L12

Thursday, September 22, 2022 10:24 AM

Linear

* Vector space base on a finite field $F = GF(p^m)$

* An informal definition:

  - $\vec{V} \in F^n$ being an n-dim vector with each coordinate $V_i \in F$
  - $\vec{V} + \vec{U} = (V_1 + U_1, \cdots, V_n + U_n)$
  - $a\vec{V}$ where $a \in F$
    $= (aV_1, aV_2, \cdots, aV_n)$ all multi in F.

A linear sub-vector space is determined by a spanning set

set $\{\vec{V}_1, \cdots, \vec{V}_k\}$ such that

$V_1 = \{ \sum_{i=1}^{k} a_i \vec{V}_i \mid a_i \in F \}$

$$V_{subspace} = \left\{ \sum_{k=1}^{K} \alpha_k \vec{v}_k : \forall \alpha_k \in F \right\}$$

The minimum spanning set (with minimal cardinality) is a basis of V.

The dimension of V is the size of the basis. We write $\dim(V) = k$

Inner Product

$$\vec{u} \cdot \vec{v} = \sum_{i=1}^{n} u_i \cdot v_i \quad \text{in } F$$

Properties $\vec{u} \cdot \vec{v} = \vec{v} \cdot \vec{u}$

$$a \cdot (\vec{u} \cdot \vec{v}) = (a \cdot \vec{u}) \cdot \vec{v}$$

$$\vec{u} \cdot (\vec{v} + \vec{w}) = \vec{u} \cdot \vec{v} + \vec{u} \cdot \vec{w}$$

Dual Space

S is a linear subspace

S is a linear subspace

and $S^\perp$ is the set of all vectors u such that $\vec{u} \cdot \vec{v} = 0$ for all $v \in S$

$S^\perp$ is called the dual space.

Properties: ① $S^\perp$ is a linear subspace as well

② $\dim(S) + \dim(S^\perp) = \dim(V)$

$\Longrightarrow$ The whole space.

Remark: It is a bit different than the Euclidean space.

E.g. $V = (GF(2))^2 = \{(a_1, a_2) : a_1, a_2 \in GF(2)\}$

$S = \{a(1,1) : a \in GF(2)\}$

$= \{(0,0), (1,1)\}$.

$S^\perp = \{b(1,1) : b \in GF(2)\} = S$

We do have

$$\dim(S) + \dim(S^\perp) = 2 = \dim\left((GF(2))^2\right)$$

but. the <u>span</u> of S and $S^\perp$ is the same as S, and it's not $GF(2)^2$

In Euclidean space

span the entire 2-D space.

Revisit linear block codes.

* A linear block code in $GF(p^m) = F$ is characterised by a generator matrix

$$\vec{G} \in F^{n \times k}$$

and a codeword

$$\vec{x} = G \cdot \vec{m}$$ where all the operations are in F

operations are in F

* We call it (n, k) linear block code.

n: codeword length, k: message length

* It can also be characterized by the parity check matrix $H \in F^{(n-k)\times n}$ such that all codewords $\vec{x}$ satisfy

$$\vec{0} = H \cdot \vec{x}$$

* If $H = [I_{n-k}, P]$, (after row operations in F)

then $G = \begin{bmatrix} -P \\ I \end{bmatrix}$ where $P \in F^{(n-k)\times k}$

---

* H can be viewed as the generating matrix of a dual code $C^{\perp}$

(G is the generating matrix of C.)

Hamming distance

$$d_{\text{Hamming}}(\vec{v}, \vec{w}) = \#\text{ of } i \text{ such that } v_i \neq w_i$$

The weight of a vector

$$\text{weight}(\vec{v}) = d_{\text{Hamming}}(\vec{v}, \vec{0})$$

Minimal distance of a codebook

$$C = \{ \vec{c}_i : i = 0, \dots, M-1 \}$$

↳ where M is usually $p^k = p^{n \cdot R}$

is

$$d_{\min} = \min_{\substack{i \neq j \\ 0 \leq i, j \leq M-1}} d_{\text{Hamming}}(\vec{c}_i, \vec{c}_j)$$

Corollary. The minimal distance of a linear block code is

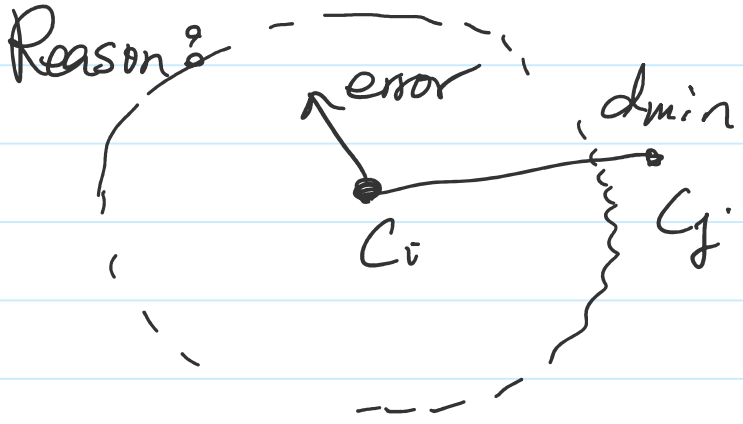
$$d_{\min} = \min \text{ weight}(\vec{c}_i)$$

$$d_{min} = \min_{1 \le i \le M-1} \text{weight}(\vec{c}_i)$$

$$= \min_{1 \le i \le M-1} d_{Hamming}(\vec{c}_i, \vec{0})$$

Here we assume $\vec{c}_0 = \vec{0}$

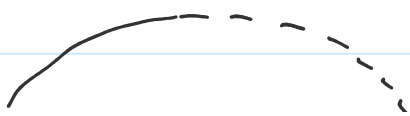
A code can "detect" all error patterns of weight $\le d_{min} - 1$

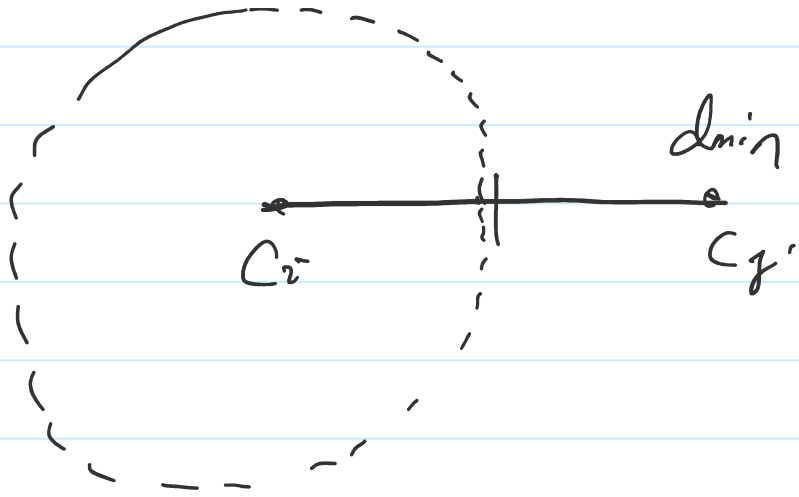


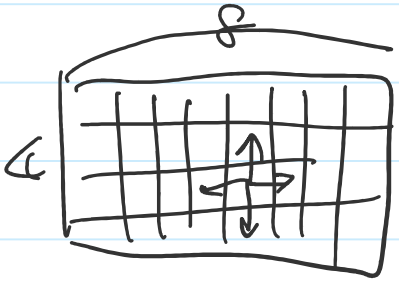
A code can "correct" all error patterns of weight $< \frac{d_{min}}{2}$

or equivalently

$$\text{weight} \le \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor$$





Recall the  example

the upper bound is $\frac{32}{5}$

Suppose a code of length n can decode $\leq t$ errors. in $\left[GF(p^m)\right]^n$ vector space

$\Rightarrow$ each codeword occupies

$$\sum_{\ell=0}^{t} \binom{n}{\ell} \cdot (p^m - 1)^{\ell} \cdot \quad \text{spaces.}$$

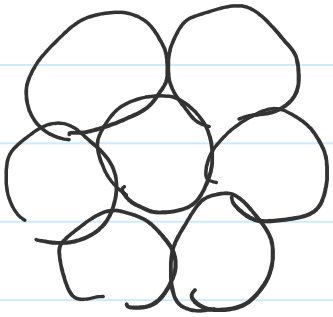
and the total numbes of codewords must satisfy

$$\left(\quad m\right)^n$$

must satisfy

$$M \leq \frac{(p^m)^n}{\sum_{\ell=0}^{t} \binom{n}{\ell} \cdot (p^m - 1)^{\ell}}$$

* Any code that attains the equality is called a perfect code

i.e.  all the spheres are perfectly packed.

Example of perfect codes.

① $\mathcal{C} = \mathbb{F}_p^n$, $t = 0$.

$$(p)^n = \frac{p^n}{1}$$

② $\mathcal{C} = \{\vec{0}\}$ $t = n$

$$1 \quad 10^n$$

$$1 = \frac{p^n}{p^n}$$

③ $\mathcal{C} = \{\vec{0}, \vec{1}\}$ and n is odd

$$\Rightarrow t = \frac{n-1}{2}$$

$$2 = \frac{p^n}{\sum_{i=0}^{\frac{n-1}{2}} \binom{n}{i} \cdot (p-1)^i}$$

---

④ binary Hamming Code $(7,4)$. $t=1$ can correct one error

$$2^4 = \frac{2^7}{\binom{7}{0} + \binom{7}{1}}$$

$$16 = \frac{128}{1+7}$$

⑤ binary Golay Code

$(23, 12)$ $t=3$ $d_{min} = 7$

No other perfect code exists

(except for the $GF(p^m)$ versions of either Hamming or Golay Codes.