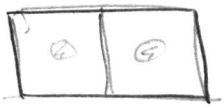
I. Introduction

Quantum Information: Study information processing w/ quantum mechanical systems.

- What IS quantum information/data?
- How can we store/transmit/process it?
- What can we do with it?
- How can we realize it physically?

Why study info. processing w/ q. mechanical systems? Isn't information indep. of physical realization?

Landauer (1961): Erasing information releases heat:



particle in box at unknown position:

1 bit of information

entropy $S_0 = k \ln 2$

particle at known position:

bit erased

entropy $S_1 = 0$.

$$\Rightarrow \quad \Delta S_{sys} = -k \ln 2 \quad \Rightarrow \quad \Delta Q_{env} = -T \Delta S_{sys} = kT \ln 2$$

⇒ Erasing 1 bit releases $\Delta Q = kT \ln 2$ heat.

⇒ "Information is physical"

(i.e.: we cannot think about information processing in physical systems w/out the physics)

Other motivation: "Moore's Law" → # transistors/chip doubles every 18 months

→ transistor size approaches atomic size!

→ must take into account q.m. effects

⇒ better to use them!

Basic ideas of Q. Info:

- Quantum bits (qubits):

Classical info:

basic unit: Bit $b = 0, 1$ (2 possibilities)

N bits: bit string $b_1 \dots b_N = 0\dots0, 0\dots01, 0\dots10, \dots$

2^N possibilities!

Quantum information:

basic unit: quantum bit $|b\rangle = |0\rangle, |1\rangle$
(qubit)

quantum mechanics: any superposition possible!

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

$\alpha, \beta \in \mathbb{C}$ → "infinitely many" possibilities!

N qubits:

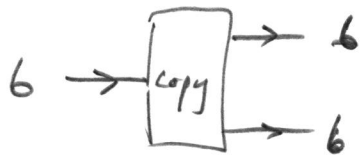
$$|\underline{b}\rangle = \alpha_{0\ldots0}|0\ldots0\rangle + \alpha_{0\ldots01}|0\ldots01\rangle + \ldots$$

2^N complex parameters!

→ Can we store/extract "infinitely much" information?

→ How to quantify amount of information?

e.g. Cloning: Can we copy information?

Classically: 

: works! ✓

Q. Mech: **NO!**

Why? $|0\rangle \xrightarrow{\text{copy}} |0\rangle\otimes|0\rangle$ (a)

$|1\rangle \xrightarrow{\text{copy}} |1\rangle\otimes|1\rangle$ (b)

$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \xrightarrow{\text{copy}} \frac{1}{2}(|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle)$

But linearity: (1)+(2):

$\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) \xrightarrow{(1)+(2)} \frac{1}{\sqrt{2}}(|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle)$

"No-cloning theorem"

Quantum information cannot be cloned!

⟹ Questions: How can we then store/transmit q. info? How can we deal w/ errors?

• Entanglement, teleportation, Bell inequalities

Consider two parties (Alice (A) & Bob (B)) sharing a quantum system:

with total state $|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B\right)$

(i) Alice & Bob measure in $\{|0\rangle, |1\rangle\}$ basis

→ outcomes <u>perfectly anti-correlated</u>!

Quantum feature? No, happens also for classical variables (e.g. gloves, Berkmann's socks)

(ii) But: outcomes in <u>all</u> bases are perfectly anti-correlated!

Is this non-classical?

<u>No</u>: local hidden variable (LHV) model:

each spin is described by a list of bits, one for each meas. direction (ϕ, ϑ):

$\sigma_A(\phi_A, \vartheta_A)$ and $\sigma_B(\phi_B, \vartheta_B)$ s.th.

$$\sigma_A(\phi, \vartheta) + \sigma_B(\phi, \vartheta) = 1$$

(or even prob. distributions)

$\Rightarrow$ perfect anti-corr. in <u>any bases</u> w/ "classical" model.

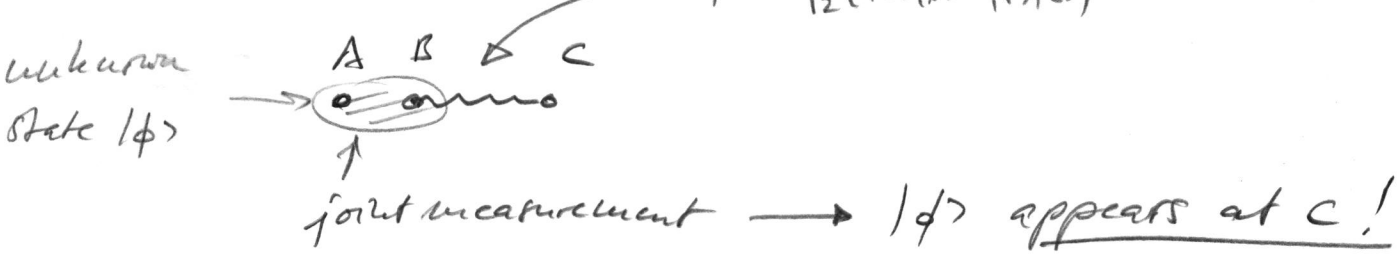
<u>But</u>: QM incompatible w/ <u>any</u> LHV model!

Bell inequalities

QM cannot be described by a <u>local</u> & <u>realistic</u> model!

<u>Teleportation</u>:

QI cannot be cloned: how to transport it over long distances?



$\longrightarrow |\phi\rangle$ <u>appears at C!</u>

But... doesn't this allow for faster-than-light communication?

No: State in C is "scrambled": meas. outcome is needed for unscrambling: must be communicated classically!

Note: The state of the system is teleported, not the system itself!

(A. Peres: "disembodied reincarnation")

- Quantum Computing:

  Build computer acting on quantum bits rather than classical bits: can process superposition of exp. many possibility: exponential speed-up?

  Subtle: Tricky to extract information!

  Shor '94: Quantum computer can factor numbers exponentially faster than any known class. method!

- Quantum error correction:

  Noise can destroy quantum info.

  How can we protect it?

  Classically: Make copies: $0 \to 000$, $1 \to 111$ (or smarter methods...)

Obs: $|0\rangle \longrightarrow |000\rangle$
$|1\rangle \longrightarrow |111\rangle$ } protected against bit flip

$$\frac{|0\rangle+|1\rangle}{\sqrt{2}} \longrightarrow \frac{|000\rangle+|111\rangle}{\sqrt{2}}$$

not protected against phase flip: $|0\rangle \to |0\rangle$
$|1\rangle \to -|1\rangle$

$$\frac{|000\rangle+|111\rangle}{\sqrt{2}} \longrightarrow \frac{|000\rangle-|111\rangle}{\sqrt{2}} \stackrel{\wedge}{=} \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

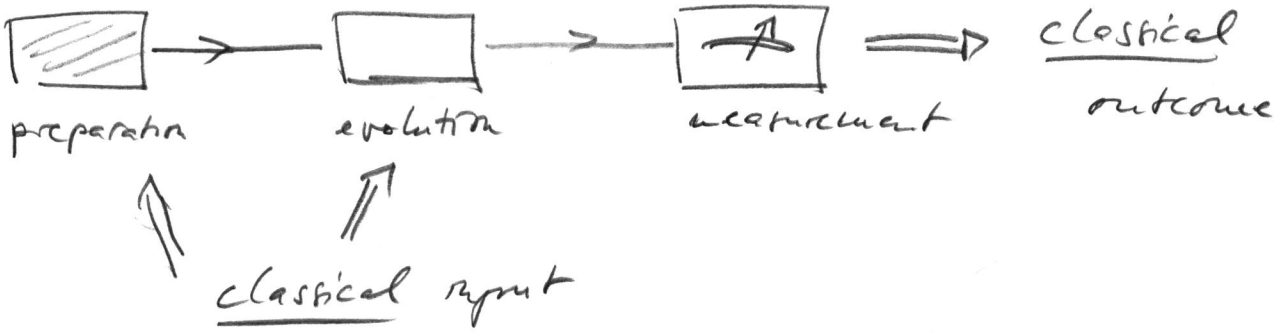
($\leftrightarrow$ cf. no-cloning thm.!)

$\Rightarrow$ Quantum Error Correction Codes (QECC) necessary!

II. The formalism: States, measurements, evolution

1. Pure states, unitary evolution, projective measurements

Q.M. setup:



Q.M. system ⟶ Hilbert space $\mathcal{H} \cong \mathbb{C}^d$

(Q. Info: typ. finite dim. H.S.)

State of system: vector $|\psi\rangle \in \mathcal{H}$ with $\||\psi\rangle\|^2 = \langle\psi|\psi\rangle = 1$.

(more precisely: rays $|\psi\rangle \sim e^{i\phi}|\psi\rangle$)

Use ket-bra notation:

$|v\rangle \in \mathbb{C}^d$: column vector

$\langle v| = (|v\rangle)^\dagger$: row vector

$\langle w|v\rangle$: scalar product $\left(\vec{w}^\dagger \vec{v} = \vec{w}^* \cdot \vec{v}\right)$

Basis notation:

"Computational basis" $|0\rangle, |1\rangle, \ldots |d-1\rangle$ of $\mathbb{C}^d$

$$|k\rangle \hat{=} e_k = \begin{pmatrix} 0 \\ \vdots \\ 1 \leftarrow k\text{'th position} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$|v\rangle = \sum_{k=0}^{d-1} v_k |k\rangle = \begin{pmatrix} v_0 \\ \vdots \\ v_{d-1} \end{pmatrix}$$

Linear operators:

$M : \mathbb{C}^d \longrightarrow \mathbb{C}^d$ is linear.

$$M(\alpha|v\rangle + \beta|w\rangle) = \alpha M(|v\rangle) + \beta M(|w\rangle)$$

Write $M|v\rangle \equiv M(|v\rangle)$.

Matrix notation / expansion:

$$M = \left(\sum_{i=0}^{d-1} |i\rangle\langle i|\right) M \left(\sum_{j=0}^{d-1} |j\rangle\langle j|\right) =$$

$$= \sum_{i,j=0}^{d-1} M_{ij} |i\rangle\langle j| = \begin{pmatrix} M_{00} & M_{01} & \cdots \\ M_{10} & \ddots & \\ \vdots & & \ddots \\ & & & M_{d-1,d-1} \end{pmatrix}$$

with $M_{ij} = \langle i|M|j\rangle$.

(i) Preparation:

Prepares known initial state $|\phi\rangle \in \mathbb{C}^d$.

(ii) Evolution:

Evolution = unitary transformation $U: \mathbb{C}^d \to \mathbb{C}^d$;

$$|\phi\rangle \longmapsto U|\phi\rangle.$$

U unitary $:\Longleftrightarrow U^\dagger U = UU^\dagger = \mathbb{1} \leftarrow \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

$$\left(\text{or: } \sum (U^\dagger)_{ij} U_{jk} = \sum \overline{U_{ji}}\, U_{jk} = \delta_{ik}\right)$$

(Note 1: $\langle\phi|U^\dagger U|\phi\rangle = \langle\phi|\phi\rangle = 1 \Rightarrow$ norm preserved, if and only if U unitary.)

(Note 2: U can in part. be generated by time evolution w/ Hamiltonian.)

(iii) Measurement:

Observable quantities $\equiv$ hermitian operator $A = A^\dagger$

Eigenvalue decomposition:

$$A = \sum_a a_a E_a \;;\quad E_a^2 = E_a = E_a^\dagger \text{ projector onto eigenspace } \left(\text{e.g. } E_a = |\psi_a\rangle\langle\psi_a|\right)$$

Measurement of A in state $|\phi\rangle$:

Outcome a_n w/ prob. $p_n = \langle\phi|E_n|\phi\rangle = \|E_n|\phi\rangle\|^2$

$\left(= |\langle\psi_n|\phi\rangle|^2\right)$

(Note: $\sum p_n = \langle\phi|\underbrace{\sum E_n}_{=1}|\phi\rangle = \langle\phi|\phi\rangle = 1$)

State after meas.:

$$|\phi_n\rangle = \frac{E_n|\phi\rangle}{\|E_n|\phi\rangle\|}$$

Expectation value:

$$\langle\phi|A|\phi\rangle = \sum a_n \langle\phi|E_n|\phi\rangle$$

2. Composite systems

Consider system w/ two <u>separate parts</u> ("subsystems")
A (= Alice) and B (= Bob).

$\Rightarrow$ Joint system: Hilbert space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.

What is general form of $|\phi\rangle \in \mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$?

$|i\rangle_A$ basis of $\mathcal{H}_A = \mathbb{C}^{d_A}$

$|j\rangle_B$ basis of $\mathcal{H}_B = \mathbb{C}^{d_B}$

$\Rightarrow |i\rangle_A \otimes |j\rangle_B \equiv |i\rangle_A |j\rangle_B \equiv |i,j\rangle_{AB} \equiv |ij'\rangle_{AB} \equiv |ij'\rangle$

is a basis of $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B = \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \cong \mathbb{C}^{d_A d_B}$,

$i = 0, \dots, d_A - 1$; $j = 0, \dots, d_B - 1$.

General state $|\phi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$:

$$|\phi\rangle_{AB} = \sum_{\substack{i=0,\dots,d_A-1 \\ j=0,\dots,d_B-1}} c_{ij} |i\rangle_A |j\rangle_B \quad : \quad d_A \cdot d_B - \text{dim. vector } (c_{ij})_{ij}$$

What if A acts w/ M_A on her system, and/or B w/ N_B resp.?

(Note: M_A, N_B could be unitaries, measurements (E_n), or "do-nothing", $N_B = \mathbb{1}_B$.)

Consider first $|\phi\rangle_{AB} = |i\rangle_A \otimes |j\rangle_B$.

Action of A should only change her system (as if B wasn't there):

$$|i\rangle_A \longmapsto \Pi_A |i\rangle_A \quad , \quad |i\rangle_A \otimes |j\rangle_B \longmapsto (\Pi_A |i\rangle_A) \otimes |j\rangle_B$$

Same for Bob, finally:

$$|i\rangle_A \otimes |j\rangle_B \longmapsto \Pi_A |i\rangle_A \otimes N_B |j\rangle_B$$

$$\equiv (\Pi_A \otimes N_B) |i\rangle_A \otimes |j\rangle_B$$

Linearity:

$$|\phi\rangle_{AB} \longmapsto (\Pi_A \otimes N_B) |\phi\rangle_{AB}$$

Matrix elements:

$$\langle i_A i_B | \Pi_A \otimes \Pi_B | j_A j_B \rangle = \langle i_A | \Pi_A | j_A \rangle \langle i_B | \Pi_B | j_B \rangle$$

$$\| \qquad\qquad\qquad\qquad \|$$

$$(\Pi_A \otimes \Pi_B)_{(i_A i_B),(j_A j_B)} \qquad (\Pi_A)_{i_A j_A} \cdot (N_B)_{i_B j_B}$$

$$\Pi_A \otimes N_B = \left(\begin{array}{c|c|c} (M_A)_{00} \cdot N_B & (\Pi_A)_{10} \cdot N_B & \cdots \\ \hline (\Pi_A)_{01} \cdot N_B & \cdots & \\ \hline \vdots & & \end{array}\right)$$

Examples:

Qubit: $\mathcal{H} = \mathbb{C}^2$,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \; ; \quad |\alpha|^2 + |\beta|^2 = 1$$

Observable $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \underbrace{|0\rangle\langle 0|}_{E_0} - \underbrace{|1\rangle\langle 1|}_{E_1}$

$a_0 = +1 \qquad a_1 = -1$

Measurement:

outcome $a_0 = +1$ w/ prob. $\langle\psi|E_0|\psi\rangle = |\alpha|^2$

outcome $a_1 = -1$ w/ prob. $\langle\psi|E_1|\psi\rangle = |\beta|^2$

Observable $X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \underbrace{|+\rangle\langle +|}_{E_+} - \underbrace{|-\rangle\langle -|}_{E_-}$

with $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$

Measurement: outcomes $\pm$ w/ prob. $\left|\langle \pm|(\alpha|0\rangle + \beta|1\rangle)\right|^2 = \frac{|\alpha \pm \beta|^2}{2}$

Evolution: $U = H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ "Hadamard gate"

$$U|\psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}(\alpha|0\rangle + \beta|1\rangle)$$

$$= \frac{\alpha+\beta}{\sqrt{2}}|0\rangle + \frac{\alpha-\beta}{\sqrt{2}}|1\rangle$$

Meas. in 2-basis $\{|0\rangle, |1\rangle\}$

outcome 0 w/ prob. $\frac{|\alpha+\beta|^2}{2}$

outcome 1 w/ prob. $\frac{|\alpha-\beta|^2}{2}$

H transforms betw. X and Z basis.

In fact, $H = |+\rangle\langle 0| + |-\rangle\langle 1| = |0\rangle\langle +| + |1\rangle\langle -| = H^\dagger$

Measurement on bipartite state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle)$$

Alice & Bob measure Z:

project onto $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

$\Rightarrow P_{01} = P_{10} = \frac{1}{2}$; $P_{00} = P_{11} = 0$

Alice & Bob measure X:

project onto $|++\rangle, |+-\rangle, |-+\rangle, |--\rangle$:

$|\langle ++|\psi\rangle|^2 = 0$

$|\langle +-|\psi\rangle|^2 = \left|-\frac{1}{2\sqrt{2}} - \frac{1}{2\sqrt{2}}\right|^2 = \frac{1}{2}$

$|\langle -+|\psi\rangle|^2 = \ldots = \frac{1}{2}$

$|\langle --|\psi\rangle|^2 = 0$

(using $\langle +|0\rangle = \langle +|1\rangle = \langle -|0\rangle = -\langle -|1\rangle = \frac{1}{\sqrt{2}}$)

$\Rightarrow$ perfect anti-correlation

(in fact, in any basis $\rightarrow$ Homework!)

Alice meas X, Bob meas Z:

$$|\langle +0|\psi\rangle|^2 = \left|-\tfrac{1}{2}\right|^2 = \frac{1}{4}$$

$$|\langle +1|\psi\rangle|^2 = \left|\tfrac{1}{2}\right|^2 = \frac{1}{4}$$

$$|\langle -0|\psi\rangle|^2 = \ldots = \frac{1}{4}$$

$$|\langle -1|\psi\rangle|^2 = \ldots = \frac{1}{4}$$

Outcomes for A & B are separately completely random,

but outcomes in the same basis are perfectly anti-corr.