Theory @ UCLA Week 3 presented by Nakul

Defn] linear codes : subspace of $\mathbb{F}_2^n$

G generator matrix if its k columns span $C \subseteq \mathbb{F}_2^n$
$\in \mathbb{F}_2^{n \times k}$

$x \mapsto Gx$ is an encoding

Ex] binary parity check
binary repetition
hamming code.

Defn] Distance of a code $= \min_{c_1, c_2 \in C} \Delta(c_1, c_2)$

parity check : dist $= 2$
hamming: dist $= 3$

Equivalent] ① C has dist $2t+1$
② C can correct t symbol errors
③ C can detect $2t$ symbol errors.

Ex] For a linear code, min dist = min hamming weight of non-zero codewords.

Ex] **Defn]** Parity check matrix:
$H \in \mathbb{F}_2^{(n-k) \times n}$ (full row rank) such that $C = \{c \in \mathbb{F}_2^n \mid Hc = 0\}$ i.e nullspace of H

$HG = 0$

Lemma] min # of lin dep columns of $H(C) = \Delta(C)$

$$G = \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \quad \begin{bmatrix} \quad \end{bmatrix} \rightarrow \begin{bmatrix} \quad \\ \quad \\ \quad \\ \quad \\ \quad \\ \quad \\ \quad \end{bmatrix}$$

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

corollary dist = 3 $\Rightarrow$ can correct 1 error!!

Ex] slick way to correct y

$y = c + e_i$ for some e_i

$Hy = H(c+e_i) = He_i$ = i^{th} column $\rightarrow$ binary rep of i!

Generalized Hamming code:

$C^{(r)}_{Ham} :=$ nullspace of H_r $\quad r \times 2^r - 1$ binary counting.

Claim: dist = 3

pf] lin dep columns

no two lin dep

and $1+2+3 = 0$

need to motivate this. what exactly am I proving?

lemma] Hamming bound

$$|C| \leq \frac{2^n}{n+1}$$

Some exercise on dual codes:

Ex 4 1-3

$\rightarrow$ don't wanna go into Hadamard codes...