Proof of Linearity of Hadamard Code given by Sylvester Matrices

Mitsuru Takigahira

証明

数学的帰納法で示す。
$n = 2^m$ のとき

- Sylvester Matrix を S_m
- S_m から生成される Hadamard Code を C_m
- $C_m = \{\mathbf{u}_1^m, \bar{\mathbf{u}}_1^m, \ldots, \mathbf{u}_{2^m}^m, \bar{\mathbf{u}}_{2^m}^m\}$

と表記することにする

証明 (1/3)

$m = 0$ のとき

$S_m = \left(1\right)$ or $\left(-\right)$ より、$C_0 = \{\left(1\right), \left(0\right)\}$
よって、C_0 は $\left(1\right)$ を基底として線形になり、C_0 は線形符号。

帰納法の仮定

$m = k \geq 0$ のとき C_k が線形になると仮定する。
このとき C_k は 2^{k+1} 個の符号 $\{\mathbf{u}_1^k, \bar{\mathbf{u}}_1^k, \ldots, \mathbf{u}_{2^k}^k, \bar{\mathbf{u}}_{2^k}^k\}$ を持ち、
これらは $k+1$ 個の基底 $\mathbf{e}_1^k, \ldots, \mathbf{e}_{k+1}^k$ をもち、線形である。

証明 (2/3)

S_{k+1} から作られる符号の線形性

補題 6.24 より $S^{k+1} = \begin{pmatrix} S_k & S_k \\ S_k & -S_k \end{pmatrix}$ なので、C_{k+1} に含まれる符号は
$1 \le i \le 2^k$ に対して、 $(\mathbf{u}_i^k, \mathbf{u}_i^k), (\bar{\mathbf{u}}_i^k, \bar{\mathbf{u}}_i^k), (\mathbf{u}_i^k, \bar{\mathbf{u}}_i^k), (\bar{\mathbf{u}}_i^k, \mathbf{u}_i^k)$ の形になる。
帰納法の仮定から、
$1 \le i \le 2^k$ のとき $\mathbf{u}_i^k, \bar{\mathbf{u}}_i^k$ はそれぞれ $\mathbf{e}_1^k, \dots, \mathbf{e}_{k+1}^k$ の線型結合で表せるので、
$1 \le i \le k+1$ のもと $\mathbf{e}_i^{k+1} = (\mathbf{e}_i^k, \mathbf{e}_i^k)$ とおけば、
$(\mathbf{u}_i^k, \mathbf{u}_i^k), (\bar{\mathbf{u}}_i^k, \bar{\mathbf{u}}_i^k)$ の形の符号は $\mathbf{e}_1^{k+1}, \dots, \mathbf{e}_{k+1}^{k+1}$ の線型結合で表せる。

証明 (3/3)

S^{k+1} から作られる符号の線形性

更に、C_k は線形符号なので、$\mathbf{0} = (0 \dots 0)$ を含むため、
C_{k+1} は $(\mathbf{0}, \bar{\mathbf{0}}) = (0 \dots 01 \dots 1)$ を含み、これは $(\mathbf{u}_i^k, \mathbf{u}_i^k), (\bar{\mathbf{u}}_i^k, \bar{\mathbf{u}}_i^k)$ の形ではない。
$\mathbf{e}_{k+2}^{k+1} = (0 \dots 01 \dots 1)$ とおくと、$1 \le i \le 2^k$ に対し
$\mathbf{e}_{k+2}^{k+1} + (\bar{\mathbf{u}}_i^k, \bar{\mathbf{u}}_i^k) = (\bar{\mathbf{u}}_i^k, \mathbf{u}_i^k)$ かつ $\mathbf{e}_{k+2}^{k+1} + (\mathbf{u}_i^k, \mathbf{u}_i^k) = (\mathbf{u}_i^k, \bar{\mathbf{u}}_i^k)$
よって、C_k が線形のとき C_{k+1} は $\mathbf{e}_1^{k+1}, \dots, \mathbf{e}_{k+2}^{k+1}$ を基底として線形となる。

以上から、数学的帰納法により、Sylvester Matrix から作られる Hadamard Code は線形であることが示された。