8/30 応用数学特論II

Proposition

For a linear code $\mathcal{C}$, the minimum weight of the code is the minimum distance.

Proof: Let $v, w \in \mathcal{C}$.

$$d(v, w) = d(v - w, 0)$$
$$= wt(v - w).$$

$$v = (v_1, \boxed{v_2}, \ldots, v_n)$$
$$w = (w_1, \boxed{w_2}, \ldots, w_n)$$

$v_2 - w_2 = 0$ iff $w_2 = v_2$

($\Leftarrow$) If d is the min distance of $\mathcal{C}$.

there must exist a codeword of $wt = d$.

($\Rightarrow$) If there exists a codeword x of $wt = d$.

then $d(x, 0) = d$.

Proposition

Let V be a vector space of dimension k over $\mathbb{F}_q$, then $|V| = q^k$.

Proof: V is a vector space of dim k.

$\Longleftrightarrow$ $\exists$ basis (基底)

$\{v_1, v_2, \ldots, v_k\}$

独立

($v_1, v_2, \ldots, v_k$: independent)

Any vector in V can be written as

$$x = \alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k.$$

Here, $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{F}_q$.

So, the ways of choices of $(\alpha_1, \ldots \alpha_k)$ are q^k.

$\blacksquare$

Theorem

If a linear code $\mathcal{C}$ is generated by $[I_k \quad A]$, then $\mathcal{C}^{\perp}$ is generated by $[-A^{\top} \quad I_{n-k}]$.

H

Proof: Let G be the generator matrix.

$$G = [I_k \ A] = \underbrace{\begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}}_{k}\underbrace{\begin{bmatrix} a_{11} & \cdots & a_{1,n-k} \\ a_{22} & \cdots & a_{2,n-k} \\ \vdots & & \\ a_{k,n-k} & \cdots & a_{k,n-k} \end{bmatrix}}_{n-k} {}_{k \times n} = \begin{bmatrix} g_1 \\ \vdots \\ g_n \end{bmatrix}$$

$A : (n-k) \times k$

$$H = [-A^{T} \ I_{n-k}] = \begin{bmatrix} -a_{11} & \cdots & -a_{k,1} & 1 & & 0 \\ -a_{12} & \cdots & -a_{k,2} & & \ddots & \\ \vdots & \ddots & \vdots & 0 & & \\ -a_{1,n-k} & \cdots & -a_{k,n-k} & & & 1 \end{bmatrix} = \begin{bmatrix} h_1 \\ \vdots \\ h_n \end{bmatrix}$$

- The row vectors of G (H) form a basis of $\mathcal{C}$ ($\mathcal{C}^{\perp}$).
- It suffices to show $\langle g_i, h_j \rangle = 0 \quad \forall i, j$

$$\langle g_i, h_j \rangle$$

$$= \langle (0, 0, \dots, \underset{(i\text{th})}{\underset{\uparrow}{1}}, 0, 0, \; a_{i1}, a_{i2} \cdots a_{i,n-k}),$$

$$(-a_{1j}, -a_{2j}, \dots, -a_{kj}, \; 0, 0, \dots, \overset{(j\text{th})}{\overset{\downarrow}{1}} \dots, 0)\rangle$$

$$= (-a_{ij}) + (a_{i,j})$$

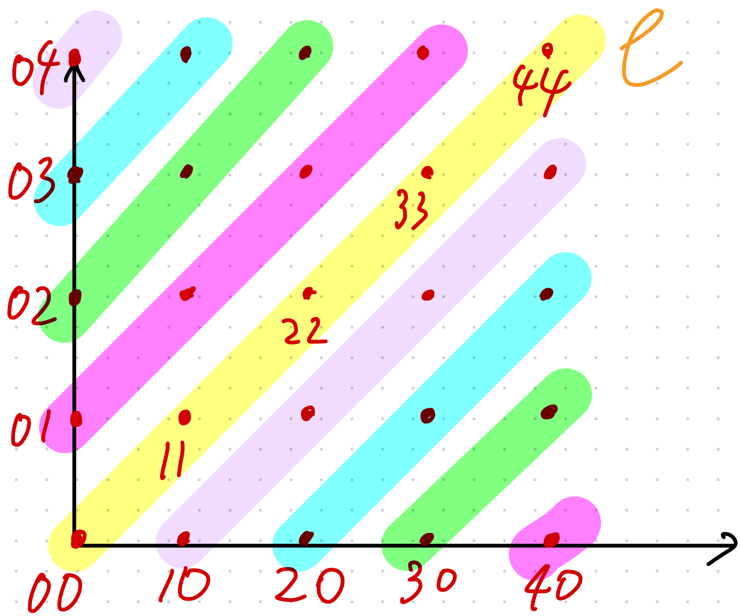
$$= 0$$

$\blacksquare$

Example:

Repetition code in $\mathbb{F}_p^2$, $p=5$

$$\mathcal{C} = \{(0,0), (1,1), (2,2), (3,3), (4,4)\}$$



4 cosets: $\mathcal{C}+(1,0)$, $\mathcal{C}+(2,0)$

$\mathcal{C}+(3,0)$, $\mathcal{C}+(4,0)$

$AG(2, \mathbb{F}_5)$ a 1-flats

$$H = \left[h_1, h_2, h_i, \ldots, h_n \right]$$

$$\left(H \cdot e_i^T \right)^T = e_i \cdot H^T$$

$$= \left[0, 0, \underset{\substack{\uparrow \\ i}}{1}, \ldots 0 \right] \cdot \begin{bmatrix} h_1^T \\ \vdots \\ h_n \end{bmatrix}$$

$$= h_i^T$$

$$\Longleftrightarrow \quad H \cdot e_i^T = h_i$$

Proposition

- For any vector $\mathbf{v} \in \mathbb{F}_q^n$ there are $\binom{n}{s}(q-1)^s$ vectors in $\mathbb{F}_q^n$ that have Hamming distance s from $\mathbf{v}$.
- For any vector $\mathbf{v} \in \mathbb{F}_q^n$ there are $\sum_{s=0}^{t} \binom{n}{s}(q-1)^s$ vectors in the sphere of radius t centered at $\mathbf{v}$.

Proof (1). There are $\binom{n}{s} = \frac{n!}{s!\,(n-s)!}$ ways to choose s cooridinate from $v \in \mathcal{C} \subseteq \mathbb{F}_q^n$.

For each coordinate, there are $(q-1)$ choices to change. $\boxtimes$