

I. Introduction

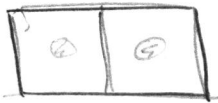
(1)

Quantum information: Study information processing of 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

$$\text{entropy } S_0 = k \ln 2$$



particle at
known position:

bit erased

$$\text{entropy } S_1 = 0.$$

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

⇒ 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 $s_1 \dots s_N = \underbrace{0 \dots 0, 0 \dots 01, 0 \dots 10, \dots}$

2^N possibilities!

Quantum information:

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

quantum mechanics: any superposition possible!

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

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

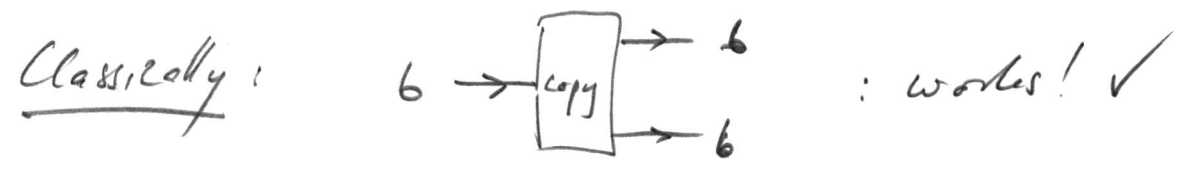
N qubits:

$$|b\rangle = \underbrace{\alpha_{0\dots 0}|0\dots 0\rangle + \alpha_{0\dots 01}|0\dots 01\rangle + \dots}$$

2^N complex parameters!

- \rightarrow Can we store/extract "infinitely much" information?
- \rightarrow How to quantify amount of information?

Cloning: Can we copy information?



Q. Tech: NO!

(4)

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

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

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

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

(5)

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



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

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

→ outcomes perfectly anti-correlated!

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

(ii) But: outcomes in all bases are perfectly
anti-correlated!

Is this non-classical?

No: Local hidden variable (LHV) model:

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

$b_A(\phi_A, \mathcal{D}_A)$ and $b_B(\phi_B, \mathcal{D}_B)$ s.t.

(6)

$$b_A(\phi, \mathcal{D}) + b_B(\phi, \mathcal{D}) = 1$$

(or even prob. distributions)

\Rightarrow perfect anti-corr. in any basis w/ "classical" model.

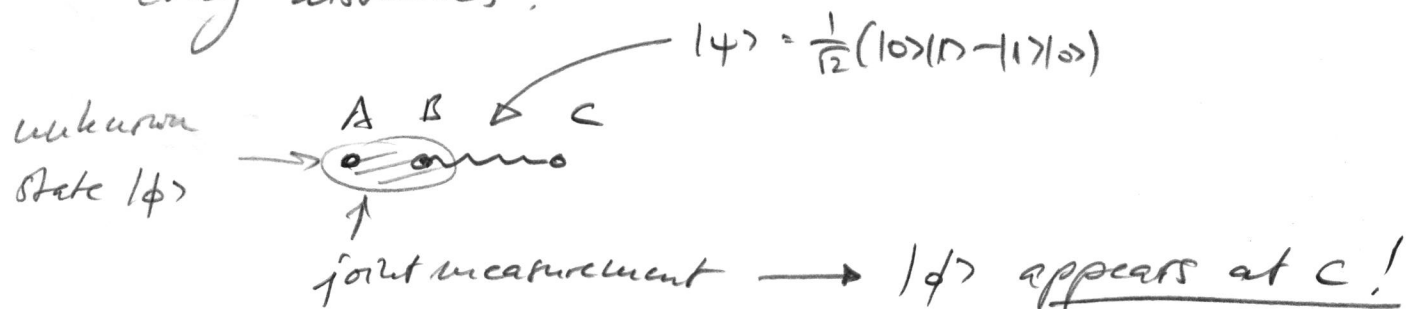
But: QM incompatible w/ any LHV model!

Bell inequalities

QM cannot be described by a local & realistic model!

Teleportation:

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



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

No: State in C is "scrambled": meas. outcome (7) is needed for unscrambling: must be communicated classically!

Note: The state of the system is teleported, not the system itself!
(A. Peres: "disembodied reincarnation")

o Quantum Computing:

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

Subtle: Tricky to extract information!

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

o Quantum error correction:

Noise can destroy quantum info.

How can we protect it?

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

Q7: $|0\rangle \rightarrow |000\rangle$
 $|1\rangle \rightarrow |111\rangle$ } protected against bit flip (8)

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

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

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

(\leftrightarrow cf. no-cloning theorem!)

\Rightarrow Quantum Error Correction Codes (QECC)

necessary!