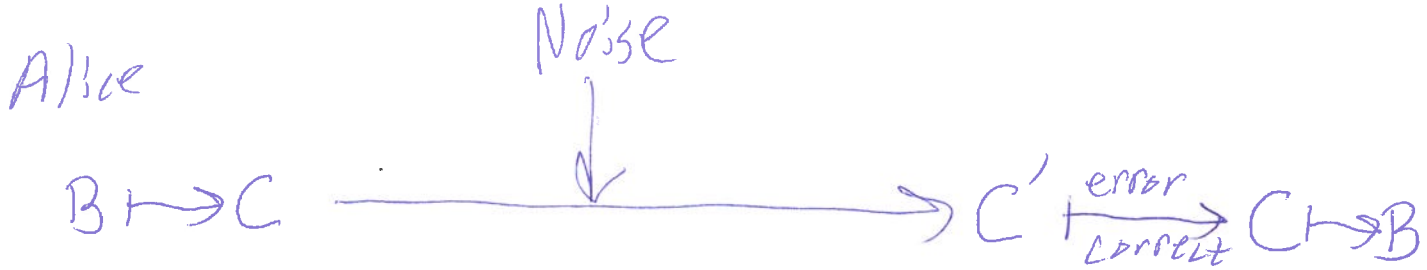
CSCE 785
11/28/2023

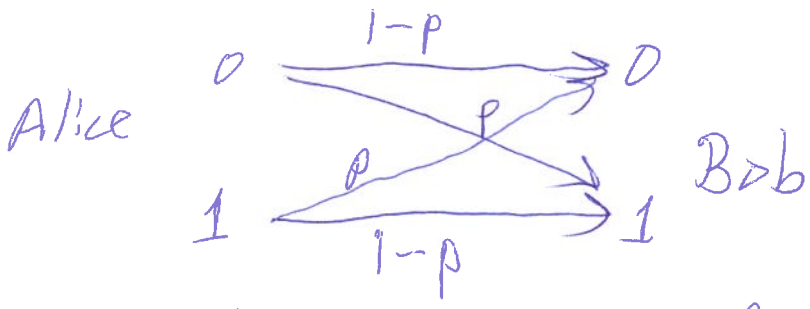
Classical error correction: binary linear codes

Block of k bits $B \longmapsto$ block of n bits C (codeword)

$n > k$



Binary symmetric channel with error prob p $\left(0 \le p \le \frac{1}{2}\right)$



Set of codewords is a subspace of $\mathbb{Z}_2^n$ (code space)

Encoding Map $\mathbb{Z}_2^k \to \mathbb{Z}_2^n$ is linear, rep. by an $n \times k$ matrix G (generator).

Example: Majority-of-3 code: $k = 1$, $n = 3$

Encoding $0 \longmapsto 000$

$1 \longmapsto 111$

$b \in \{0,1\}$ Error correction: $bbb \longmapsto b$

$bb\bar{b}$, $b\bar{b}b$, $\bar{b}bb$ $\longmapsto b$

$$\text{Prob[Bob is wrong]} = \Pr\{\text{2 bits flipped}\} + \Pr\{\text{3 bits flipped}\}$$

$$= 3p^2(1-p) + p^3 = 3p^2 - 3p^3 + p^3 = \boxed{3p^2 - 2p^3}$$

$$= O(p^2) \ll p \text{ if } p \ll 1.$$

Hamming Code (7-bit) (later)

Check matrix H. For an $[k,n]$-code

H is an $(n-k)\times n$ matrix of full rank

such that $HG = 0$ $\quad [G \text{ is } n\times k, \text{ full rank}]$

($(n-k)\times k$ null matrix)

All with 1's is in $\mathbb{Z}_2$

Ex: maj-of-3 code: $G = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$

$G[0] = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$ $\quad G[1] = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$

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

Bob gets $\begin{bmatrix} a \\ b \\ c \end{bmatrix}$ $\quad a,b,c \in \{0,1\}$

Computes $H\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} a+b \\ b+c \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$ — no error

$\begin{bmatrix} a+b \\ b+c \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$: flip a

$\begin{bmatrix} \quad \\ \quad \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$: flip c

$\begin{bmatrix} \quad \\ \quad \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$: flip b

↑

possible error syndromes

7-bit Hamming code

$k = 4$, $n = 7$

Check Matrix

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

each codeword $v = \begin{bmatrix} \quad \\ \quad \end{bmatrix}_7$ satisfies $Hv = 0 \in \mathbb{Z}_2^3$

error syndromes:

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

no error flip 1st bit flip 2nd bit

Alice $v \longrightarrow v+e$

e has ≤ 1 many 1s if correctable

$$H(v+e) = Hv + He = He = \text{one column of } H.$$

Ex: Bob computes $H(v+e) = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} = He$

If one bit flipped, must have $e = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$ 5th col of H

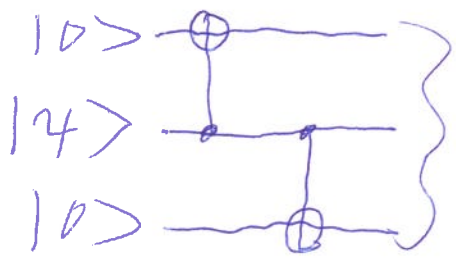
So $v+e$ differs from v in the 5th bit

Quantum bit-flip channel $\mathcal{E}(\rho) = (1-p)\rho + pX\rho X$ where $\rho = |\psi\rangle\langle\psi|$

Alice has 1-qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$\longrightarrow \alpha|000\rangle + \beta|111\rangle$

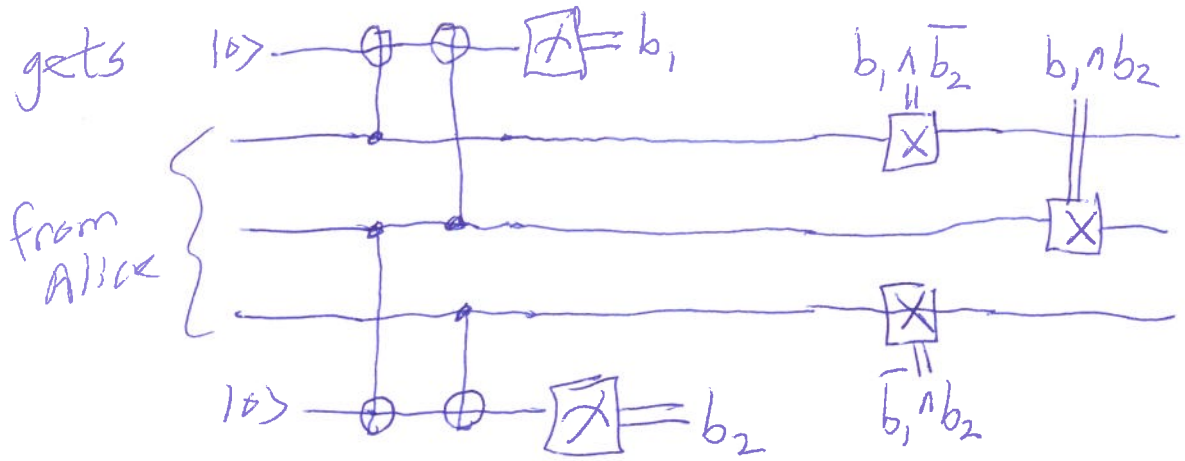
Encoding circuit:



Assuming channel is $\mathcal{E}$ on each qubit independently

so actual channel is $\mathcal{E}^{\otimes 3} = \mathcal{E} \otimes \mathcal{E} \otimes \mathcal{E}$

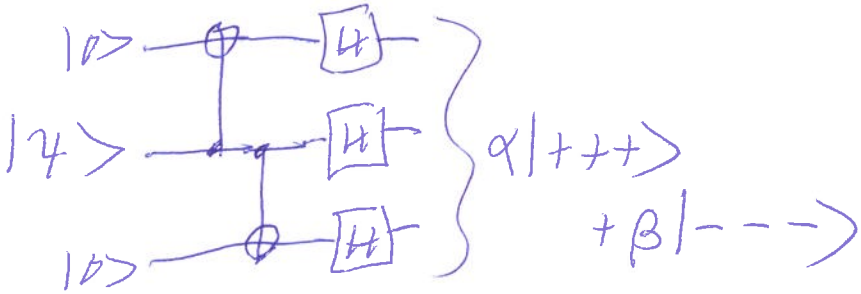
Bob gets



Phase-flip code: $F(\rho) = (1-p)\rho + p Z\rho Z$

actual channel: $F^{\otimes 3}$

Encoding circuit



$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = H|0\rangle$

$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = H|1\rangle$

$F^{\otimes 3}$ is basically $\mathcal{E}^{\otimes 3}$ on this "Hadamard" basis

Bob: