Brief administrative remarks.

- lecture notes posted to Canvas; recorded lectures if traveling
- 6 HWs, due "every other week" → this is your grade
    - 2 drops or extensions, read syllabus for details
- AI use OK (as is collaboration) but acknowledge!

Classical information is usually sent as bits:

Hey $\longmapsto$ 0001101001 . . .

environment

What if environment corrupts message?

0011100101 . . . $\longmapsto$ No

Error correction: encode info <u>redundantly</u> to protect it

Repetition code: $\begin{cases} 0 \\ 1 \end{cases} \longrightarrow \begin{cases} 000 \\ 111 \end{cases}$

logical bit — physical bits

Decode message?

000, 001, 010, 100 $\longrightarrow$ 0

111, 110, 101, 011 $\longrightarrow$ 1

So the logic of error correction will be:

$$\text{decoder}\big(\text{noise}(\text{info})\big) = \text{info} \quad \text{(ideally!)}$$

Modern communication networks are based on such codes (although using more clever types of codes, related to constructions we'll discuss much later).

No code will be perfect. Some errors can't be fixed:

$0 \longrightarrow 000 \longrightarrow 001 \longrightarrow 0$ decodable error

$0 \longrightarrow 000 \longrightarrow 011 \longrightarrow 1$ undecodable/logical error

Later, we'll want to think about how to make "good codes".

Unfortunately we can't protect quantum information this way.

Quantum logical bit: $\alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$

A key difference vs. classical bits is that α & β are continuous parameters. Need to protect the superposition...

Challenge #1: no-cloning theorem:

no linear operation $Q\left[\alpha|0\rangle + \beta|1\rangle\right] = \left(\alpha|0\rangle + \beta|1\rangle\right) \otimes \left(\alpha|0\rangle + \beta|1\rangle\right)$.

Proof: $Q|0\rangle = |0\rangle \otimes |0\rangle$ and $Q|1\rangle = |1\rangle \otimes |1\rangle$.

so $Q\left[\alpha|0\rangle + \beta|1\rangle\right] = \alpha|0\rangle \otimes |0\rangle + \beta|1\rangle \otimes |1\rangle$. ∎

We can't copy information like in classical systems.

Challenge #2: "two" kinds of errors.

Pauli operators: $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$, $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$

identity

$X_1 = X \otimes I \otimes I$

$Z_2 = I \otimes Z \otimes I$

bit flip: $X_1\left[\alpha|000\rangle + \beta|111\rangle\right] = \underbrace{\alpha|100\rangle + \beta|011\rangle}_{\text{detectable!}}$

phase flip: $Z_1\left[\alpha|000\rangle + \beta|111\rangle\right] = \underbrace{\alpha|000\rangle - \beta|111\rangle}_{\text{undetectable}}$

We might also think about other errors. Suppose an eavesdropper measures Z_1:

$$\alpha|000\rangle + \beta|111\rangle \xrightarrow[\text{measure } Z_1]{} \begin{cases} |000\rangle & \text{prob. } |\alpha|^2 \\ |111\rangle & \text{prob. } |\beta|^2 \end{cases}$$

We need a way to talk about quantum mechanics that allows us to capture generic error processes...

The right mathematical framework is that of open quantum systems.

closed system. pure state: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

open system. mixed state (density matrix): $\rho = a|0\rangle\langle 0| + b|1\rangle\langle 1| + c|0\rangle\langle 1| + \bar{c}|1\rangle\langle 0|$

$= \begin{pmatrix} a & c \\ \bar{c} & b \end{pmatrix}$ complex conjugate

where: • $\rho = \rho^\dagger$ (Hermitian)

• eigenvalues of ρ in $[0,1]$

• $\mathrm{tr}(\rho) = 1$.

This is so we can interpret:

$$\rho = \sum p_n \underbrace{|\psi_n\rangle\langle\psi_n|}$$ as a mixture of pure states.

note: $\langle\psi_n|\psi_{n'}\rangle = \delta_{nn'}$ since ρ is Hermitian.

Interpret: we're in state $|\psi_n\rangle$ w/ probability p_n.

Caution: decomposition NOT unique if we don't demand $|\psi_n\rangle$ orthogonal

Measurements via Born's rule. If A has eigenvalues a, P_a projects onto that subspace $(AP_a = aP_a)$,

$$\rho \longrightarrow \frac{P_a \rho P_a}{\mathrm{tr}(P_a \rho P_a)} \overset{\text{define!}}{=:} \rho_a \quad \text{w/ prob.} \quad \mathrm{tr}(P_a \rho P_a) =: p_a$$

if we detect measurement outcome a.

So measurement is still not linear. But, suppose we measure and discard knowledge of the outcome.

$$\rho_{\text{ignore}} = \sum_a p_a \rho_a = \sum_a \cancel{\mathrm{tr}(P_a \rho P_a)} \frac{P_a \rho P_a}{\cancel{\mathrm{tr}(P_a \rho P_a)}}$$

$$= \underbrace{\sum_a P_a \rho P_a}_{} =: \mathcal{N}_a[\rho] \quad \text{which is linear!}$$

A noise: "environment" measures A, we never learn outcome.

We'll think of the environment in this way. So even if we start w/ pure state, environment generally turns mixed!

E.g. start w/ $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

$\hookrightarrow \rho_0 = |\psi\rangle\langle\psi| = \begin{pmatrix} |\alpha|^2 & \alpha\bar{\beta} \\ \bar{\alpha}\beta & |\beta|^2 \end{pmatrix}$.

<u>decohere</u> in Z $\hookrightarrow \mathcal{N}_Z(\rho_0) = \begin{pmatrix} |\alpha|^2 & 0 \\ 0 & |\beta|^2 \end{pmatrix}$ is now mixed.

$\mathcal{N}_Z$ preserves the properties of ρ (it stays a valid mixed state). What's the most generic operation that does this?

Quantum channel: $\mathcal{C} : \{\text{density matrix}\} \longrightarrow \{\text{density matrix}\}$

We need:

1. $\mathrm{tr}(\mathcal{C}(\rho)) = \mathrm{tr}(\rho) = 1$ [trace-preserving]
2. $\mathcal{C}(p_1\rho_1 + p_2\rho_2) = p_1\mathcal{C}(\rho_1) + p_2\mathcal{C}(\rho_2)$

Because we interpret mixed states as capturing some classical uncertainty in which state we have!

3. complete positivity: consider

system S entangled w/ reference R

Then: $(\mathcal{C}_S \otimes \mathcal{I}_R)(\rho_{SR})$ must be positive.

This is because in quantum systems we want to allow for systems of interest to be entangled w/ unknown DOF...

Thm: $\mathcal{C}(\rho)$ is CPTP (completely positive, trace-preserving) if and only if $\mathcal{C}(\rho) = \sum_i K_i \rho K_i^\dagger$ where $\sum_i K_i^\dagger K_i = I$.

Kraus operator

Proof: $\mathcal{C} \Rightarrow$ CPTP: $\quad \mathrm{tr}(\mathcal{C}) = \mathrm{tr}\left(\sum_i \rho K_i^\dagger K_i\right) = \mathrm{tr}(\rho I) = 1.$

and
$$\langle \psi_{SR}|\mathcal{C}|\psi_{SR}\rangle = \sum_i \langle \psi_{SR}|(K_i \otimes I)\rho_{SR}(K_i\otimes I)^\dagger|\psi_{SR}\rangle$$
$$= \sum \langle \psi_i|\rho_{SR}|\psi_i\rangle \geq 0, \qquad |\psi_i\rangle = K_i^\dagger|\psi_{SR}\rangle$$

CPTP $\Rightarrow \mathcal{C}$: Take $\dim(R) = \dim(S)$, and "Bell state":
$$\rho = |\Omega\rangle\langle\Omega| \qquad \text{with} \qquad |\Omega\rangle = \sum_\alpha |\alpha\rangle_S \otimes |\alpha\rangle_R.$$

$$(\mathcal{C}_S \otimes \mathcal{I}_R)(\rho) =: \sigma_{SR} = \sum_i |\sigma_i\rangle\langle\sigma_i| \quad \text{by positivity}$$
$$\hookrightarrow \quad = \sum_{\alpha,\alpha'} \mathcal{C}(|\alpha\rangle\langle\alpha'|) \otimes |\alpha\rangle\langle\alpha'|$$

c. conj here so

important $|\kappa_i\rangle$ linear in $|\psi\rangle$

$$|\kappa_i\rangle_S = \langle\bar{\psi}_R|\sigma_i\rangle$$

Now:
$$\mathrm{tr}_R\left[\sigma_{SR}(I_S \otimes |\bar{\psi}_R\rangle\langle\bar{\psi}_R|)\right] =: \sum_i |\kappa_i\rangle\langle\kappa_i|$$
$$= \sum_{\alpha,\alpha'} \overline{\langle\psi|\alpha\rangle}\,\overline{\langle\alpha'|\psi\rangle}\, \mathcal{C}(|\alpha\rangle\langle\alpha'|) = \mathcal{C}(|\psi\rangle\langle\psi|).$$

But $|\kappa_i\rangle$ is a linear function of $|\psi\rangle$, so: $\quad |\kappa_i\rangle = K_i|\psi\rangle.$

Thus $\mathcal{C}(\rho) = \sum_i K_i \rho K_i^\dagger$. Trace-preserving comes as before. ☒

Goal of QEC: $\mathcal{D}(\mathcal{N}(\mathcal{E}(\rho))) = \rho$

decoder

noise/ error

encoder

logical data

sequence of channels: $\mathcal{D} \circ \mathcal{N} \circ \mathcal{E} = \mathcal{I}$
for suitable (decodable) $\mathcal{N}$

let's now foreshadow the essence of QEC....

Step 1: $\mathcal{E}$ encodes logical info in subspace (codespace):

$\text{Span}\{|000\rangle, |100\rangle, |010\rangle, |001\rangle, |110\rangle, |101\rangle, |011\rangle, |111\rangle\}$

But, need entanglement to protect against 2-errors too

Step 2: correctable $\mathcal{N}$ move out of codespace?

Step 3: decoder $\mathcal{D}$ deduces error and fixes it