Tutorial: Linear block codes

Note Title

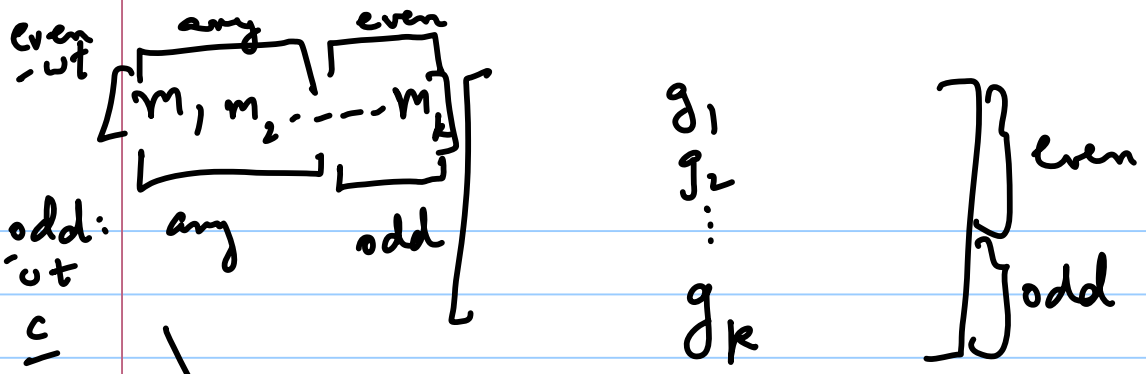
(8) C : linear code

- has at least one odd-wt codeword

$$C_e = \{ \underline{c} \in C : wt(\underline{c}) : even \}$$

$$C_o = \{ \underline{c} \in C : wt(\underline{c}) : odd \}$$

We have to show $|C_e| = |C_o|$



# of odd-wt codewords $= 2^{k-1} =$ # of even-wt codewords

$C_e \subseteq C$, subcode; C_o: coset of C_e ?

Cosets of C_e: partition C

$C_e \cup C_o = C \Rightarrow$ only two cosets

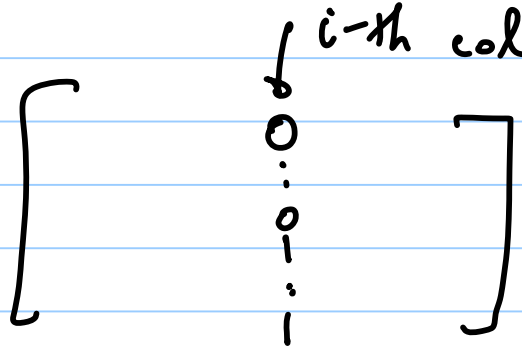
$2^{k-1} = |C_o| = |C_e|$

(9) C : code (n,k) (non-trivial: no coordinate is 0 in all codewords)

Show: $C_0^{(i)} = \{c \in C : c_i = 0\}$: subcode

$C_1^{(i)} = \{c \in C : c_i = 1\}$: coset of $C_0^{(i)}$

$\Rightarrow |C_0^{(i)}| = |C_1^{(i)}| = 2^{k-1}$.



(11)

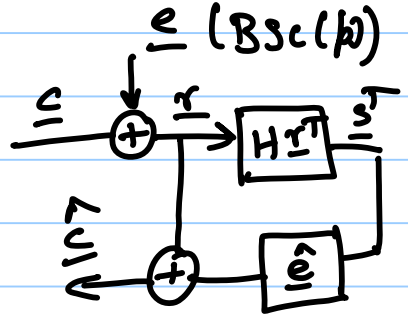
$$H = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Use : BSC(p)

Max-likelihood decoder : Syndrome decoder

$\underline{s}^T$	$\hat{\underline{e}}^T$: lowest wt s.t. $H\hat{\underline{e}} = \underline{s}$
000	000000
001	001001
010	100000
011	000010
100	010000
101	000100
110	001000
111	000001

$\Pr(\underline{c} \neq \hat{\underline{c}}) = ?$



$$Pr(\underline{c} = \hat{\underline{c}}) = Pr(\underline{c} \in \underset{\text{table}}{\hat{\underline{e}}\text{'s in}})$$

$$= (1-p)^6 + 6p(1-p)^5 + p^2(1-p)^4$$

$$Pr(\underline{c} \neq \hat{\underline{c}}) = 1 - (1-p)^6 - 6p(1-p)^5 - p^2(1-p)^4$$

as $p \to 0$, $\quad -15p^2 + 6p \cdot 5p - p^2$

$$= 14p^2 + p^3 \text{ on higher}$$

(13) C: linear code (n, k, d)

Take $u \notin C$. Show $C \cup u + C$: linear code

$(n, k+1, ?)$

(14) (a) $\left(C^{\perp}\right)^{\perp} = C$

$$C^{\perp} = \{ \underline{v} : \underline{v} \cdot \underline{c} = 0 \ \forall \ \underline{c} \in C \}$$

$$\left(C^{\perp}\right)^{\perp} = \{ \underline{u} : \underline{u} \cdot \underline{v} = 0 \ \forall \ \underline{v} \in C^{\perp} \}$$

(b) C, D: two linear codes in $\{0,1\}^n$

$$C + D = \{ u + v : u \in C, v \in D \}$$

linear code?

G_C, G_D

$$(C+D)^\perp = C^\perp \cap D^\perp \qquad \begin{bmatrix} G_C \\ G_D \end{bmatrix}$$

Pf: Let $x \in (C+D)^\perp$

$\Rightarrow x \cdot (u+v) = 0 \quad \forall\ u \in C \ \& \ v \in D$

Take $v = 0$. $x \cdot u = 0 \ \forall u \in C \Rightarrow x \in C^\perp$

Take $\underline{u} = 0$, $\underline{x} \cdot \underline{v} = 0 \ \forall \underline{v} \in D \Rightarrow \underline{x} \in D^\perp$

$\Rightarrow \underline{x} \in C^\perp \cap D^\perp$

$\Rightarrow (C+D)^\perp \subseteq C^\perp \cap D^\perp$.

Let $\underline{x} \in C^\perp \cap D^\perp$

$\underline{x} \cdot (\underline{u}+\underline{v}) = \underline{x} \cdot \underline{u} + \underline{x} \cdot \underline{v}$

$\underline{u} \in C, \underline{v} \in D \quad = 0 + 0 = 0$

$\Rightarrow \underline{x} \in (C+D)^\perp \quad \underline{Q \subseteq D}$

15

G, G'

C_1 & C_2 are equivalent

Equivalent codes: if $\exists$ π (perm) s.t.

$$C_2 = \{[c_{\pi(1)}\ c_{\pi(2)} \cdots c_{\pi(n)}] : [c_1\ c_2 \cdots c_n] \in C_1\}$$