

Lecture 20 CPSC 447/547 - Intro to QC

Basics of Quantum Error Correction II

Outline

- Classical error detection/correction
 - Classical coding theory.
 - Quantum errors
 - Projective measurement.
-

(Classical) Protection against errors

Errors

• Bit flips : $0 \xrightarrow{\mathcal{E}} 1$, $1 \xrightarrow{\mathcal{E}} 0$

• **Random** bit flips: \mathcal{E} : flip each bit **with prob. p** .

$$x \longrightarrow \mathcal{E}(x) = \begin{cases} \neg x & \text{w.p. } p \leftarrow \text{error rate} \\ x & \text{w.p. } 1-p \end{cases}$$

Use **repetition**/**redundancy** (review from last time)

Encode $0 \xrightarrow{\mathcal{E}} 000$, $1 \xrightarrow{\mathcal{E}} 111$

• Probability of **no** error ? $000 \xrightarrow{\mathcal{E}} 000$.
 $(1-p)^3$

• Probability of **1-bit error**? $000 \xrightarrow{\epsilon} 001$, etc.

$$3 \cdot p(1-p)^2$$

• Probability of **2-bit error**? $000 \xrightarrow{\epsilon} 101$, etc

$$3 \cdot p^2(1-p)$$

• Probability of **3-bit error**? $000 \xrightarrow{\epsilon} 111$.

$$p^3$$

Decode

Majority of the bits.

$$000 \xrightarrow{D} 0, 001 \xrightarrow{D} 0, 011 \xrightarrow{D} 1, \dots$$

As long as **not too many errors**, majority still works.

How well does the 3-bit repetition code protect 1 bit of info?

{ Correct up to any 1-bit error! (Arbitrary position)
Detect up to any 2-bit error! (If not 000 or 111 , report error.)

Error Rate

After error correction, what is the error rate?

Prob ("error even after correction")

$$= \text{Prob}(2\text{-bit error}) + \text{Prob}(3\text{-bit error})$$

$$= 3p^2(1-p) + p^3 < p \text{ for small } p.$$

Can we do better? **n-bit repetition**.

Encode: $E(0) = 0^n$, $E(1) = 1^n$

Decode: Majority. (assume odd n).

- { Can correct up to $\frac{n-1}{2}$ errors.
- { Can detect up to $n-1$ errors.

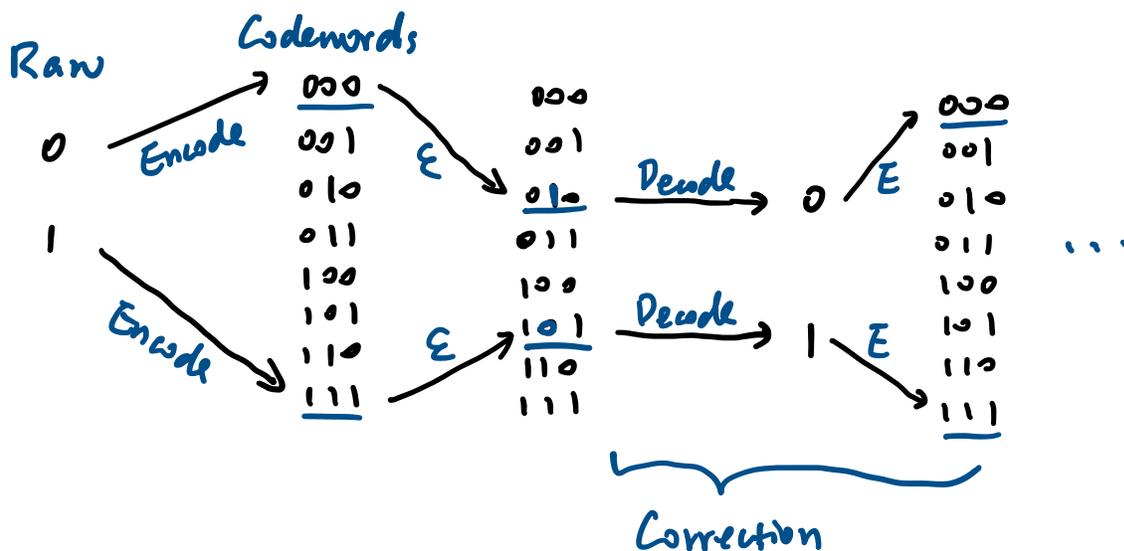
Error rate: $\Pr [D(E(E(x))) \neq x]$

$$= \Pr [\text{Binomial}(n, p) \geq \frac{n}{2}]$$

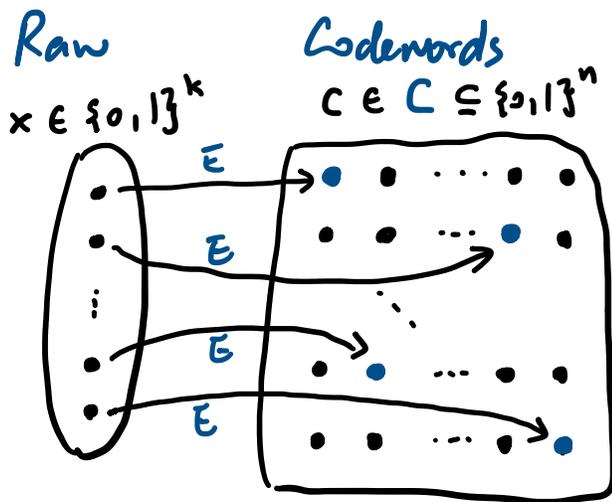
$$\leq \exp(-\frac{n}{2} (\frac{1}{2} - p)^2) \text{ (Chernoff bound)}$$

Classical Error Correcting Code.

Goal: Protect 1 bits of info.



more generally, to protect k bits of info.



Encode: $E: \{0,1\}^k \rightarrow C$

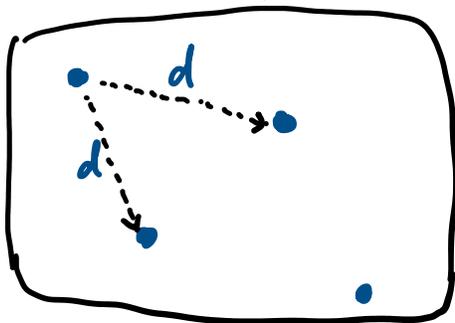
Decode: Pick "nearest" codeword.

↑
Hamming distance
= # bits that differ
= $\|x-y\|_1$.

$C =$ set of codewords

$D(x) = E^{-1}(\operatorname{argmin}_{y \in C} (\|x-y\|_1))$

How well does C protect k -bit info? $y \in C$



Distance of a code:

$d =$ Min hamming distance between any two codewords.

Detection: As long as not a codeword, we report error.

Q: When does this strategy fail?

A: If $c_1 \xrightarrow{\Sigma} c_2$, for $c_1, c_2 \in C$.

So Σ needs to flip at least d bits.

\Rightarrow We can detect up to $d-1$ errors.

Suppose a family of errors $e \in \{0,1\}^n$, $\|e\| \leq d-1$,
 then we can decide if $x \stackrel{?}{=} \Sigma(x) = x+e$.

Correction: Maps to **nearest** codeword.

Q: When does it fail?

A:  If $\|e\| \leq \frac{d-1}{2}$, we are fine.

⇒ We can correct up to $\frac{d-1}{2}$ errors.

Quantum Error Correction (cont'd from last lecture)

Can we generalize "redundancy encoding" to qubits?

- **Analog errors** can be tricky.

Suppose we want to protect $|\psi\rangle$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$\downarrow E(0)$

$\downarrow E(1)$

\leftarrow What's the circuit that does this?

Encode: $E(|\psi\rangle) = \alpha|000\rangle + \beta|111\rangle$.

$$\rho = \alpha\alpha^*|000\rangle\langle 000| + \alpha\beta^*|000\rangle\langle 111| + \beta\alpha^*|111\rangle\langle 000| + \beta\beta^*|111\rangle\langle 111|.$$

Error: $E(\rho) = \sum_k E_k \rho E_k^\dagger$, Kraus operators $\sum_k E_k^\dagger E_k = I$

- **Detection** can be tricky:

Direct measurement destroys P .

Solution: Projective Measurement (**digitize error** + **detection**).

Suppose **codewords**: $|000\rangle, |111\rangle$.

We define **operators**: $A_1 = Z \otimes Z \otimes I, A_2 = I \otimes Z \otimes Z$.

$$\left. \begin{aligned} ZZI |000\rangle &= |000\rangle \\ ZZI |111\rangle &= |111\rangle \\ IZZ |000\rangle &= |000\rangle \\ IZZ |111\rangle &= |111\rangle \end{aligned} \right\} \text{for codewords: } (+1)\text{-eigenstates} \\ \text{for all } A.$$

$$\left. \begin{aligned} ZZI |100\rangle &= -|100\rangle \\ IZZ |100\rangle &= |100\rangle \\ \text{etc} \end{aligned} \right\} \text{for non-codewords: } (-1)\text{-eigenstates.} \\ \text{for some } A.$$

More: A_1 and A_2 together \Rightarrow can **infer location** of a bit flip.

E.g. $ZZI|\psi\rangle = -|\psi\rangle, IZZ|\psi\rangle = -|\psi\rangle$

$$\Rightarrow |\psi\rangle = |100\rangle \text{ or } |011\rangle \text{ or } \alpha|100\rangle + \beta|011\rangle.$$

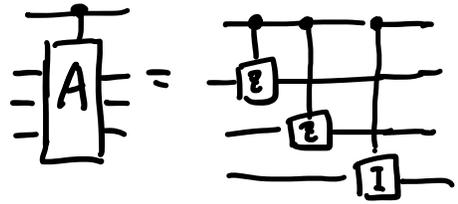
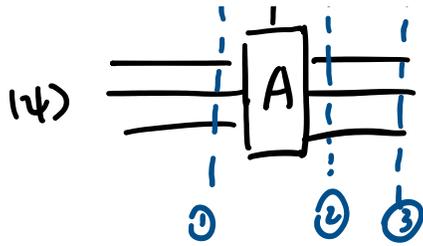
↑ one bit flip

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

Projective Measurement:



E.g. if $A = Z \otimes Z \otimes I$,



$$\textcircled{1} |+\rangle|\psi\rangle$$

$$\textcircled{2} \frac{1}{\sqrt{2}} (|0\rangle|\psi\rangle + |1\rangle A|\psi\rangle)$$

$$\textcircled{3} \frac{1}{\sqrt{2}} (|+\rangle|\psi\rangle + |-\rangle A|\psi\rangle) = \frac{1}{2} ((|0\rangle+|1\rangle)|\psi\rangle + (|0\rangle-|1\rangle)A|\psi\rangle)$$

$$= |0\rangle \frac{I+A}{2} |\psi\rangle + |1\rangle \frac{I-A}{2} |\psi\rangle$$

If $|\psi\rangle$ is (+) eigenstate of A : $A|\psi\rangle = |\psi\rangle$ (for codewords)

$$\begin{cases} \frac{I+A}{2} |\psi\rangle = \frac{1}{2} |\psi\rangle + \frac{1}{2} |\psi\rangle = |\psi\rangle. \\ \frac{I-A}{2} |\psi\rangle = \frac{1}{2} |\psi\rangle - \frac{1}{2} |\psi\rangle = 0 \end{cases} \quad \begin{array}{l} \text{State becomes} \\ \Rightarrow |0\rangle|\psi\rangle + |1\rangle \cdot 0 \end{array}$$

\Rightarrow Measure ancilla : outcome is $|0\rangle$.

If $|\psi\rangle$ is (-) eigenstate of A : $A|\psi\rangle = -|\psi\rangle$ (for non-codewords)

$$\begin{cases} \frac{I+A}{2} |\psi\rangle = 0 \\ \frac{I-A}{2} |\psi\rangle = |\psi\rangle. \end{cases} \quad \begin{array}{l} \text{State becomes} \\ \Rightarrow |0\rangle \cdot 0 + |1\rangle|\psi\rangle \end{array}$$

\Rightarrow Measure ancilla : outcome is $|1\rangle$.

Ancilla's measurement outcome can be used to detect errors!

Example : $|\psi\rangle = \alpha|000\rangle + \beta|111\rangle$.

$$A_1 = ZZI, A_2 = IZZ.$$

If **no error**, what are projective measurement outcomes?

If **one bit flip** : $|\psi'\rangle = \alpha|100\rangle + \beta|011\rangle$.

then what are the projective measurement outcomes?

what is the post measurement state?