From last lecture:

$\mathcal{C} = [n,k]$ binary linear code = linear subspace of $\mathbb{F}_2^n$ w/ dimension k $\quad k \le n$

code words of $\mathcal{C}$ $\equiv$ vectors in $\mathcal{C}$

$$\underbrace{w}_{\text{vector of length } n} = \underbrace{d}_{\text{length } k} \; \underbrace{G}_{k \times n \text{ matrix}}$$

k rows
n cols

$$G = [I_k, \underbrace{A}_{k \times (n-k)}]$$

$[7,4]$ Hamming code

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

$4 \times 3 = A$

encode $d = (1,0,0,1)$ as $w = dG$

$$= (1,0,0,1) \begin{pmatrix} 1 & & & & 1 & 1 & 0 \\ & 1 & & & 1 & 0 & 1 \\ & & 1 & & 0 & 1 & 1 \\ & & & 1 & 1 & 1 & 1 \end{pmatrix} = \begin{array}{c} x_5 \; x_6 \; x_7 \\ (1,0,0,1,0,0,1) \end{array}$$

$\mathcal{C}^\perp$ = dual code = $\{ v \in \mathbb{F}_2^n \mid v \cdot w = 0,\ \text{all } w \in \mathcal{C} \}$

H = generating matrix for $\mathcal{C}^\perp$, H is $n-k$ by n

last time showed $\quad \underbrace{G}_{k \times n} \underbrace{H^T}_{n \times (n-k)} = 0$

Check that $H = [-A^T, \mathbb{1}_{n-k}]$ over $\mathbb{F}_2^n$

$[G, H^T] \overset{?}{=} 0$

$$[G, H^T] = [\mathbb{1}_{k,k}, A_{k,n-k}] \begin{bmatrix} -A_{k,n-k} \\ \mathbb{1}_{n-k,n-k} \end{bmatrix} = -A_{k,n-k} + A_{k,n-k} = 0$$

Hamming

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \qquad A^T = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix}$$

$$\left(\overbrace{\begin{matrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{matrix}}^{A^T} \; \overbrace{\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}}^{\mathbb{1}_{k,k}} \right)$$

suppose data word $\quad d \xrightarrow{\text{encode}} w$ in $\mathcal{C}$ (can be Hamming code

error 1-bit

$$w' = w + e$$

$$H w'^T = \underbrace{H w^T}_{0} + H e^T$$

$$\text{if } e = (0, 0, \dots, \underset{j}{1}, 0, \dots) \quad \text{pos}^n$$

$$\longrightarrow \quad He^T = j\text{th column of } H$$

Take w', compute $\quad Hw'^T = \begin{cases} 0 \\ \neq 0 \end{cases}$

no error

- if you get jth column of H, there was error in jth bit
- otherwise in trouble

H : $n, n-k$

e : $1, n$

e^T : $n, 1$

a word w in code is vector — point in $\mathbb{F}_2^7$

$w' = w + \underset{\uparrow \text{ 1 bit error}}{e}$

2 codewords w_1 & w_2. Hamming distance between w_1 & w_2 is # of bits where they differ

$w_1 = (000\underline{111}1) \xrightarrow{\text{encodes}} (0,0,0,1)$

$w_2 = (00\underline{10}\,\underline{0}11) \xrightarrow{\text{encodes}} (0,0,1,0)$

$\rightarrow h(w_1, w_2) = 3$

Hamming distance of a code e is the minimum Hamming distance between any 2 distinct codewords

Check: Hamming distance of the [7,4] code is 3

Golay Code: [23, 12] code

QM time! :)

Singlest classical error correction is repitition code

have to copy / "clone" bits

Can you clone the quantum state?

Consider a 2 qubit system

$|\psi\rangle \otimes |\phi\rangle \xrightarrow{\text{interact}} |\psi\rangle \otimes |\psi\rangle \qquad \langle\phi|\phi\rangle = 1$

$|\psi\rangle$: state we want to copy

$|\phi\rangle$: standard reference

want $|\psi\rangle \otimes |\psi\rangle = U(|\psi\rangle \otimes |\phi\rangle)$ true for any $|\psi\rangle$

good enough : $U(|\psi\rangle \otimes |\phi\rangle) = e^{i\alpha} \; |\psi\rangle \otimes |\psi\rangle$

$U(|\psi'\rangle \otimes |\phi\rangle) = e^{i\beta} \; |\psi'\rangle \otimes |\psi'\rangle$ true for any $|\psi\rangle, |\psi'\rangle$

$$\left({}_1\langle\psi'| \otimes {}_2\langle\phi| \right) \left(|\psi\rangle_1 \otimes |\phi\rangle_2 \right) = {}_1\langle\psi'|\psi\rangle_1$$

$$\left(e^{-i\beta} \; {}_1\langle\psi'| \otimes {}_1\langle\psi'| \, U \right) \left(U^{+} e^{i\alpha} \; |\psi\rangle_1 \otimes |\psi\rangle_2 \right)$$

$$= e^{i(\alpha-\beta)} \; {}_2\langle\psi'|\psi\rangle_2$$

$$|\langle\psi'|\psi\rangle| = |\langle\psi'|\psi\rangle|^2$$

$$\longrightarrow \quad \langle\psi'|\psi\rangle = 0 \text{ or } 1$$

orthogonal or same. not true for arbitrary states