Lecture 3

Note Title 1/4/2008

k-D subspace of $\{0,1\}^n$: Code

↳ denoted (n,k) code

n: block length, k: dimension/message length

Dual of an (n,k) Code → $(n, n-k)$ Code

Examples : $n = 6$

1) $k = 0$ $(6,0)$ Code $\{000000\}$

Dual $(6,6)$ Code $\{0,1\}^6$ "uncoded"

2) $k = 1$ $(6,1)$ codes → 63 of them?

→ $G_1 = [100000]$ Code = $\{000000, 100000\}$

→ $G_2 = [010000]$ Code = $\{000000, 010000\}$

→ $G_3 = [001001]$ Code = $\{000000, 001001\}$

→ Duals: 1) $C = \{000000, 100000\}$

$C^{\perp} = ?$

$G = [1 \mid 00000]$ $\quad H = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} I_5$

Rows of H: form a basis for $C^{\perp}$.

2) $C = \{000000, 010000\}$ $\quad G = [0 \mid 10000]$

→ Undo column swaps to get exact dual.

$G_S = [1 \mid 00000]$

$H_S =$ [,]

$k=2$: $(6,2)$ codes

Example: $G = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 \end{bmatrix}$

$C = \{000000, 110000, 111100, 001100\}$

$G_s = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$ (2 rows, 6 columns)

$H_s = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$ (4 rows, 6 columns)

$G_s = [I_2 \mid P]$

$H = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

$C^{\perp} = \langle 110000, 001100, 000010, 000001 \rangle$

$C \cap C^{\perp} = C$ Surprise!! $C \subseteq C^{\perp}$

"self-orthogonal"

→ Code this in C/MATLAB

$k=3$: $(6,3)$ codes

$\sum_x$: $G = \begin{bmatrix} 1&1&0&0&0&0 \\ 0&0&1&1&0&0 \\ 0&0&0&0&1&1 \end{bmatrix}$ rank$(G)=3$

$H = \begin{bmatrix} \text{"} & \text{"} & \text{"} \end{bmatrix}$ $C = C^{\perp}$ "self-dual"

$k=2$: $(6,2)$ Code with $G = \begin{bmatrix} 1&0&1&1&1&0 \\ 0&1&0&1&1&1 \end{bmatrix}$

$C = \{000000, 101110, 010111, 111001\}$

$H = \begin{bmatrix} 1&0&1&0&0&0 \\ 1&1&0&1&0&0 \\ 1&1&0&0&1&0 \\ 0&1&0&0&0&1 \end{bmatrix}$

$[1\,1\,0\,1\,0\,0] \in C^{\perp}$

$\underline{c} = [c_0\, c_1\, c_2\, c_3\, c_4\, c_5]$

$c_0 + c_1 + c_3 = 0$ ← parity check

$c_0 + c_2 = 0$

$c_0 + c_1 + c_4 = 0$

$c_1 + c_5 = 0$

→ Every nonzero vector in $C^\perp$ is a parity-check for C.

Ex: $G = \begin{bmatrix} 0&1&0&1&0&1&0&1 \\ 0&0&1&1&0&0&1&1 \\ 0&0&0&0&1&1&1&1 \\ 1&1&1&1&1&1&1&1 \end{bmatrix}$ $n = 8$, $k = 4$

$G = H$

→ $G H^T = 0$

→ $G G^T = 0 \Rightarrow C \subseteq C^\perp$

→ $C \subseteq C^\perp$ & $k = n/2 \Rightarrow C = C^\perp$