アルゴリズム論特論 （塩田）

2016 年 7 月 25 日

1. アダマール符号

```
--------------------
Code Length = 2
--------------------
Hadamard Matrix:
 1 1
 1-1

Code Words:
 1 1
 1 0
 0 0
 0 1

Minimal Distance = 1

--------------------
Code Length = 4
--------------------
Hadamard Matrix:
 1 1 1 1
 1-1 1-1
 1 1-1-1
 1-1-1 1

Code Words:
 1 1 1 1
 1 0 1 0
 1 1 0 0
 1 0 0 1
 0 0 0 0
 0 1 0 1
 0 0 1 1
 0 1 1 0

Minimal Distance = 2

--------------------
Code Length = 8
--------------------
Hadamard Matrix:
 1 1 1 1 1 1 1 1
 1-1 1-1 1-1 1-1
 1 1-1-1 1 1-1-1
 1-1-1 1 1-1-1 1
 1 1 1 1-1-1-1-1
 1-1 1-1-1 1-1 1
 1 1-1-1-1-1 1 1
 1-1-1 1-1 1 1-1

Code Words:
 1 1 1 1 1 1 1 1
 1 0 1 0 1 0 1 0
 1 1 0 0 1 1 0 0
 1 0 0 1 1 0 0 1
 1 1 1 1 0 0 0 0
 1 0 1 0 0 1 0 1
 1 1 0 0 0 0 1 1
 1 0 0 1 0 1 1 0
 0 0 0 0 0 0 0 0
 0 1 0 1 0 1 0 1
 0 0 1 1 0 0 1 1
 0 1 1 0 0 1 1 0
 0 0 0 0 1 1 1 1
 0 1 0 1 1 0 1 0
 0 0 1 1 1 1 0 0
 0 1 1 0 1 0 0 1

Minimal Distance = 4

--------------------
Code Length = 16
--------------------
Hadamard Matrix:
 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
 1-1 1-1 1-1 1-1 1-1 1-1 1-1 1-1
 1 1-1-1 1 1-1-1 1 1-1-1 1 1-1-1
 1-1-1 1 1-1-1 1 1-1-1 1 1-1-1 1
 1 1 1 1-1-1-1-1 1 1 1 1-1-1-1-1
 1-1 1-1-1 1-1 1 1-1 1-1-1 1-1 1
 1 1-1-1-1-1 1 1 1 1-1-1-1-1 1 1
 1-1-1 1-1 1 1-1 1-1-1 1-1 1 1-1
 1 1 1 1 1 1 1 1-1-1-1-1-1-1-1-1
 1-1 1-1 1-1 1-1-1 1-1 1-1 1-1 1
 1 1-1-1 1 1-1-1-1-1 1 1-1-1 1 1
 1-1-1 1 1-1-1 1-1 1 1-1-1 1 1-1
 1 1 1 1-1-1-1-1-1-1-1-1 1 1 1 1
 1-1 1-1-1 1-1 1-1 1-1 1 1-1 1-1
 1 1-1-1-1-1 1 1-1-1 1 1 1 1-1-1
 1-1-1 1-1 1 1-1-1 1 1-1 1-1-1 1

Code Words:
 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0
 1 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1
 1 1 1 1 0 0 0 0 1 1 1 1 0 0 0 0
 1 0 1 0 0 1 0 1 1 0 1 0 0 1 0 1
 1 1 0 0 0 0 1 1 1 1 0 0 0 0 1 1
 1 0 0 1 0 1 1 0 1 0 0 1 0 1 1 0
 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0
 1 0 1 0 1 0 1 0 0 1 0 1 0 1 0 1
 1 1 0 0 1 1 0 0 0 0 1 1 0 0 1 1
 1 0 0 1 1 0 0 1 0 1 1 0 0 1 1 0
 1 1 1 1 0 0 0 0 0 0 0 0 1 1 1 1
 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0
 1 1 0 0 0 0 1 1 0 0 1 1 1 1 0 0
 1 0 0 1 0 1 1 0 0 1 1 0 1 0 0 1
 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1
 0 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1
 0 1 1 0 0 1 1 0 0 1 1 0 0 1 1 0
 0 0 0 0 1 1 1 1 0 0 0 0 1 1 1 1
 0 1 0 1 1 0 1 0 0 1 0 1 1 0 1 0
 0 0 1 1 1 1 0 0 0 0 1 1 1 1 0 0
 0 1 1 0 1 0 0 1 0 1 1 0 1 0 0 1
 0 0 0 0 0 0 0 0 1 1 1 1 1 1 1 1
 0 1 0 1 0 1 0 1 1 0 1 0 1 0 1 0
 0 0 1 1 0 0 1 1 1 1 0 0 1 1 0 0
 0 1 1 0 0 1 1 0 1 0 0 1 1 0 0 1
 0 0 0 0 1 1 1 1 1 1 1 1 0 0 0 0
 0 1 0 1 1 0 1 0 1 0 1 0 0 1 0 1
 0 0 1 1 1 1 0 0 1 1 0 0 0 0 1 1
 0 1 1 0 1 0 0 1 1 0 0 1 0 1 1 0

Minimal Distance = 8
```

2. ブロックデザイン

- 集合 V と、V の部分集合いくつかから成る集合 $\mathbf{B}$ が次の条件を満たすとき $t-(m,k,\lambda)$ デザインと呼ぶ：
  (a) $\sharp V = m$
  (b) $\sharp B = k \quad (\ \forall B \in \mathbf{B}\ )$
  (c) t 個の $v \in V$ を含む $B \in \mathbf{B}$ は必ず λ 個ある

- $V = \{\, v_1, \cdots, v_m \,\}$, $\mathbf{B} = \{\, B_1, \cdots, B_n \,\}$ と番号付けて、デザイン $(V, \mathbf{B})$ の接続行列 $N = (n_{ij})$ を次で定める：

$$n_{ij} = \begin{cases} 1 & v_i \in B_j \text{ のとき} \\ 0 & v_i \notin B_j \text{ のとき} \end{cases}$$

- ブロックデザインの良い対称性が接続行列 N にも反映されているので、N から性能の良い符号を構成することができる：
  (1) N の行ベクトル達を符号語とする符号
  (2) N の列ベクトル達を符号語とする符号
  (3) N を検査行列とする二進線形符号
  (4) N から生成行列作った二進線形符号　etc.

3. 有限幾何

二元体 $\mathbf{F}_2$ を座標に用いて幾何学を展開するとブロックデザインを構成し易い。

- $\mathbf{F}_2$ 上の xy-平面で $V = \{$ 点たち $\}$, $\mathbf{B} = \{$ 直線たち $\}$ の場合

  ◦ $V = \{\, v_1,\ v_2,\ v_3,\ v_4 \,\}$
  $v_1 = 00, \quad v_2 = 10, \quad v_3 = 01, \quad v_4 = 11$

  ◦ $\mathbf{B} = \{\, B_1,\ B_2,\ B_3,\ B_4,\ B_5,\ B_6 \,\}$
  $B_1 = \{\, v_1, v_3 \,\} : x = 0,$
  $B_2 = \{\, v_2, v_4 \,\} : x = 1,$
  $B_3 = \{\, v_1, v_2 \,\} : y = 0,$
  $B_4 = \{\, v_3, v_4 \,\} : y = 1,$
  $B_5 = \{\, v_1, v_4 \,\} : x + y = 0,$
  $B_6 = \{\, v_2, v_3 \,\} : x + y = 1$

  ◦ $N = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$

- $\mathbf{F}_2$ 上の xyz-空間で $V = \{$ 点たち $\}$, $\mathbf{B} = \{$ 直線たち $\}$ の場合
  - $V = \{\, v_1,\, v_2,\, v_3,\, v_4\, v_5,\, v_6,\, v_7,\, v_8 \,\}$
    $v_1 = 000, \quad v_2 = 100, \quad v_3 = 010, \quad v_4 = 110,$
    $v_5 = 001, \quad v_6 = 101, \quad v_7 = 011, \quad v_8 = 111$
  - $\mathbf{B} = \{\, B_1,\, B_2, \cdots, B_{28} \,\}$
    $B_1 = \{\, v_1, v_2 \,\}, \quad B_2 = \{\, v_1, v_3 \,\}, \quad B_3 = \{\, v_1, v_4 \,\}, \quad B_4 = \{\, v_1, v_5 \,\},$
    $B_5 = \{\, v_1, v_6 \,\}, \quad B_6 = \{\, v_1, v_7 \,\}, \quad B_7 = \{\, v_1, v_8 \,\}, \quad B_8 = \{\, v_2, v_3 \,\},$
    $B_9 = \{\, v_2, v_4 \,\}, \quad B_{10} = \{\, v_2, v_5 \,\}, \quad B_{11} = \{\, v_2, v_6 \,\}, \quad B_{12} = \{\, v_2, v_7 \,\},$
    $B_{13} = \{\, v_2, v_8 \,\}, \quad B_{14} = \{\, v_3, v_4 \,\}, \quad B_{15} = \{\, v_3, v_5 \,\}, \quad B_{16} = \{\, v_3, v_6 \,\},$
    $B_{17} = \{\, v_3, v_7 \,\}, \quad B_{18} = \{\, v_3, v_8 \,\}, \quad B_{19} = \{\, v_4, v_5 \,\}, \quad B_{20} = \{\, v_4, v_6 \,\},$
    $B_{21} = \{\, v_4, v_7 \,\}, \quad B_{22} = \{\, v_4, v_8 \,\}, \quad B_{23} = \{\, v_5, v_6 \,\}, \quad B_{24} = \{\, v_5, v_7 \,\},$
    $B_{25} = \{\, v_5, v_8 \,\}, \quad B_{26} = \{\, v_6, v_7 \,\}, \quad B_{27} = \{\, v_6, v_8 \,\}, \quad B_{28} = \{\, v_7, v_8 \,\}$
  - $N = \begin{pmatrix} 1&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&0&0&0&0&1&0&0&0&0&0&1&1&1&1&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&0&0&0&0&1&0&0&0&0&1&0&0&0&0&1&1&1&1&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&0&1&1&1&0&0&0 \\ 0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&1&0&0&1&1&0 \\ 0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&1&0&1&0&1 \\ 0&0&0&0&0&0&1&0&0&0&0&0&1&0&0&0&0&1&0&0&0&1&0&0&1&0&1&1 \end{pmatrix}$

- $\mathbf{F}_2$ 上の xyz-空間で $V = \{$ 点たち $\}$, $\mathbf{B} = \{$ 平面たち $\}$ の場合
  - $V = \{\, v_1,\, v_2,\, v_3,\, v_4\, v_5,\, v_6,\, v_7,\, v_8 \,\}$
    $v_1 = 000, \quad v_2 = 100, \quad v_3 = 010, \quad v_4 = 110,$
    $v_5 = 001, \quad v_6 = 101, \quad v_7 = 011, \quad v_8 = 111$
  - $\mathbf{B} = \{\, B_1,\, B_2, \cdots, B_{14} \,\}$
    $B_1 : x = 0, \quad B_2 : x = 1, \quad B_3 : y = 0,$
    $B_4 : y = 1, \quad B_5 : z = 0, \quad B_6 : z = 1,$
    $B_7 : x + y = 0, \quad B_8 : x + y = 1, \quad B_9 : y + z = 0,$
    $B_{10} : y + z = 1, \quad B_{11} : z + x = 0, \quad B_{12} : z + x = 1,$
    $B_{13} : x + y + z = 0, \quad B_{14} : x + y + z = 1$
  - $N = \begin{pmatrix} 1&0&1&0&1&0&1&0&1&0&1&0&1&0 \\ 0&1&1&0&1&0&0&1&1&0&0&1&0&1 \\ 1&0&0&1&1&0&0&1&0&1&1&0&0&1 \\ 0&1&0&1&1&0&1&0&0&1&0&1&1&0 \\ 1&0&1&0&0&1&1&0&0&1&0&1&0&1 \\ 0&1&1&0&0&1&0&1&0&1&1&0&1&0 \\ 1&0&0&1&0&1&0&1&1&0&0&1&1&0 \\ 0&1&0&1&0&1&1&0&1&0&1&0&0&1 \end{pmatrix}$

- $\mathbf{F}_2$ 上の xyz-空間で $V = \{\, O$ 以外の点たち $\}$, $\mathbf{B} = \{\, O$ を通る平面たち $\}$ の場合

  - $V = \{\, v_1,\, v_2,\, v_3,\, v_4\, v_5,\, v_6,\, v_7 \}$
    $v_1 = 100, \quad v_2 = 010, \quad v_3 = 110, \quad v_4 = 001,$
    $v_5 = 101, \quad v_6 = 011, \quad v_7 = 111$
  - $\mathbf{B} = \{\, B_1,\, B_2, \cdots, B_7 \}$
    $B_1 : x = 0, \qquad B_2 : y = 0, \qquad B_3 : z = 0,$
    $B_4 : x + y = 0, \qquad B_5 : y + z = 0, \quad B_6 : z + x = 0,$
    $B_7 : x + y + z = 0$
  - $N = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$

4. 使用例

- 符号長 32 のアダマール符号は 1971 年に発射された火星探査衛星マリナー 9 号で利用された。
- 12-(11,6,3) デザインの接続行列から第 2 節 (4) の方法で構成される符号長 24 のゴレイ符号は、1977 年に発射された宇宙探査衛星ボイジャー 1 号、ボイジャー 2 号で利用されている。