Lecture 2

Note Title 1/3/2008

Linear Encoder

"Generator" $\underline{c} = \underline{m}\, G$ → $k \times n$

$\underline{c}$: n bit, $\underline{m}$: k bits

"Parity-check"

Ex:

$$p_0 = m_0 + m_1 \qquad p_0 + m_0 + m_1 = 0$$
$$p_1 = m_1 + m_2 \qquad p_1 + m_1 + m_2 = 0$$
$$p_2 = m_0 + m_2 \qquad p_2 + m_0 + m_2 = 0$$

Parity-check matrix H: $H\,\underline{c}^T = \underline{0}$ for all codewords $\underline{c}$.

$$\begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} m_0 \\ m_1 \\ m_2 \\ p_0 \\ p_1 \\ p_2 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

H for example code

In general, $G = [I_k \; P]$

$$H = [P^T \; I_{n-k}]$$

Vector space view

$\{0,1\}^n$: n-D vector space over $\{0,1\}$

Addition: bitwise XOR

Trivial scalar multiplication

Basis : canonical basis.

Subspaces : define using basis.

Inner product : $\underline{x} \cdot \underline{y} = \langle \underline{x}, \underline{y} \rangle = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n \mod 2.$

$\longrightarrow$ Difference from $\mathbb{R}^n$.

$\underline{x} \cdot \underline{x} = 0 \not\Rightarrow \underline{x} = \underline{0}.$

Dual spaces : S : m-D subspace of $\{0,1\}^n$

Dual $S^\perp = \{ \underline{x} \in \{0,1\}^n : \underline{x} \cdot \underline{y} = 0 \ \forall \underline{y} \in S \}.$

$S^\perp$ subspace of $\dim = n - m$

$\longrightarrow$ Difference from $\mathbb{R}^n$

$\rightarrow S \cap S^\perp$ can be non-trivial

$\rightarrow S = S^\perp$ is possible!!

Example: $n = 6$

$$S = \langle \underbrace{100001}_{u_1}, \underbrace{100010}_{u_2} \rangle$$

$$= \{ a u_1 + b u_2 : a, b \in \{0,1\} \}$$

$$= \{ 000000, 100001, 100010, 000011 \}$$

Generator matrix:

$$\text{Codeword } \underline{c} = \underline{m} G$$

$$\text{Code} = \{ \underline{c} = \underline{m} G : \underline{m} \in \{0,1\}^k \}$$

$$G = \underset{k}{\left[\underbrace{I_k}_{n} \;\vdots\; P \right]} = \begin{bmatrix} \leftarrow g_1 \rightarrow \\ \leftarrow g_2 \rightarrow \\ \vdots \\ \leftarrow g_k \rightarrow \end{bmatrix}$$

linearly independent

$$\underline{c} = m_0 \underline{g}_1 + m_1 \underline{g}_2 + \cdots + m_{k-1} \underline{g}_k \;, \quad m_i \in \{0, 1\}.$$

Code: subspace $\langle \underline{g}_1, \underline{g}_2, \ldots, \underline{g}_k \rangle$

- general definition of a linear code.
- sum of two codewords is another codeword.