Linear Codes

A linear code is a vector subspace of $\mathbb{F}^n$ over $\mathbb{F}$

[n,k,d] linear code

(n, M)

min. distance

dimension

length / blocklength

$$R = \frac{\log_2 M}{n} = \frac{\log_2 |\mathbb{F}|^k}{n} = k\frac{\log_2 |\mathbb{F}|}{n}$$

= # of info bits sent per channel use.

Generator matrix

One way of specifying a linear code: Describe basis.

- Codewords are row vectors $1 \times n$

- Generator matrix: $k \times n$ matrix of basis vectors (rows)

$$G = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} \quad \text{over } \mathbb{F}_2$$

$$C = \left\{ [1\ 0\ 1],\ [1\ 1\ 0],\ [0\ 1\ 1],\ [0, 0, 0] \right\}$$

$$[m_1 \quad m_2] \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix} = [c_1 \quad c_2 \quad c_3]$$

message vector

codeword

m_1	m_2	c_1	c_2	c_3
0	0	0	0	0
0	1	1	1	0
1	0	1	0	1
1	1	0	1	1

ENCODING: $\underline{m}\,G = \underline{c}$

Minimum Hamming distance and minimum Hamming weight

$$d_{min}(C) = \min_{\substack{\underline{c}_1 \neq \underline{c}_2 \\ \underline{c}_1, \underline{c}_2 \in C}} d_H(\underline{c}_1, \underline{c}_2)$$

$$wt(C) = \min_{\substack{\underline{c} \in C \\ \underline{c} \neq \underline{0}}} wt_H(\underline{c})$$

Claim: for any linear code, $wt(C) = d_{min}(C)$

Proof: ① Suppose $d_{min}(C) = d$

$\exists\ \underline{c}_1, \underline{c}_2$ s.t. $d_H(\underline{c}_1, \underline{c}_2) = d$

$\Rightarrow wt_H(\underline{c}_1 - \underline{c}_2) = d$

$\Rightarrow \underline{c}_1 - \underline{c}_2 \in \underline{C}$ (linear)

$\Rightarrow wt(C) \leq d$

If $\underbrace{wt(C)}_{d'} < d \Rightarrow \exists\ \underline{c} \in C$ st $wt_H(\underline{c}) = d'$

$d_H(\underline{c}, \underline{0}) = d' < d_{min}$

Contradiction!

Parity-check matrix

Four fundamental s/s

1. Row space
2. Col space
3. Right nullspace
4. Left nullspace

$C = \text{rowspace}(G)$

$C = \text{right NS}(H)$
$\downarrow$
parity check matrix

If H is PCM for C & $\underline{c} \in C$,

$H \underline{c}^T = \underline{0}^T$

$(n-k) \times n$

$C = NS(H) = \{ \underline{c} \in \mathbb{F}^n \text{ st } H \underline{c}^T = \underline{0}^T \}$

For any H, $\text{Rank}(H) + \text{Nullity}(H) = \#$ of columns of H

$$\#\text{rows}(H) + k = n$$

$$\#\text{rows}(H) = n-k$$

Dual Code

$G : k \times n$

$C = \text{rowspan}(G)$

$C^{\perp} = \text{rightNS}(G) \rightarrow$ dual code of $\underline{c}$

$\underline{c} \in C \quad \perp \quad \underline{\tilde{c}} \in C^{\perp} \Rightarrow \underline{c}\,\underline{\tilde{c}}^{T} = \underline{0}$

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \qquad C = \left\{ \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 \end{bmatrix} \right\}$$

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

$H \underline{x}^T = \underline{0}$ iff & $\underline{\text{ONLY IF}}$ $\underline{x} \in C$

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \longrightarrow C = \left\{ \begin{matrix} [0 & 0 & 0 & 0] \\ [1 & 0 & 0 & 1] \\ [0 & 1 & 1 & 0] \\ [1 & 1 & 1 & 1] \end{matrix} \right\}$$

$$H = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \checkmark \qquad NS(H) = C$$

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

Self dual code

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

Claim: H is a parity check matrix for C

$$HG^T = \underline{0}$$

& $\text{rank}(H) = n-k$

$$= n - \text{rank}(G)$$

G is any generator matrix for C

$$G \xrightarrow[\text{reduced ech}]{\text{row}} \begin{bmatrix} I_{k\times k} & A_{k\times(n-k)} \end{bmatrix}$$

$$H = \begin{bmatrix} -A^T & I_{(n-k)\times(n-k)} \end{bmatrix}$$

$\text{rank}(H) = n-$

$$HG^T = \begin{bmatrix} -A^T & I \end{bmatrix} \begin{bmatrix} I \\ A^T \end{bmatrix} = -A^T + A^T = 0$$

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

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

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

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

Minimum distance from the parity-check matrix

<u>Claim</u> Given any $[n, k, d]$ linear code C, let H be any PCM for C. Let l be the maximum no. st every l columns of H are linearly independent. Then,

$$l = d - 1.$$

OR: (i) Every set of $d-1$ cols of H are l.i

& (ii) Some set of d cols of H are l.d.

<u>Proof</u>:

$$H\underline{x} = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ \underline{0} & \underline{0} & 1 & \underline{0} & 1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

$$d-1 = 2$$

$$d = 3$$

(ii) $\Rightarrow$ $\exists\ \underline{x}$ with $wt_H(\underline{x}) = d$ & $H\underline{x} = \underline{0}$

$\Rightarrow$ $\underline{x} \in C$ with $wt_H(\underline{x}) = d$

This is true!

(i) Every $d-1$ cols are l.i $\Rightarrow$ $H\underline{x} \neq \underline{0}$

as long as # of nonzero entries in $\underline{x} \leq d-1$

If $H\underline{x} = 0$, then $wt_H(\underline{x}) \geq d$

$\therefore$ $H\underline{x} \neq \underline{0}$ for all $\underline{x}$ with $0 < wt_H(\underline{x}) \leq d-1$

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

Complexity of finding rank $(n-k) \times l$ matrix ; $O((n-k) \times l)$

Total complexity : $\displaystyle\sum_{l=2}^{d} \binom{n}{l} O((n-k) \times l)$

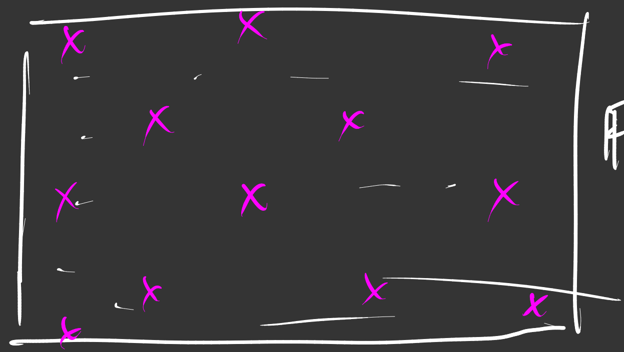
Decoding linear codes: Array decoding

Decoding over bit-flip channel

Decoding using a table

Cosets, coset leaders

C is a subspace of $\mathbb{F}^n$



$\mathbb{F}^n$

$(C, \oplus)$ forms an Abelian group.

$(\mathbb{Z}, +)$ $\qquad$ $(2\mathbb{Z}, +)$

Group: $(G, \oplus)$ is a Abelian group if

1. Closure $\quad a \oplus b \in G \;\; \forall\, a, b \in G$
2. Commutative $\quad a \oplus b = b \oplus a$
3. Associative
4. Identity
5. Inverse

Take any positive integer a

$$a\mathbb{Z} = \{ax : x \in \mathbb{Z}\}$$

is a subgroup of $\mathbb{Z}$

$$2\mathbb{Z} \subseteq \mathbb{Z}$$

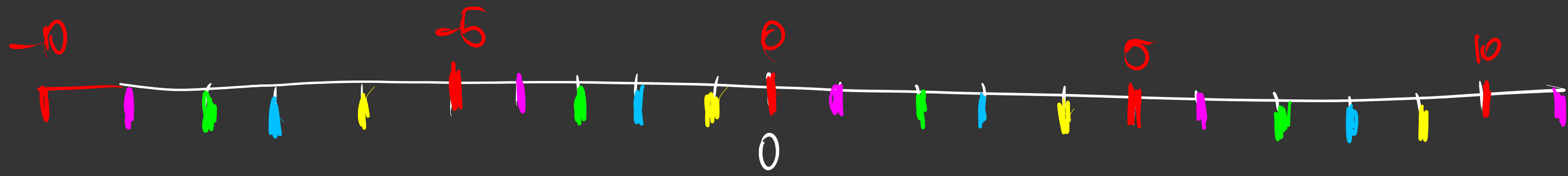
$$\mathbb{Z} = (2\mathbb{Z}) \cup (2\mathbb{Z}+1)$$

$$2\mathbb{Z}+1 = \{2x+1 : x \in \mathbb{Z}\}$$

$2\mathbb{Z}+1$ & $2\mathbb{Z}$ are cosets of $2\mathbb{Z}$ in $\mathbb{Z}$

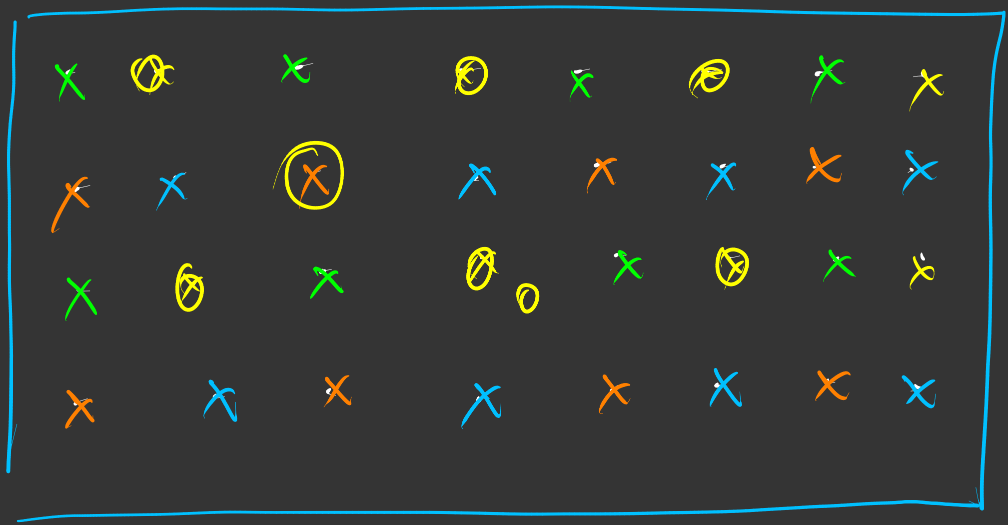
$\mathbb{Z}$, $5\mathbb{Z}$

Cosets: $5\mathbb{Z}$, $5\mathbb{Z}+1$, $5\mathbb{Z}+2$, $5\mathbb{Z}+3$, $5\mathbb{Z}+4$



$$5\mathbb{Z} + \underbrace{\{0, 1, 2, 3, 4\}}_{\text{Coset representatives}} = \mathbb{Z}$$

$$10\mathbb{Z} + \{0, 1, \ldots, 9\} = \mathbb{Z}$$



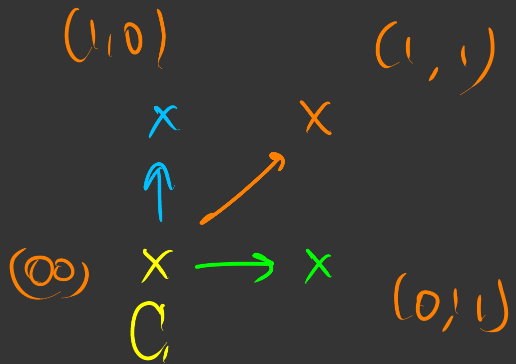
$\mathbb{F}^n$ $\quad k$

$2^n = 2^{n-k} \times 2^k$

C_1

$5\mathbb{Z} + 10 = 5\mathbb{Z}$

$C_1 + C$



$4\mathbb{Z}$ $\quad \{0, 1, 2, 3\}$

Decoding linear codes: Syndrome decoding

$$C = \{ \underline{x} \in \mathbb{F}^n : \quad H\underline{x} = \underline{0} \}$$

$$C + \underline{e} = \{ \underline{x} \in \mathbb{F}^n : \quad H\underline{x} = H\underline{e} \}$$

$$\begin{aligned} H\underline{e} &= \underline{b} \end{aligned}$$

$$H\underline{x} = \underline{b}$$

$$C_b =$$

$$H\underline{x} \longrightarrow \text{Syndrome of } \underline{x}$$

All vectors $\underline{x} \in \mathbb{F}^n$ having the same syndrome form a <u>coset</u>

DECODING:

Store: For each coset, store the error vector / the element with (syndrome) the least Hamming wt

- Given $\underline{y}$, compute $H\underline{y} = \underline{s}$

$$\hat{\underline{x}} = \underline{y} - \underline{e}_s$$