線形ブロック符号の自己同型群と重み分布計算

OSAKA UNIVERSITY
Live Locally, Grow Globally

藤原　融
大阪大学　大学院情報科学研究科

目次

- 自己同型群
- 自己同型群の利用
- 線形符号の重み分布計算（これも自己同型群の利用）
- BCH符号とRM (Reed-Muller) 符号
- トレリスダイアグラムと自己同型群

必要な基礎知識

- 有限体 $\mathbf{GF}(2^m)$，群の基礎
- ハミング符号，BCH符号，それらの拡大符号の定義
- RM (Reed-Muller) 符号の定義

目次

- 自己同型群
  - 符号の記号位置置換
  - 自己同型群
  - ２元拡大原始狭義BCH符号とアフィン変換（自己同型部分群）
- 自己同型群の利用
- 線形符号の重み分布計算（これも自己同型群の利用）
- BCH符号とRM (Reed-Muller) 符号
- トレリスダイアグラムと自己同型群

置換

- 有限集合S上の置換：SからSへの全単射
  - S 上の置換の総数は $|S|!$
- 置換の例
  - $S = \{1,2,3\}$
  - 置換 π: $\pi(1) = 2, \pi(2) = 3, \pi(3) = 1$
  - これを $(2, 3, 1)$で表す
  - $\{1,2,3\}$上の置換の総数　$3! = 6$ 通り
    $(1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2), (3,2,1)$

符号の記号位置置換

- 符号長 n の符号 $C \subseteq V^n$
  - V：通信路記号の集合，V^n：長さ n の通信路記号列全体の集合

$$V^n \triangleq \{(v_1, v_2, \ldots, v_n) | v_1, v_2, \ldots, v_n \in V\}$$

- 符号 C の記号位置の集合 S　例えば $\{1,2,\ldots,n\}$ とする
- S上の置換 π と $\bar{v} = (v_1, v_2, \ldots, v_n) \in V^n$ に対して
  第 i 成分 v_i を第 $\pi(i)$ 成分に移動する置換

$$\pi(\bar{v}) \triangleq \left(v_{\pi^{-1}(1)}, v_{\pi^{-1}(2)}, \ldots, v_{\pi^{-1}(n)}\right)$$

- 符号 $C \in V^n$ の置換 π による記号位置置換した符号

$$\pi(C) \triangleq \{\pi(\bar{v}) | \bar{v} \in C\}$$

記号位置置換の例（その１）

- 符号C: (7,4)巡回ハミング符号の拡大符号
  - 生成多項式 $1+x+x^3$
- 置換 $\pi_1(x)$: $(1 \quad 2 \quad 3 \quad 5 \quad 4 \quad 7 \quad 8 \quad 6)$
- 生成行列で置換
  - 置換前：拡大ビットが先頭，低次の係数から高次へ
  - 置換後：RM符号となり， $\pi_1(C) \neq C$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}$$

記号位置置換の例
（その２ 拡大ビットを除く巡回置換）

- 符号C: (7,4)巡回ハミング符号の拡大符号
  - 生成多項式 $1+x+x^3$
- 置換 $\pi_2(x)$: $(1 \quad 8 \quad 2 \quad 3 \quad 4 \quad 5 \quad 6 \quad 7)$
- 生成行列で置換
  - 置換前：拡大ビットが先頭，低次の係数から高次へ
  - 置換後：同じ符号，すなわち $\pi_2(C) = C$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

符号Cの自己同型群 $\mathrm{Aut}(C)$
Automorphism Group of C

- 符号 C
- 符号 C の記号位置の集合 S
- 集合 S 上の置換全体の集合（群） Π

- 符号 C の自己同型群：次式を満たすΠ の部分集合

$$\mathrm{Aut}(C) \triangleq \{\pi | \pi(C) = C\}$$

  - $\mathrm{Aut}(C)$は群をなす
  - Permutation Group of C とも言う

置換の群

- 置換の積
  - $\pi_1.\pi_2 \in \Pi$に対して，その積 $\pi_2\pi_1$ ($\pi_1\pi_2$と書く方が一般的かも)

$$\pi_2\pi_1(x) \triangleq \pi_2(\pi_1(x))$$

- 置換全体の集合 Π は，積に関して群 (Group) をなす
  - 結合則：$\pi_3\pi_2\pi_1 = \pi_3(\pi_2\pi_1) = (\pi_3\pi_2)\pi_1$
  - 単位元 π_I ：$\pi\pi_I = \pi_I\pi = \pi$
    - $\pi_I(x) \triangleq x$ で定義される置換（恒等置換） π_I が単位元
  - 逆元 π^{-1}：$\pi^{-1}\pi = \pi\pi^{-1} = \pi_I$
    - 置換 π に対して，$\pi^{-1}\big(\pi(x)\big) = x$ で定義される置換 π^{-1} が逆元

符号の自己同型群（続き）
Automorphism Group of Code

- 一般に $\mathbf{Aut}(C)$ を求めることは難しい
- $\mathbf{Aut}(C)$ の部分群は，BCH符号やReed-Muller符号について知られている
  - 拡大原始狭義BCH符号：有限体上のアフィン変換（群）
  - Reed-Muller符号：ブール変数に対するアフィン変換（群）

アフィン変換

- ここでは，有限体 $\mathrm{GF}(2^m)$上で考える
- $S = \mathrm{GF}(2^m) = \{0,1,\alpha,\alpha^2,\alpha^3,\ldots,\alpha^{2^m-2}\}$, αは原始元
- アフィン変換

$$\pi(x) = ax + b, \qquad a, b \in \mathrm{GF}(2^m), a \neq 0$$

  - $b = 0$となるアフィン変換 $\pi(x) = ax$ は$\{\cancel{0},1,\alpha,\alpha^2,\alpha^3,\ldots,\alpha^{2^m-2}\}$上の巡回置換

アフィン変換の例

- 原始多項式 $x^3 + x + 1$で生成される有限体$\mathrm{GF}(2^3)$
- アフィン変換：$\pi(x) = \alpha x + 1$

変換前の記号位置			変換後の記号位置		
1	0	0	1	1	2
2	1	1	$\alpha + 1$	α^3	5
3	α	α	$\alpha^2 + 1$	α^6	8
4	α^2	α^2	α	α	3
5	α^3	$\alpha + 1$	$\alpha^2 + \alpha + 1$	α^5	7
6	α^4	$\alpha^2 + \alpha$	$\alpha^2 + \alpha$	α^4	6
7	α^5	$\alpha^2 + \alpha + 1$	α^2	α^2	4
8	α^6	$\alpha^2 + 1$	0	0	1

2元原始（狭義）BCH符号

- 符号長 $2^m - 1$.　… 原始
- 設計距離 δ
- 生成多項式の根 $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{\delta-1}$　　… 狭義
  - $\delta = 3$ の場合はハミング符号

BCH符号と有限体上のアフィン変換

- ２元拡大原始狭義BCH符号の自己同型群はアフィン変換を含む
  - 符号語のビットの並びは，拡大ビットが先頭，符号語多項式の低次の係数から高次の順とし
  - 記号位置は，先頭から $0,1,\alpha,\alpha^2,\alpha^3,\ldots,\alpha^{2^m-2}$

目次

- 自己同型群
- 自己同型群の利用
  - 置換群の推移性
  - 符号とその拡大符号の重み分布の関係
  - Reed-Muller Codes Achieve Capacity on Erasure Channel

    Information Theory Society Paper Award 2021

    Shrinivas Kudekar, Santhosh Kumar, Marco Mondelli, Henry D. Pfister, Eren Şaşoğlu, and Rüdiger Urbanke, IEEE Trans. Information Theory, vol.65, no.7, 2017
- 線形符号の重み分布計算（これも自己同型群の利用）
- BCH符号の重み分布計算の実現(インプリメント)
- BCH符号とRM (Reed-Muller) 符号
- トレリスダイアグラムと自己同型群

自己同型群の利用

- 対称性（置換前と置換後の不変性）の利用
  - 対称性＋推移性（Transitivity）
  - 対称性

置換群の推移性（Transitivity）

- 置換群 $G \subseteq \Pi$
- G が推移的 である (transitive)
  - 任意の $i,j \in S$ に対して, ある置換 $\pi \in G$があって,
$$\pi(i) = j$$
- G が2重に推移的である (doubly transitive)
  - 任意の $i_1, i_2, j_1, j_2 \in S$ $(i_1 \neq i_2, j_1 \neq j_2)$ に対して, ある置換 $\pi \in G$ があって,
$$\pi(i_1) = j_1, \qquad \pi(i_2) = j_2$$
  - （等価な定義）任意の $i_1, i_2, j_2 \in S$ $(i_1 \neq i_2)$に対して, ある置換 $\pi \in G$があって, $\pi(i_1) = i_1$, $\pi(i_2) = j_2$

アフィン変換の推移性

- 有限体上のアフィン変換は２重に推移的

$$\pi(x) = ax + b, \qquad a, b \in \mathrm{GF}(2^m), a \neq 0$$

（証明）任意の $i_1, i_2, j_1, j_2 \in S$ $(i_1 \neq i_2, j_1 \neq j_2)$ に対して，次式を満たす$a, b \in \mathrm{GF}(2^m)$が存在

$$ai_1 + b = j_1, \qquad ai_2 + b = j_2$$

対称性＋推移性の利用
符号Cとその拡大符号C_{ex}の重み分布

- まずは、重み分布とは

符号の重み分布

- 符号語の重み（ハミング重み）：0 でない成分数
  - 符号語(0,1,0,0,1,1) の重み3
- 符号 C の重み分布（符号は線形でなくてもよい）

  $(a_0, a_1, a_2, \ldots, a_n)$，$a_i$は符号$C$の重み$i$の符号語数
- 符号 C の重み分布多項式

$$W_C(x,y) = \sum_{i=0}^{n} a_i x^i y^{n-i}$$

符号Cとその拡大符号C_{ex}の重み分布

- 重み分布多項式

$$W_C(x,y)=\sum_{i=0}^{n} a_i x^i y^{n-i}, \qquad W_{C_{\mathrm{ex}}}(x,y)=\sum_{i=0}^{n+1} A_i x^i y^{n-i}$$

- 符号Cの重み分布から拡大符号C_{ex}の重み分布が求まる

$$A_{2j}=a_{2j-1}+a_{2j}$$
$$A_{2j-1}=0$$

- 逆はどうだろうか？

対称性＋推移性の利用
符号Cとその拡大符号C_{ex}の重み分布

- $\mathrm{Aut}(C_{\mathrm{ex}})$ が推移的 (transitive)ならば

$$a_{2j-1} = \frac{2jA_{2j}}{n+1}$$

- 従って

$$a_{2j} = A_{2j} - a_{2j-1} = \frac{(n+1-2j)}{n+1} A_{2j}$$

推移的 $\rightarrow a_{2j-1} = \frac{2jA_{2j}}{n+1}$ の証明

- 拡大符号C_{ex}の重み$2j$の符号語のリストを使う
  - リスト中の行の総数A_{2j}, 列の総数 $(n+1)$
  - リストに含まれる1の個数 $2jA_{2j}$
  - 各行の1の個数 $2j$
  - $\mathrm{Aut}(C_{\mathrm{ex}})$ が推移的ならば, 各列の1の個数も均一
    - 各列の1の個数 $\frac{2jA_{2j}}{n+1}$
    - この数は, パリティビットが1の符号語数

重み4の符号語

$(1,0,0,0,1,0,1,1)$
$(1,0,0,1,0,1,0,1)$
$(0,0,0,1,1,1,1,0)$
$(1,0,1,0,0,1,1,0)$
$(0,0,1,0,1,1,0,1)$
$(0,0,1,1,0,0,1,1)$
$(1,0,1,1,1,0,0,0)$
$(0,1,0,0,0,1,1,1)$
$(1,1,0,0,1,1,0,0)$
$(1,1,0,1,0,0,1,0)$
$(0,1,0,1,1,0,0,1)$
$(1,1,1,0,0,0,0,1)$
$(0,1,1,0,1,0,1,0)$
$(0,1,1,1,0,1,0,0)$

対称性＋推移性の利用

Reed-Muller Codes Achieve Capacity on Erasure Channel

- Extrinsic Information Transfer (EXIT) 関数
  - iビット目のEXIT関数　$h_i(\underline{p})$
  - $h_i(p) = h_i(\underline{p})\Big|_{\underline{p}=(p,\ldots,p)}$
- Transitive なら

$$h_j(p) = h_k(p)$$

- さらに, doubly transitiveなら

$$\left.\frac{\partial h_i\left(\underline{p}\right)}{\partial p_j}\right|_{\underline{p}=(p,\ldots,p)} = \left.\frac{\partial h_i\left(\underline{p}\right)}{\partial p_k}\right|_{\underline{p}=(p,\ldots,p)}$$

目次

- 自己同型群
- 自己同型群の利用
- 線形符号の重み分布計算（これも自己同型群の利用）
  - 部分符号によるコセット展開を用いた重み分布計算法
  - 実現法: Union-Findの利用
  - BCH符号の重み分布計算
- BCH符号とRM (Reed-Muller) 符号
- トレリスダイアグラムと自己同型群

部分符号によるコセット展開を用いた2元(n,k)線形符号Cの重み分布計算

- (n,k_0)線形部分符号 $C_0 \subseteq C$
- Cの生成行列

$$G \triangleq \begin{pmatrix} G_0 \\ G_1 \end{pmatrix}$$ ここでG_0は C_0の生成行列

- G_1を生成行列とする$(n,k-k_0)$符号をC_1とする
- Cの分割：$C/C_0 \triangleq \{\bar{v}+C_0 | \bar{v} \in C_1\}, |C/C_0| = 2^{k-k_0}$

$$C = \bigcup_{\bar{v} \in C_1} \bar{v} + C_0 = \bigcup_{D \in C/C_0} D$$

- $D \in C/C_0$は，C_0のコセット（剰余類）

部分符号によるコセット展開を用いた重み分布計算（続き）

- 符号 C の重み分布多項式

$$W_C(x,y) = \sum_{D \in C/C_0} W_D(x,y)$$

- C/C_0のコセットを重み分布が同じものでまとめると計算量が減るが，それは難しいので，コセットの重み分布が同じになる十分条件を考える

部分符号によるコセット展開を用いた重み分布計算（続きの続き）

- $D_1, D_2 \in \mathrm{C}/C_0$に対し $W_{D_1}(x,y) = W_{D_2}(x,y)$ となるための十分条件（重み分布の対称性（不変性））
  （十分条件）$D_1, D_2 \in C/C_0$に対して, $\pi(D_1) = D_2$となる置換がある
- 対象とする置換の集合としては $\mathrm{Aut}(C_0) \cap \mathrm{Aut}(C)$ （の部分群）とする
  - この集合に限定するのは， $\pi(D_1) \in \mathrm{C}/C_0$ となる十分条件
  - 部分符号 C_0 として同じクラスの符号を用いれば$\mathrm{Aut}(C_0) \cap \mathrm{Aut}(C)$ （の部分群）を求めやすい

部分符号によるコセット展開を用いた重み分布計算（続きの続き）

- C/C_0の細分
  - $D_1, D_2 \in C/C_0$に対して, $\pi(D_1) = D_2$となる置換$\pi \in \mathrm{Aut}(C_0) \cap \mathrm{Aut}(C)$があれば, D_1, D_2は同じ組
  - 置換群に基づく同値類分割に相当
- 各同値類の代表元の重み分布とその同値類に含まれるコセットの個数が求まれば，符号C の重み分布が得られる

Union-Find

- 集合操作のためのデータ構造
  - U: 全体集合
  - 通常，各集合は有向木で表現され，初期状態ではUの一つの要素だけからなる集合の族が存在するものとする
- 操作は次の２つ
  - $\mathrm{Union}(T_1, T_2)$: ２つの集合 T_1, T_2 をひとつにまとめる
    ２つの木 T_1, T_2 をひとつの木に統合
  - $\mathrm{Find}(x)$: $x \in U$ が属している集合を返す
    $x \in X$ が属している木の根を求める

Union-Findを用いた コセットの同値類分割

- Union-Find における全体集合$U = C/C_0$

  - for $\pi \in \mathrm{Aut}(C_0) \cap \mathrm{Aut}(C)$の部分群
  - for $D \in C/C_0$
  - $\mathrm{Union}(\mathrm{Find}(D), \mathrm{Find}(\pi(D)))$

Union-Findを用いた コセットの同値類分割（続き）

- $\mathrm{Aut}(C_0) \cap \mathrm{Aut}(C)$の部分群が有限体上のアフィン変換の場合
  - $\pi_1(x) = \alpha \mathrm{X}, \pi_2(x) = \alpha \mathrm{X} + 1$ だけを考えればよい
    考えるべき置換の総数が　$2^m(2^m - 1) \rightarrow 2$
  - 一つの置換だけにはできない

新井, 藤原, "符号長512, 1024の2元拡大原始BCH符号における部分符号の剰余類分割と重み分布計算への応用," 信学技報, IT2021-15 (2021-07).

- for $\pi \in$ ~~$\mathrm{Aut}(C_0) \cap \mathrm{Aut}(C)$~~ $\{\pi_1, \pi_2\}$
- for $D \in C/C_0$
- $\mathrm{Union}(\mathrm{Find}(D), \mathrm{Find}(\pi(D)))$

BCH(256,187)の重み分布

- $C = \mathrm{BCH}^{\perp}(256,187)$: (256,69)符号
- $C_0 = \mathrm{BCH}^{\perp}(256,215)$: (256,41)符号
- $|C/C_0| = 2^{28}$, 代表コセットの個数 8,224
- 計算時間 2.35×10^6秒/20=1.36日
  - Intel Xeon CPU E5-2630 v4 @ 2.20 GHz
  - 10×2 cores, Popcnt + AVX2

McWilliams の等式

- C：2元線形符号
- $C^{\perp}$：符号Cの双対符号

$$W_{C^{\perp}}(x,y) = \frac{1}{|C|} W_C(x+y, x-y)$$

講演者らのBCH符号の重み分布計算

- 符号長128
  - 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, pp.1364–1371 (1997-07).
- 符号長256
  - T. Fujiwara, and T. Kasami, “The Weight Distributions of (256, k) Extended Binary Primitive BCH Codes with $k \leq 63$ and $k \geq 207$,” IEICE Technical Report, IT97-46 (1997-09).
  - T. Fujiwara, T. Kusaka, “The Weight Distributions of the (256, k) Extended Binary Primitive BCH Codes with k = 71, 187, 191, and 199”, IEICE Technical Report, IT2019-5 (2019-05).
  - T. Fujiwara, T. Kusaka, “The Weight Distributions of the (256, k) Extended Binary Primitive BCH Codes with k ≦ 71 and k ≧ 187,” IEICE Trans. Fundamentals, Vol.E104-A, No.9, pp.1321-1328 (2021-09).
- 符号長512, 1024（計算時間の評価）
  - 新井 美音, 藤原 融, "符号長512, 1024の2元拡大原始BCH符号における部分符号の剰余類分割と重み分布計算への応用," 電子情報通信学会技術研究報告, IT2021-15, pp. 1-5 (2021-07).

現在、重み分布計算可能なBCH符号

- 2元原始狭義BCH符号の拡大符号
  - 符号長 128 以下の全ての符号
  - 符号長 256　$k \leq 71, k \geq 187\ (n-k \leq 69)$
  - 符号長 512　$k \leq 58, k \geq 448\ (n-k \leq 68)$
  - 符号長 1024　$k \leq 66, k \geq 953\ (n-k \leq 71)$

目次

- 自己同型群
- 自己同型群の利用
- 線形符号の重み分布計算（これも自己同型群の利用）
- BCH符号とRM (Reed-Muller) 符号
- トレリスダイアグラムと自己同型群

Reed-Muller符号のパラメータ

- $\mathrm{RM}(m, r)$: r-th order RM code of length 2^m
  - $0 \leq r \leq m$
  - 符号長 $n = 2^m$
  - 情報記号数 $k = 1 + m + \binom{m}{2} + \binom{m}{3} + \cdots + \binom{m}{r}$
  - 最小距離 2^{m-r}
- $\mathrm{RM}(m, 0) = \{\overline{0}, \overline{1}\}$
- $\mathrm{RM}(m, m) = V^{2^m}$

m変数のブール多項式と成分数2^mのベクトル

- m変数のブール多項式
  - 加算は論理関数の排他的論理和 XOR (eXclusive OR)
- ブール多項式とベクトルの対応
  - 3変数のブール多項式$x_1 + x_2 + x_3$に対応するベクトル
    $(0,1,1,0,1,0,0,1)$

記号位置	0	1	2	3	4	5	6	7
x_3	0	0	0	0	1	1	1	1
x_2	0	0	1	1	0	0	1	1
x_1	0	1	0	1	0	1	0	1
$x_1 + x_2 + x_3$	0	1	1	0	1	0	0	1

Reed-Muller符号

- $\mathrm{RM}(m,r)$：r次以下のブール多項式に対応するベクトルの集合
  - 0次のブール多項式 0, 1
  - 1次のブール多項式 $x_1, x_2, \ldots, x_m$
  - 2次のブール多項式多項式 $x_1x_2, x_2x_3, \ldots$
- 情報記号数 $k = 1 + m + \binom{m}{2} + \binom{m}{3} + \cdots + \binom{m}{r}$

Reed-Muller符号の自己同型群の部分群

- GL (General Linear Group)

$$\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}, \qquad A\text{は}m \times m\text{正則行列}$$

- GA (General Affine Group)

$$\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} = A \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

巡回 Reed-Muller 符号

- $(\mu, 1)$-th order EG (Euclidean Geometry) 符号
- EG符号は，巡回符号
- その拡大符号が（通常の）Reed-Muller 符号と等価

Reed-Muller符号：巡回と通常

巡回 記号位置	有限体の元			RM 記号位置
1	0	0	000	1
2	1	1	001	2
3	α	α	010	3
4	α^2	α^2	100	5
5	α^3	$\alpha+1$	011	4
6	α^4	$\alpha^2+\alpha$	110	7
7	α^5	$\alpha^2+\alpha+1$	111	8
8	α^6	α^2+1	101	6

原始多項式 x^3+x+1で生成される有限体$\mathrm{GF}(2^3)$

Netsting habit

- 符号長 2^m
  - $\mathcal{B}(d)$: 設計距離 d の原始狭義BCH符号の拡大符号
  - $\mathcal{R}(r)$: RM符号　次数 r
- $\mathcal{B}(d+1) \subseteq \mathcal{B}(d), \mathcal{B}^{\perp}(d) \subseteq \mathcal{B}^{\perp}(d+1)$
- $\mathcal{R}(r) \subseteq \mathcal{R}(r+1), \mathcal{R}^{\perp}(r+1) \subseteq \mathcal{R}^{\perp}(r)$

- $\mathcal{R}(r) \subseteq \mathcal{B}(2^{m-r}-1)$

MacWilliams & Sloane pp.384-385

Houの結果
$\mathrm{RM}(m,r)/\mathrm{RM}(m,r-1)$

- $\mathrm{RM}(m,r)/\mathrm{RM}(m,r-1)$の代表コセットの数
  （次数差1なので，GL, GAで共通）
- $\mathrm{RM}(m,3)/\mathrm{RM}(m,2)$ の代表コセット （$m \leq 8$）
- コセットが与えられて，代表コセットの求め方（$m \leq 8$）

X. Hou, “GL(m, 2) Acting on $R(r, m)/R(r-1, m)$,” Discrete Mathematics, Vol.149, pp.99–122, 1996.

$m = 7$の場合

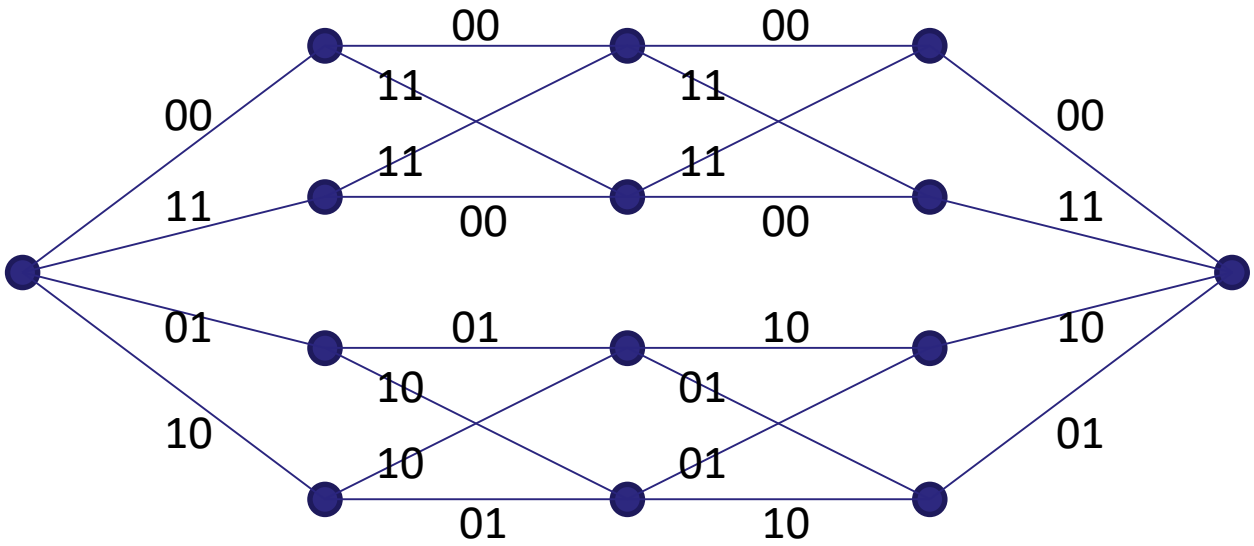
T. Kasami, T. Fujiwara, and Y. Desaki, “The Weight Distributions of Cosets of the Second-Order Reed-Muller Code of Length 128 in the Third-Order Reed-Muller Code of Length 128,” IEICE Trans. Fundamentals, Vol.E79-A, No.4, pp.600–608, Apr. 1996.

目次

- 自己同型群
- 自己同型群の利用
- 線形符号の重み分布計算（これも自己同型群の利用）
- BCH符号とRM (Reed-Muller) 符号
- トレリスダイアグラムと自己同型群

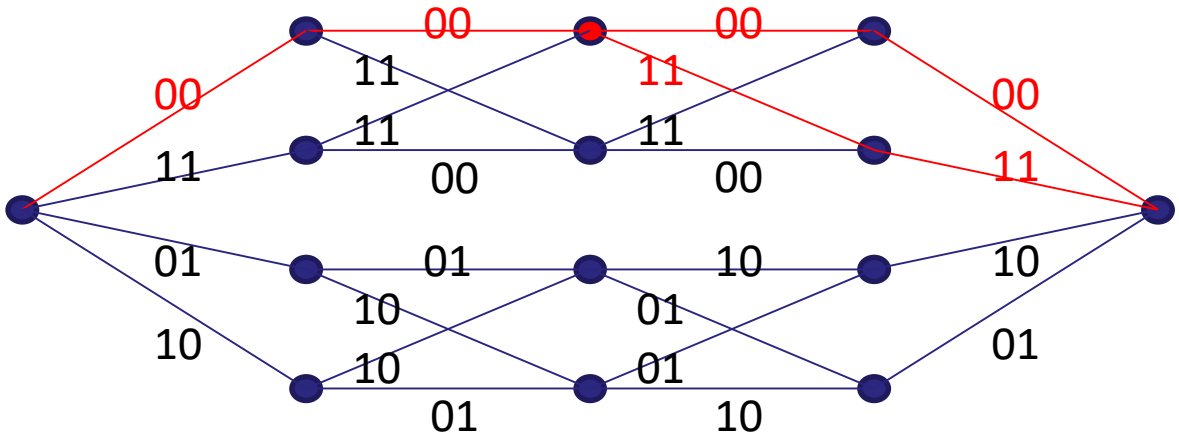
トレリスダイアグラム

- RM(3,1)のトレリスダイアグラム



トレリスの構造と部分符号

- 部分符号：Future subcode, Past subcode
  - Future subcode. その時刻まで all 0 である符号語の集合
  - Past subcode　　その時刻から all 0となる符号語の集合



トレリスと自己同型群

- 符号語の記号位置を逆順に置換
  - RM符号では，ブール変数上のアフィン変換で入れ替わる
  - これでトレリスの左右の対称性が成り立つことがわかる
    Past subcode = Future subcodeの逆順

まとめ

- 自己同型群
- 自己同型群の利用
  - 符号とその拡大符号の重み分布の関係
  - Reed-Muller Codes Achieve Capacity on Erasure Channel
- ２元拡大原始狭義BCH符号の重み分布計算

- Open Problem
  - $\mathrm{RM}(m,4)/\mathrm{RM}(m,2)$ の分類