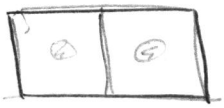
I. Introduction

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:

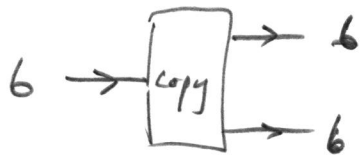
$$|\underline{b}\rangle = \alpha_{0\ldots0}|0\ldots0\rangle + \alpha_{0\ldots01}|0\ldots01\rangle + \ldots$$

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.

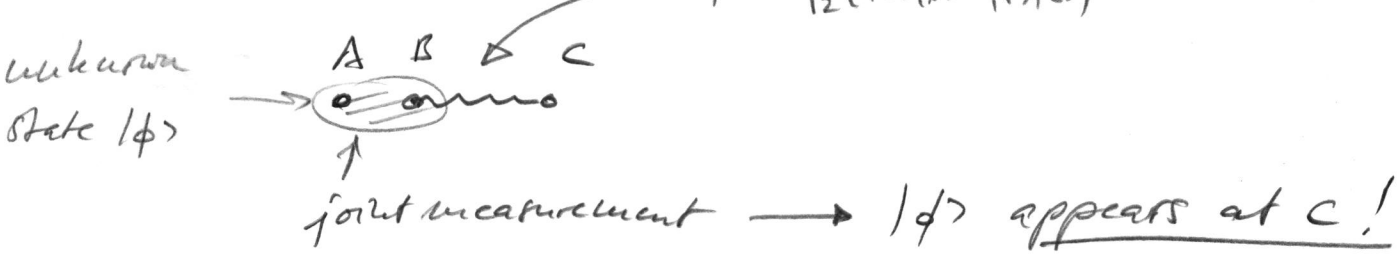
<u>But</u>: QM incompatible w/ <u>any</u> LHV model!

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: $|0\rangle \to |0\rangle$
$|1\rangle \to -|1\rangle$

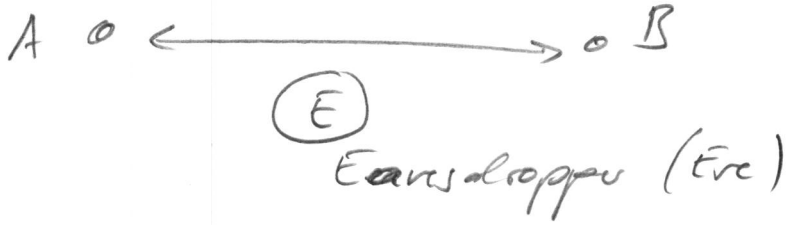
$$\frac{|000\rangle+|111\rangle}{\sqrt{2}} \longrightarrow \frac{|000\rangle-|111\rangle}{\sqrt{2}} \stackrel{\wedge}{=} \frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

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

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

• Quantum Cryptography

Can A & B establish a secret key (= random bits) through a public communication channel?



Class.: E can copy anything unnoticed!

QM: E must measure → disturbance →
→ eavesdropping can be detected!

E.g.: BB84 protocol (Bennett & Brassard '84):

1. Iterate: (i) A picks rand. bases $\{|\updownarrow\rangle, |\leftrightarrow\rangle\}$ or $\{|\nearrow\rangle, |\nwarrow\rangle\}$

iterate (ii) A send rand. bit (photon) photon polarization encoded in that basis

(iii) B meas. in rand. bases $\{|\updownarrow\rangle, |\leftrightarrow\rangle\}$ or $\{|\nearrow\rangle, |\nwarrow\rangle\}$

2. A & B compare bases: keep only cases w/ same bases.
→ those results should be identical for A & B.

3. A & B compare part of their outcome: if different, transmission line has been tampered with.

→ Q. Cryptography