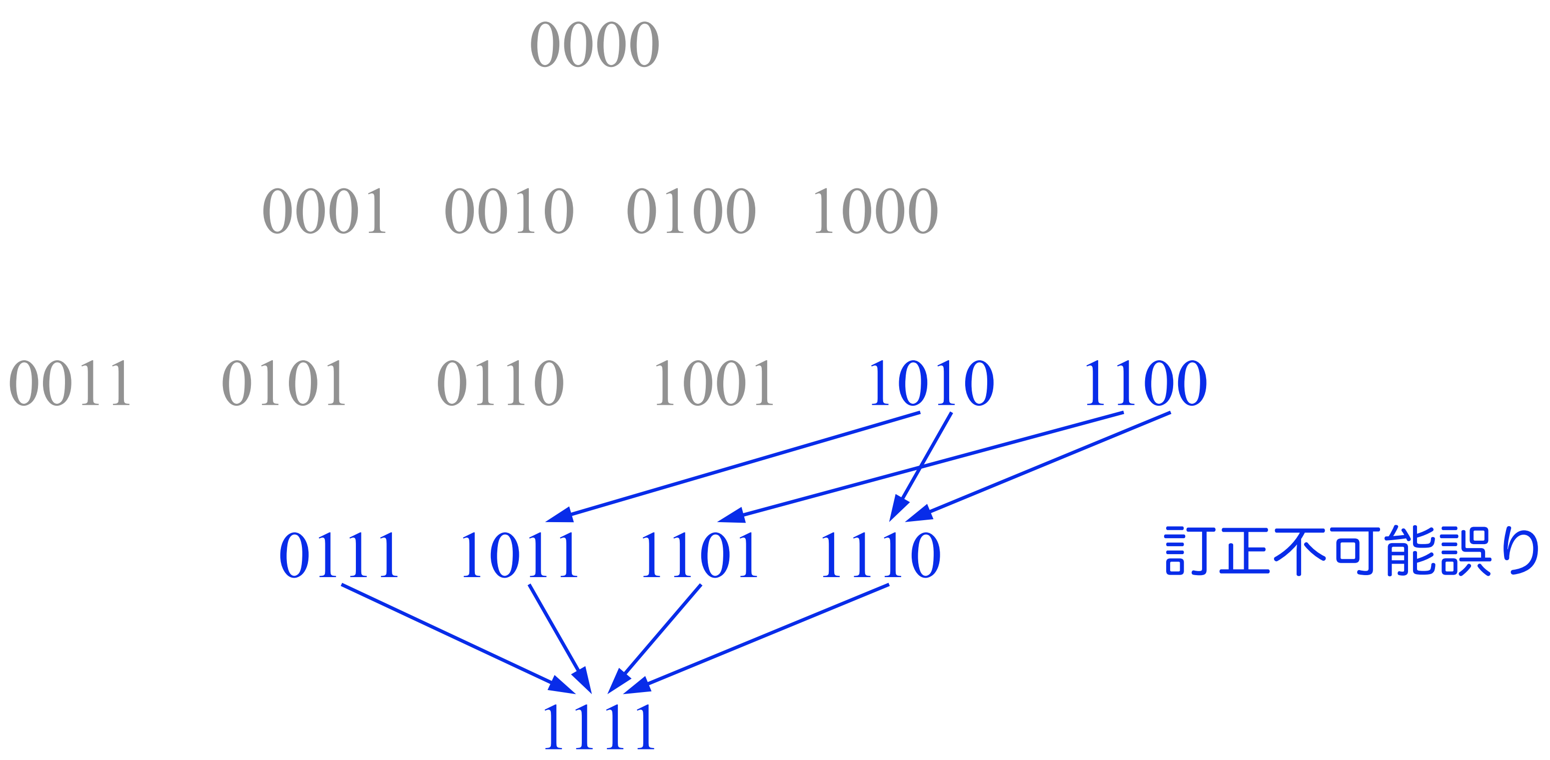
x が訂正可能　⇒ x にカバーされる誤りもすべて訂正可能
x が訂正不可能 ⇒ x をカバーする誤りもすべて訂正不可能

x が y に
カバーされる
⇔
x から y への
パスが存在



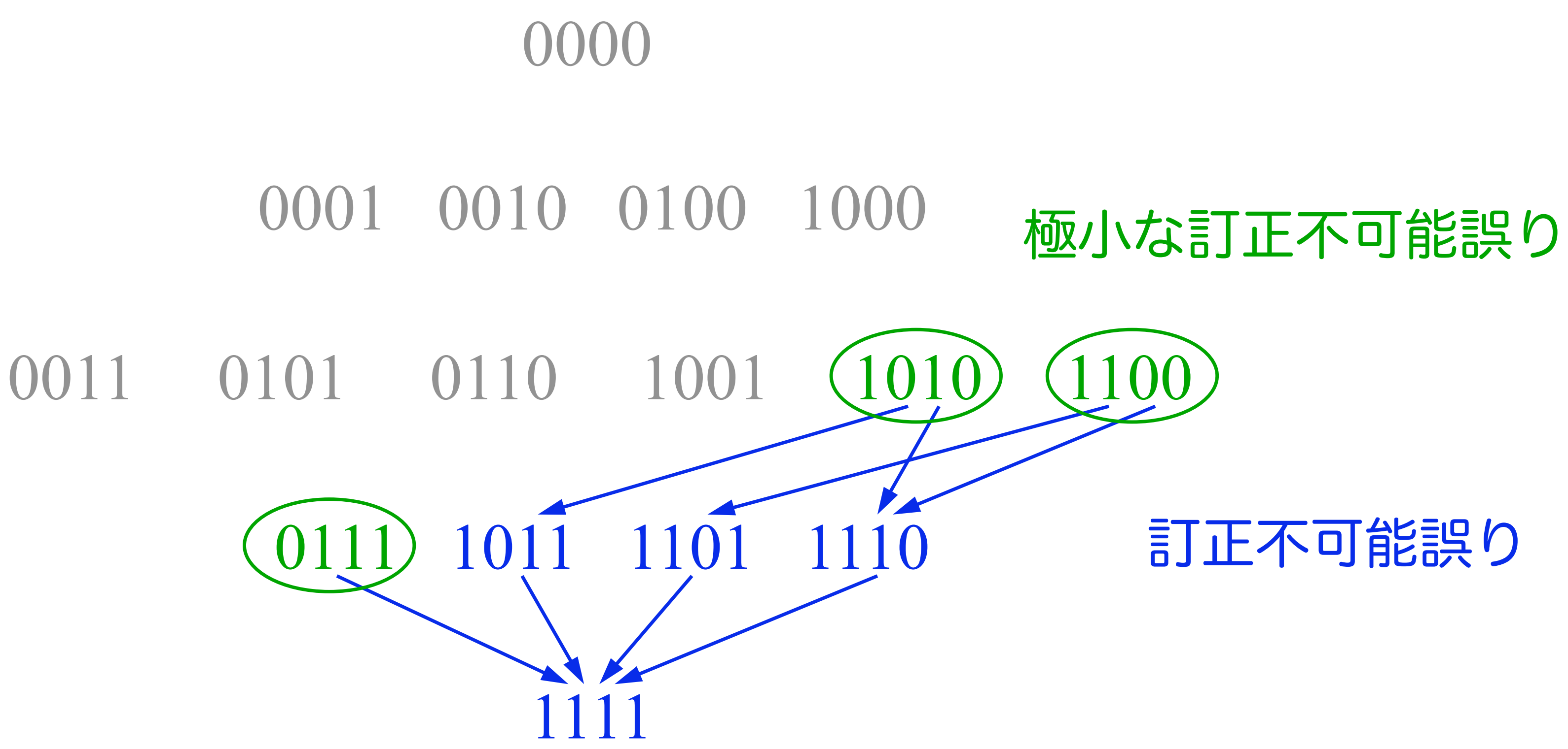
単調性があるとき

- 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



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



Larger Half

- 符号語 c の Larger Half; LH(c)
  - $M^1(C)$ を特徴付けるために導入 [Helleseth, Klove, Levenshtein 2005]
  - LH(c) := { $v \in \{0,1\}^n$: 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
  - $\boxed{M^1(C) \subseteq LH(C \setminus \{0\}) \subseteq E^1(C)}$ $\quad LH(U) = \bigcup_{c \in U} LH(c)$
  - 組み合わせ的構成法が知られている

研究成果 [Yasunaga, Fujiwara 2008]

- 一般の符号に対して
  （成果１）$t = d/2$ の訂正不可能誤りベクトルの数の下界
  （成果２）$t \geq d/2+1$ への拡張
- １次 Reed-Muller 符号に対して
  （成果３）$t = d/2$ の訂正可能誤りベクトルの数の別証明
  （成果４）$t = d/2+1$ の訂正可能誤りベクトルの数

成果１・２・４について以下で紹介

（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

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

C_w = { C の重み 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 の重み 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

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

[証明]

- $M^1(C) \subseteq LH(C \setminus \{0\}) \subseteq E^1(C)$
- 重み $\lceil d/2 \rceil$ は $E^1(C)$ で最小の重みであり、その重みの誤りは $E^1(C)$ のその他の誤りにカバーされない

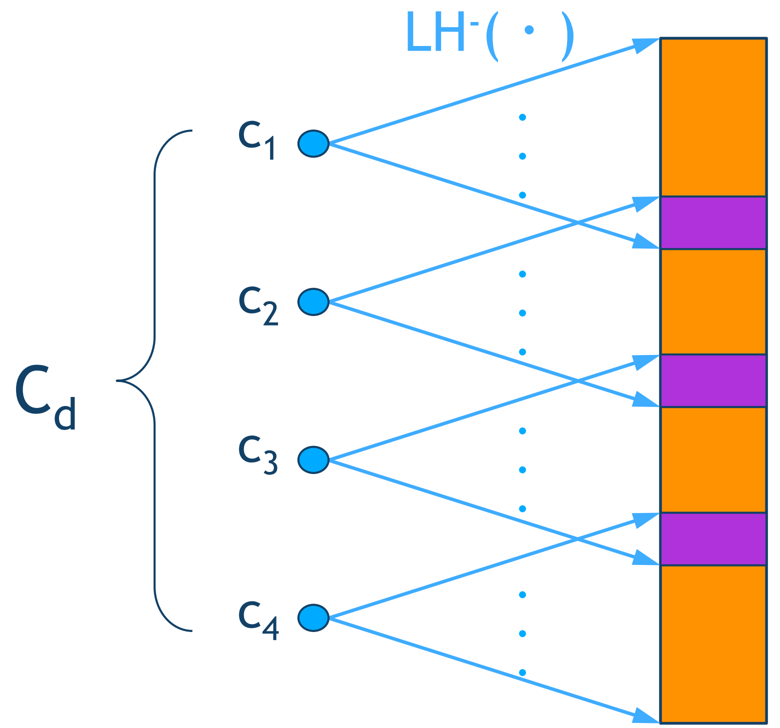
$$\Rightarrow M^1_{\lceil d/2 \rceil}(C) = E^1_{\lceil d/2 \rceil}(C)$$

- $\left|LH_{\lceil d/2 \rceil}(C \setminus \{0\})\right|$ の下界によって $\left|E^1_{\lceil d/2 \rceil}(C)\right|$ の下界を導出

（成果１）： 証明概要（d が偶数の場合）

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

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



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

$\}$ $(|C_d| - 1)/2$ 以下

各 $c_i \in C_d$ について
重複は $(|C_d| - 1)/2$ 個以下

したがって

$$(|LH(c_i)| - (|C_d| - 1)/2)\ |C_d| \le |LH_{d/2}(C \setminus \{0\})|$$

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・ $\mathbf{m} \to \infty$ で満たされる
- また、$\mathbf{m} \to \infty$ 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

条件を満たす r, m

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

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

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

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

- 重み分布は２項分布にしたがう

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

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、$d \approx d_{GV} n$ なので満たされる

- $n \to \infty$で $|C_d| \Big/ \binom{d}{d/2} \to 0,\ |C_{d+1}| \Big/ \binom{d}{(d+1)/2} \to 0$
  なので上界・下界は漸近的に一致

（成果２）： 結果

$\lceil d/2 \rceil \le i \le \lceil n/2 \rceil$ 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 (1)下界のための条件が厳しい (2) 弱い下界
  - 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

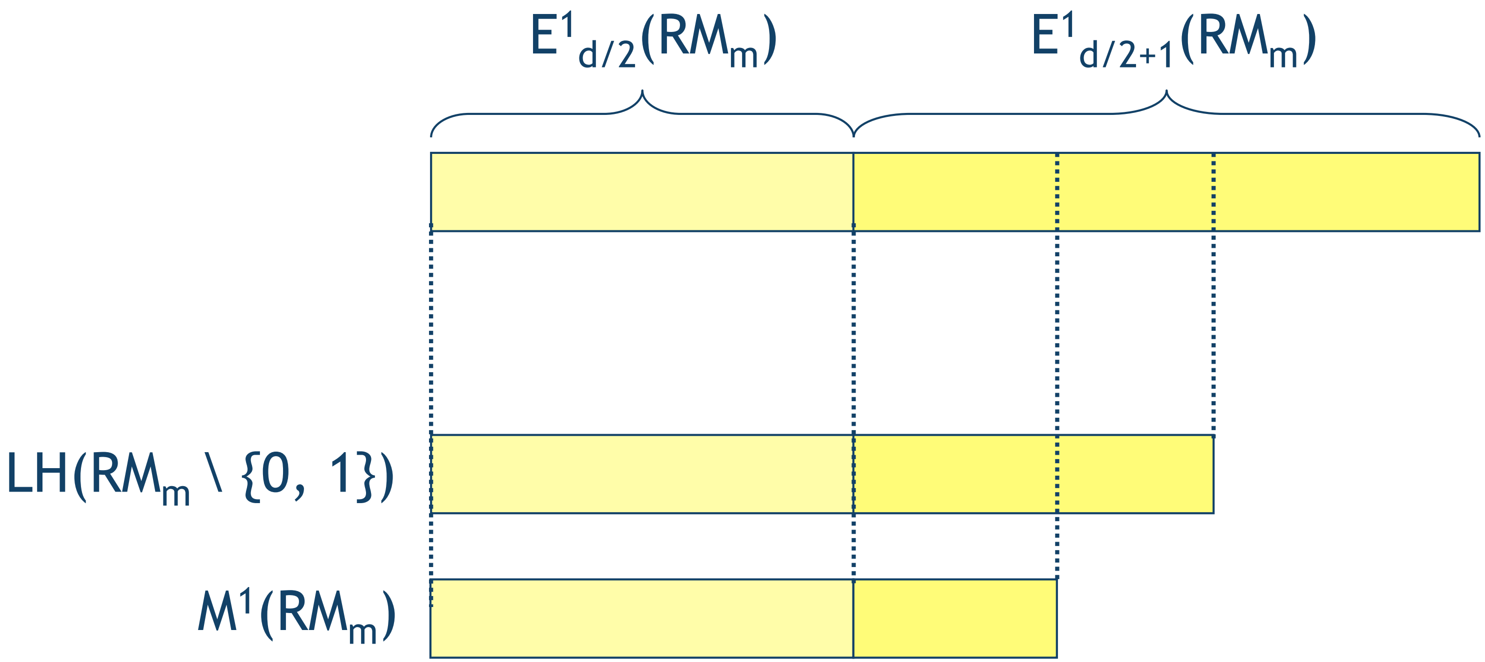
- $(2^m, m+1)$ 符号で最小距離 $d = 2^{m-1} = n/2$
  - 次元は小さいが、最小距離が非常に大きい
  - non-trivial な符号の中では構造が非常にシンプル
- 符号語は m 変数の線形ブール関数と一対一に対応
  - r 次 Reed-Muller 符号 ⇔ r 次ブール関数
- RM_m の重み i の訂正可能誤りの数
⇔ 非線形性が i のブール関数の数
  - 関数 f の非線形性：f と線形関数との距離を表す

（成果４）： 結果

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

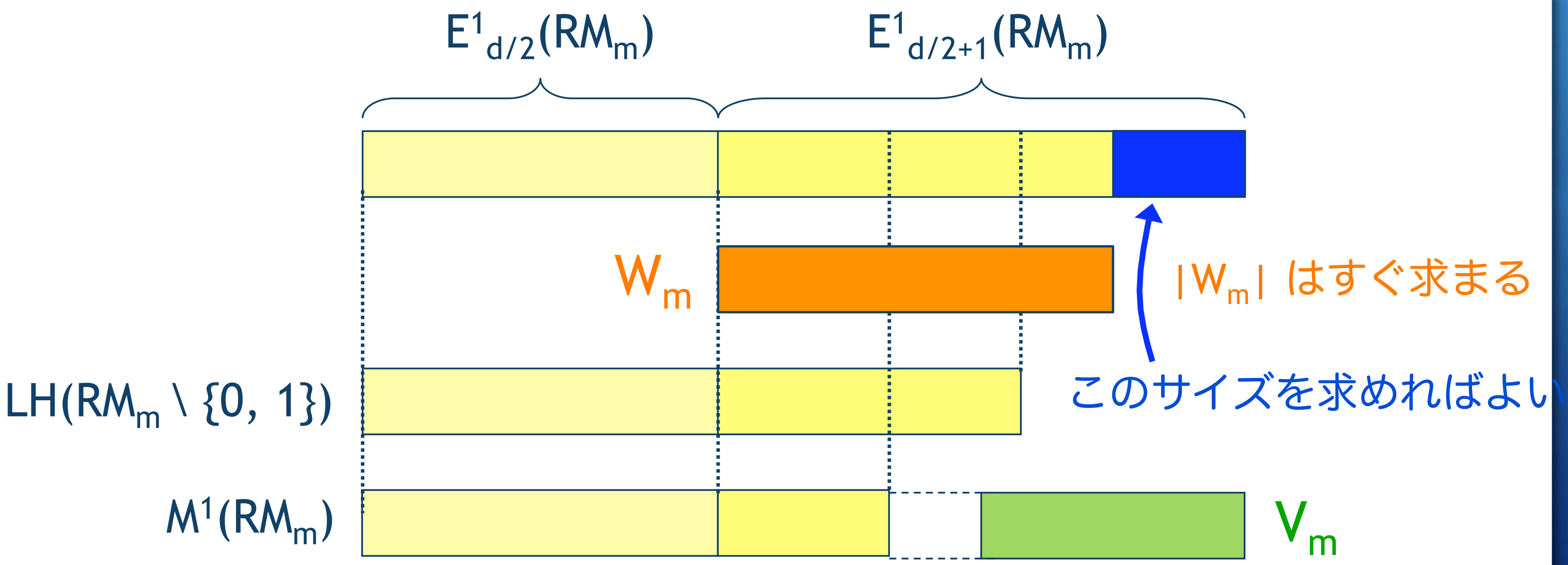
$$\left|E^1_{d/2+1}(RM_m)\right| = 4(2^m - 1)(2^{m-3} + 1)\binom{2^{m-1}}{2^{m-2} + 1} - (4^{m-2} + 3)\binom{2^m}{3}$$

（成果４）：証明概要



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

（成果４）：証明概要



- $W_m = \{ v \in \{0, 1\}^n : v \subseteq c \text{ for } c \in RM_m \setminus \{0,1\}, w(v) = d/2+1\}$ を考える
- 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

発表概要

- 誤り訂正符号
  - 線形符号
  - 通信路モデル（adversarial・確率的）
- 訂正能力分析
  - adversarial モデルにおける分析
  - 確率的モデルにおける分析
- まとめ

確率的モデルにおける訂正能力分析

- 問題
  - ２元対称通信路や加法的白色ガウス雑音通信路で最小距離復号を行ったときの復号誤り率は？

確率的モデルにおける訂正能力分析

- 問題
  - ２元対称通信路や加法的白色ガウス雑音通信路で最小距離復号を行ったときの復号誤り率は？
- 回答
  - ２元対称通信路の場合、$|E_i^1(C)|$ for $1 \leq i \leq n$ から求まる

確率的モデルにおける訂正能力分析

- 問題
  - ２元対称通信路や加法的白色ガウス雑音通信路で最小距離復号を行ったときの復号誤り率は？
- 回答
  - ２元対称通信路の場合、$|E_i^1(C)|$ for $1 \le i \le n$ から求まる
  - 一般には、受信語が送信符号語のボロノイ領域に入る確率に等しい

確率的モデルにおける訂正能力分析

- 問題
  - ２元対称通信路や加法的白色ガウス雑音通信路で最小距離復号を行ったときの復号誤り率は？
- 回答
  - ２元対称通信路の場合、$|E_i^1(C)|$ for $1 \leq i \leq n$ から求まる
  - 一般には、受信語が送信符号語のボロノイ領域に入る確率に等しい
  - しかし、計算量が莫大 → 上界・下界を計算

復号誤り率の上界・下界

- 様々な上界・下界が提案されている
  - 和集合上界
  - Gallager-type bound
  - sphere packing bound
  - de Caen’s inequality based bound

- 多くの上界・下界において、符号の重み分布を利用
  - C の重み分布 = ($|C_0|$, $|C_1|$, …, $|C_n|$)
    - C_w : C で重み w の符号語の集合

復号誤り率

- $C = \{ c_0, c_1, \ldots , c_{M-1} \}, M = 2^k$
- c_0 (= 0) を送信したと考える
  - 線形符号の場合、誤り率は符号語によらない
- A_i : c_0 を送信して c_i に復号される事象

$$P_{error} = \Pr\left(\bigcup_{i=1}^{M-1} A_i \right)$$

復号誤り率

- $C = \{ c_0, c_1, \ldots , c_{M-1} \}$, $M = 2^k$
- c_0 (= 0) を送信したと考える
  - 線形符号の場合、誤り率は符号語によらない
- A_i : c_0 を送信して c_i に復号される事象

$$P_{error} = \Pr\left(\bigcup_{i=1}^{M-1} A_i \right)$$

$$\leq \sum_{i=1}^{M-1} \Pr(A_i)$$

和集合上界 (Union bound)

和集合上界

$$P_{error} \le \sum_{i=1}^{M-1} \Pr(A_i)$$

- $\Pr(A_i)$ = { 0 を送信して c_i に復号される確率}

和集合上界

$$P_{error} \le \sum_{i=1}^{M-1} \Pr(A_i)$$

- $\Pr(A_i)$ = { 0 を送信して c_i に復号される確率}

 = { 受信語が 0 よりも c_i に近い領域に入る確率 }

和集合上界

$$P_{error} \le \sum_{i=1}^{M-1} \Pr(A_i)$$

- Pr(A_i) = { 0 を送信して c_i に復号される確率}

= { 受信語が 0 よりも c_i に近い領域に入る確率 }

← 0 と c_i の距離（c_i の重み）で決まる

和集合上界

$$P_{error} \le \sum_{i=1}^{M-1} \Pr(A_i)$$

- $\Pr(A_i)$ = { 0 を送信して c_i に復号される確率}

= { 受信語が 0 よりも c_i に近い領域に入る確率 }

← 0 と c_i の距離（c_i の重み）で決まる

➡ 和集合上界は重み分布から計算できる

２元対称通信路の場合

- ２元対称通信路での復号誤り率

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

  - p は 0 と1 の反転確率

- $|E_i^1(C)|$ に対する上界・下界
→ 復号誤り率の上界・下界

加法的白色ガウス雑音通信路の場合

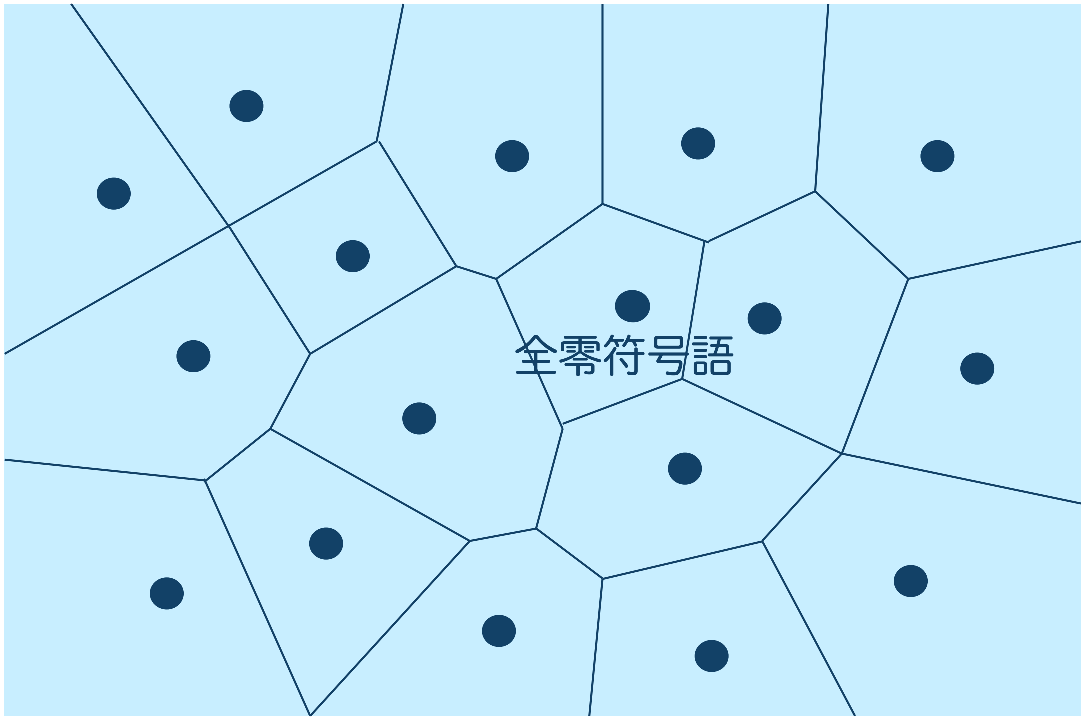
- 重み分布による上界・下界
- 局所重み分布によってより精度の高い上界・下界
- 重み分布より計算コストが高い
  - n = 128, 256 でも単純な方法では計算困難

⇒ 局所重み分布の導出法について研究

局所重み分布

- 符号 C の局所重み分布 ＝ C 中の零隣接語の重み分布
  - 零隣接語 ＝ 全零符号語とボロノイ領域が隣接する符号語

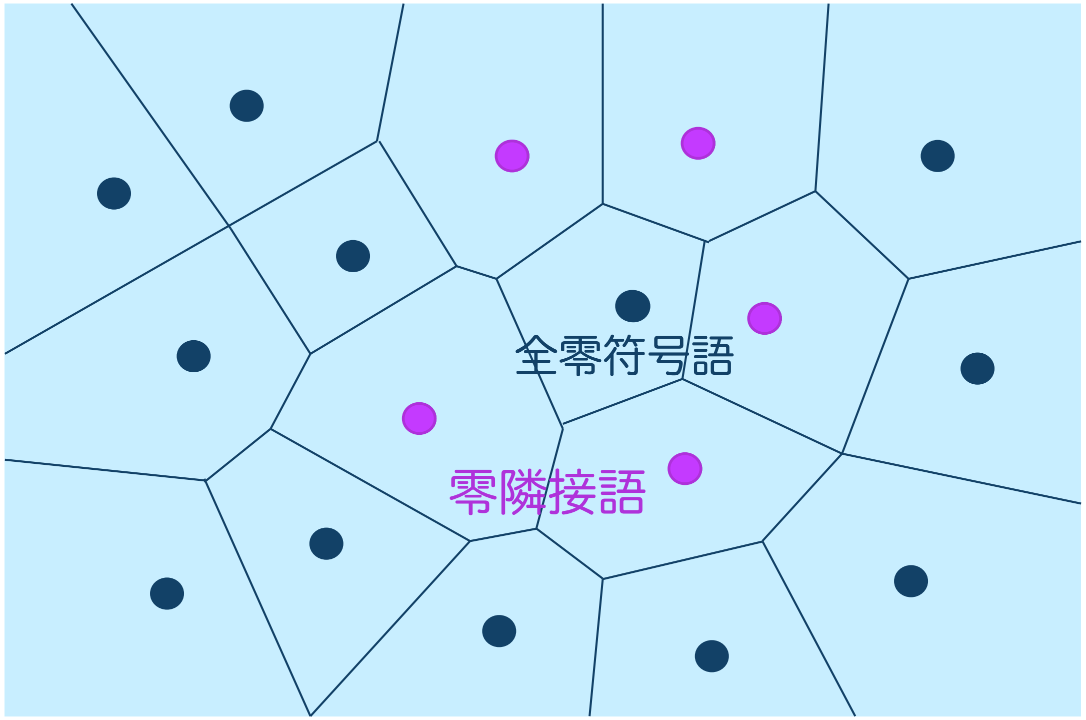
R^n 上の C の符号語



局所重み分布

- 符号 C の局所重み分布 ＝ C 中の零隣接語の重み分布
  - 零隣接語 ＝ 全零符号語とボロノイ領域が隣接する符号語

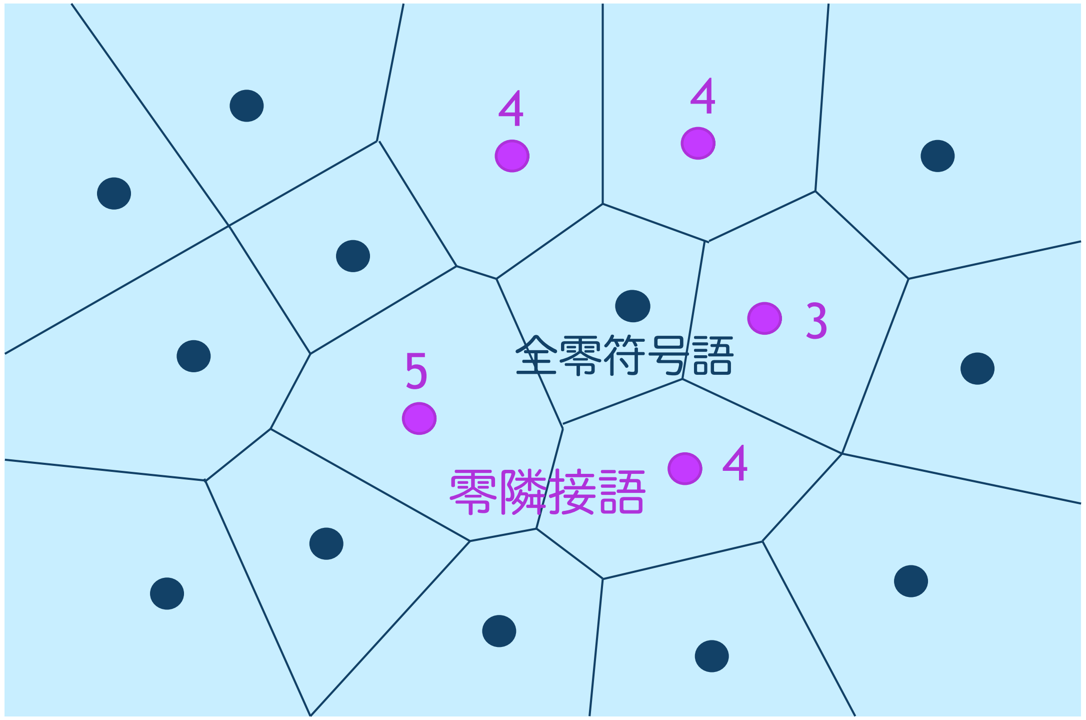
R^n 上の C の符号語



局所重み分布

- 符号 C の局所重み分布 ＝ C 中の零隣接語の重み分布
  - 零隣接語 ＝ 全零符号語とボロノイ領域が隣接する符号語

R^n 上の C の符号語



C の局所重み分布

重み	零隣接語の数
3	1
4	3
5	1

研究成果 [Yasunaga, Fujiwara 2006]

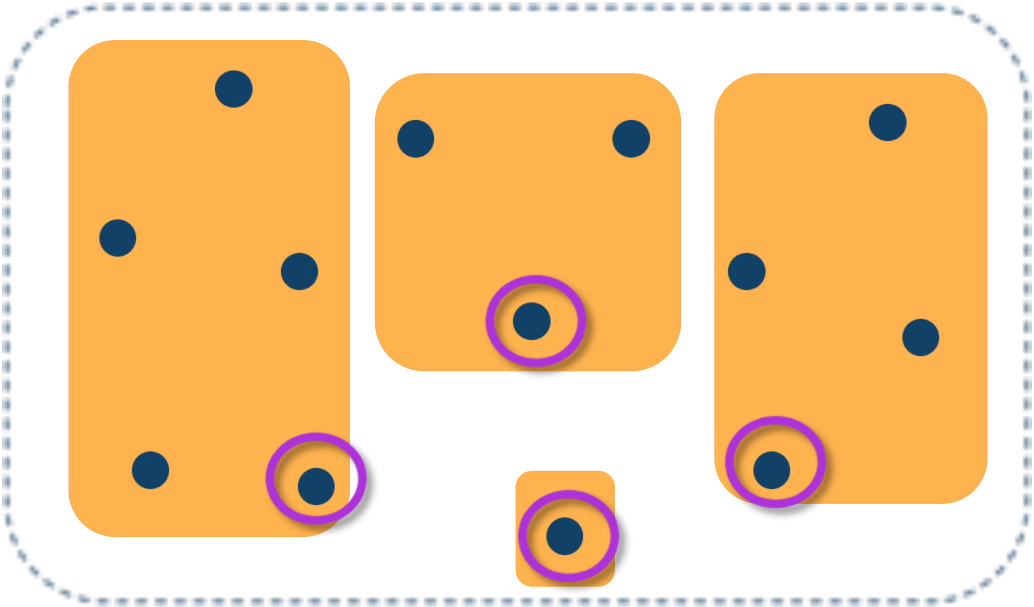
- 計算的アプローチ
  - 局所重み分布導出アルゴリズムの提案
    - 符号の代数的構造（自己同型群）を利用
- 理論的アプローチ
  - 符号とその拡大符号・偶部分符号の局所重み分布間の関係を解明
- 結果として、n = 128, 256 程度について局所重み分布導出
  - 拡大原始BCH符号
  - 原始BCH符号とその偶部分符号
  - Reed-Muller符号
  - パンクチャドReed-Muller符号とその偶部分符号

計算的アプローチ

- 単純な計算方法
  - 全符号語について零隣接性を調べることで導出
  - 計算量 $O(n^2k \cdot 2^k)$
    - 零隣接性のチェック $O(n^2k)$ × 符号語数 2^k
- 零隣接性のベクトル置換不変性を利用
  c が零隣接語 ⇔ p(c) も零隣接語
  - $p \in Aut(C) = \{p : \bigcup_{c \in C} p(c) = C\}$

提案アルゴリズム

- アイディア
  - c の零隣接性 = { p(c) : p ∈ Aut(C) } の零隣接性



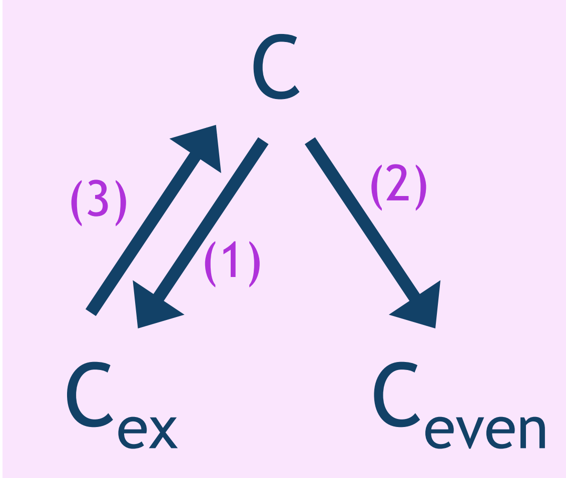
手順
1. 零隣接性が同じもの同士に分類
2. 代表符号語について零隣接性をチェック

提案アルゴリズムの評価

- 計算量
  - $O(n^2k \cdot E)$, E：同値類の数
    - Aut(C) が大きいほど E は小さくなる傾向
- Aut(C) のサイズ
  - 巡回符号（巡回置換群）$O(n)$
  - 拡大原始 BCH 符号（アフィン置換群）$O(n^2)$
  - Reed-Muller 符号 （一般化線形置換群）$2^{O(n \log n)}$

理論的アプローチ

- 符号 C, 拡大符号 C_{ex}, 偶部分符号 C_{even} の局所重み分布間の関係
  - LWD(C)：局所重み分布
  - N(C)：偶重み分解不可能符号語の分布



(成果１) LWD(C), N(C) $\Rightarrow$ LWD(C_{ex})

(成果２) LWD(C), N(C) $\Rightarrow$ LWD(C_{even})

(成果３) C_{ex} が推移不変符号(Reed-Muller, 拡大原始BCH)のとき
LWD(C_{ex}), N(C_{ex}) $\Rightarrow$ LWD(C)

(成果４) C の重みがすべて４の倍数 $\Rightarrow$ N(C) はすべて 0

- 符号長 128 以上のReed-Muller符号，(128, k) 拡大原始BCH符号 $k \leq 57$

求めた局所重み分布

- (128, k) 拡大原始BCH符号 (k = 50, 43, 36)
  - 提案アルゴリズムを利用
  - (128,50) 拡大原始BCH符号 ・・・ 従来法の 1/130 の 440 時間
- (127, k) 原始BCH符号 (k = 50, 43, 36) とその偶部分符号
  - 局所重み分布間の関係を利用
  - 提案アルゴリズムでは求めることができなかった
- (128, 64), (256, 93) Reed-Muller符号
  - 提案アルゴリズムを利用
  - (128,64) Reed-Muller符号 ・・・ 従来法の 15 億分の 1 の 13 時間
- (127, 64), (255, 93) パンクチャドReed-Muller符号とその偶部分符号
  - 局所重み分布間の関係を利用
  - 提案アルゴリズムでは求めることができなかった

上界・下界改善のための適用

「重み分布 → 局所重み分布」による上界・下界の改善

+ [Agrell 1996]
  + 和集合上界
+ [安田, 安永, 藤原 2005]
  + de Caen’s inequality based lower bound
  + （一部の）和集合下界

まとめ

- 最小距離復号を用いた場合の訂正能力分析
  - 最小距離復号：２元対称通信路・加法的白色ガウス雑音通信路で最適復号
- adversarial モデル
  → $t \geq d/2$ での訂正可能誤りベクトルの数で評価
- 確率的モデル
  → 復号誤り確率で評価

研究成果のまとめ (1/2)

- $t \geq d/2$ での訂正可能誤りベクトルの数の研究
  - 誤りの単調性を利用した分析
- 研究成果 [Yasunaga, Fujiwara 2008]
  - 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
    （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の別証明
    （成果４）重み $d/2+1$ の訂正可能誤りベクトルの数

研究成果のまとめ (2/2)

- 局所重み分布の導出について研究
  - 加法的白色ガウス雑音通信路での誤り率改善
- 研究成果 [Yasunaga, Fujiwara 2006]
  - 計算的アプローチ
    - 局所重み分布計算アルゴリズムの提案
    - 符号の自己同型群を利用
  - 理論的アプローチ
    - C, C_{ex}, C_{even} の局所重み分布間の関係の解明
  - 結果として、n = 128 程度の拡大原始 BCH 符号や Reed-Muller 符号などについて分布を求めた

参考文献 （1 / 2）

[Agrell 1996] E. Agrell, “Voronoi regions for binary linear block codes,” *IEEE Trans. Inf. Theory*, Jan. 1996.

[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*, 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*, Apr. 2006.

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

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

[Maeda, Fujiwara 2001] M. Maeda and T. Fujiwara, “Weight distribution of the coset leaders of some Reed-Muller codes and BCH codes,” *IEICE Trans. Fund.*, May 2001.

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.

[安田, 安永, 藤原 2005] 安田 隆広, 安永 憲司, 藤原 融, ``Seguin下界の局所重み分布を用いた改善,‘’ 第28回情報理論とその応用シンポジウム予稿集, 2005年11月.

[Yasunaga, Fujiwara 2006] K. Yasunaga and T. Fujiwara, “Determination of the local weight distribution of binary linear block codes,” *IEEE Trans. Inf. Theory*, Oct. 2006.

[Yasunaga, Fujiwara 2008] K. Yasunaga and T. Fujiwara, “On correctable errors of binary linear codes,” submitted.

[Wu 1998] C.K. Wu,“On distribution of Boolean functions with nonlinearity $\leq 2^{n-2}$ ”, *Australasian Journal of Combinatorics*, Mar. 1998.

Applications of LWD

- Error performance analysis
  - P_e: Error probability of soft decision decoding on AWGN

$$\underbrace{\sum_{i=1}^{n} A_i(C)\, Q\left(\sqrt{i\frac{2E_b}{N_0}}\right)}_{\text{union bound}} \geq \underbrace{\sum_{i=1}^{n} L_i(C)\, Q\left(\sqrt{i\frac{2E_b}{N_0}}\right)}_{\text{a tighter bound}} \geq P_e$$

$$Q(x) = \int_x^{\infty} (2\pi)^{-1/2} \exp(-z^2/2)dz.$$

$A_i(C)$:= #(codewords with weight i in C)
$L_i(C)$:= #(zero neighbors with weight i in C)