Workshop Seminar: Intro to Quantum information and Computing

Jasper Roosmale Nepveu, 13 Dec 2022

References
- M. Nielsen and I. Chuang (2000) "Quantum Computing and Quantum Information"
- Lecture notes by John Preskill
(- J. Lykken, 2010.02931 "Quantum Information for Particle Theorists")

Motivation

Theoretical: Quantum Computers allow for the study of quantum phenomena in a controlled environment. Therefore, study QM itself, the "Entanglement frontier".

Applications:

- Quantum Simulations.
Classical computers are good at simulating e.g. n-body problem when analytic solutions don't exist. But when those n bodies are quantum mechanical, for example atoms and electrons forming molecules, classical computers are very inefficient. Quantum computers can simulate such systems to assist production of medicines. Much faster (hopefully) than doing

experiments, although experiments needed to confirm simulations.

- Quantum Calculations.
  Classical and Quantum computers can in principle calculate the same problems, but for some tasks QC are much more efficient. Especially useful when the solution to the problem can easily be confirmed on a ~~Quan~~ Classical C. (think of P=NP).

  prime example: Shor's algorithm for finding the prime factors of an integer.

- Quantum Communication, cryptography.
  For secure interchange of information.

This lecture

Some simple, standard examples to get a feeling for what separates the classical and quantum worlds // dealing with information ways of

Bit vs Qubit

Bit: $(0,1)$

Qubit: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$

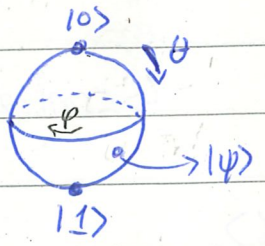
α, β are complex parameters, with a continuous range of possible values. Describing them classically (with infinite precision) requires infinitely many bits. Nature keeps track of this, but hides it: upon measurement, we find $(0,1)$. That is, one bit is accessible to us. The key is, of course, to smartly use the qubit before measuring.

Aside: Bloch sphere.

Change variables to

$$|\psi\rangle = e^{i\delta}\left(\cos\tfrac{\theta}{2}|0\rangle + e^{i\varphi}\sin\tfrac{\theta}{2}|1\rangle\right)$$

$\Rightarrow$ Single qubit is represented by a point on the sphere (where we ignore the overall phase)



This holds for a pure state; for a mixed state, that is, when the qubit is a subsystem of an entangled full system, the state resides inside the Bloch sphere

n bits, 2^n different states, $(0, \ldots, 2^n - 1)$

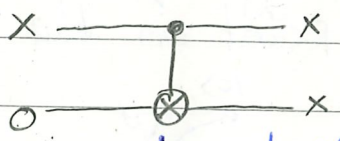
n qubits, $|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle$ (normalized)

IBM claims to have a computer with 433 qubits. This requires $2^{433} \approx 10^{130}$ complex variables to be described by a classical computer. Even with poor precision impossible.

The No-Cloning Theorem

Can we determine an unknown state by first cloning it many times and then measuring it many times? This would access the infinite amount of information in a qubit (and is impossible).

Classically fine:



↳ controlled Not (CNOT) gate

QC: $|x\rangle = \alpha|0\rangle + \beta|1\rangle$

$$|x\rangle|0\rangle \xrightarrow{\text{CNOT}} \alpha|00\rangle + \beta|11\rangle$$

$$\neq |x\rangle|x\rangle = \alpha^2|00\rangle + \alpha\beta(|01\rangle + |10\rangle) + \beta^2|11\rangle$$

unless $\alpha = 0$ or $\beta = 0$

More generally, suppose $U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$

then, if $U(|\varphi\rangle|\psi\rangle) = |\varphi\rangle|\varphi\rangle$

we find $\langle\varphi|\psi\rangle = \langle\varphi|\psi\rangle^2$

$\Rightarrow \langle\varphi|\psi\rangle = \{0,1\}$; a unitary evolution can only "clone" one specific basis. Not useful for unknown states.

Quantum parallelism and Deutsch's algorithm

Even though most quantum information is hidden to us, we can use superpositions and interference to extract global properties of functions. This is called quantum parallelism and is one of the principles underlying Shor's algorithm.

Problem: Suppose we have a function

$$f: x \to f(x), \{0,1\} \to \{0,1\}$$

with only evaluating the function once, can we determine whether

$$f(0) = f(1) \quad \text{or} \quad f(0) \neq f(1) \; ?$$

Classically: No

QC: the function is implemented as

$$U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$$

because the evolution must be unitary.

Try (too naive):

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2}}(|0\, f(0)\rangle + |1\, f(1)\rangle)$$

4 options:

$$\frac{1}{\sqrt{2}} \begin{cases} |00\rangle + |10\rangle \\ |01\rangle + |11\rangle \end{cases} \Big\} f(0) = f(1)$$

$$\frac{1}{\sqrt{2}} \begin{cases} |01\rangle + |10\rangle \\ |00\rangle + |11\rangle \end{cases} \Big\} f(0) \neq f(1)$$

These possibilities cannot be distinguished with certainty, because they don't form an orthonormal basis.

Basis choices are $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)$

or $\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)\right)$

But $\frac{1}{\sqrt{2}}(00 + 10) = \frac{1}{2}\frac{1}{\sqrt{2}}\big((00+11) + (00-11) + (01+10) - (01-10)\big)$

Better to start with

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\xrightarrow{U_f} \frac{1}{2}|0\rangle(|f(0)\rangle - |\overline{f(0)}\rangle) + \frac{1}{2}|1\rangle(|f(1)\rangle - |\overline{f(1)}\rangle)$$

where $|1 \oplus x\rangle = \text{Not}\,|x\rangle = |\bar{x}\rangle$

$$= \frac{1}{2}|0\rangle(-1)^{f(0)}(|0\rangle - |1\rangle) + \frac{1}{2}|1\rangle(-1)^{f(1)}(|0\rangle - |1\rangle)$$

$$= \frac{1}{\sqrt{2}}\left((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right)\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Now, measure the first qubit in the basis $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$

If $f(0) = f(1)$, always returns $|+\rangle$

If $f(0) \neq f(1)$, always returns $|-\rangle$

For global properties of a function, a quantum computer is much more efficient than a classical computer as it requires only one evaluation (relevant when there are more variables).

Communication: Superdense Coding.

Alice ~~se~~ prepares the maximally entangled quantum state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and sends one of her qubits to Bob.

Imagine that Eve tries to intercept the qubit, ~~measure~~ entangle with it and pass it on to Bob, hoping that he will not notice.

A and B expect that they have shared the state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

while in fact Eve's interaction may have transformed the state into

$$|00\rangle|e_{00}\rangle + |01\rangle|e_{01}\rangle + |10\rangle|e_{10}\rangle + |11\rangle|e_{11}\rangle$$

For safety, A and B send 20 qubits to each other, so that they can test on 19 if they have been tampered with. Beforehand Eve does not know which single qubit they will end up using for their secret information.

In that case, A and B can measure their qubits in the (0,1) basis (and can share their results publicly). They expect to agree each time, such that they confirm that they ~~are~~ were in the state

$$|00\rangle|e_{00}\rangle + |11\rangle|e_{11}\rangle$$

(if not, they know there was an evesdropper)

Then, A and B can measure some other qubits in the $|\pm\rangle$ basis, to confirm that they don't get a minus sign if both qubits flip.

In this way, they distinguish

$$(|00\rangle + |11\rangle)|e\rangle \quad \text{and} \quad (|00\rangle - |11\rangle)|e\rangle$$

and other states when Eve has broken the correlation

If the phase comes out as expected, they know that they are safe. Even if Eve was present, the state $(|00\rangle + |11\rangle)|e\rangle$ shows that Eve cannot be correlated with the other qubits.

This is an example of "Monogamy": if 2 qubits are maximally entangled, they cannot entangle with a third without destroying the initial correlations. Evesdropping is noticed.

Now, A and B can measure their qubit in the (0,1) basis. They find one bit of information which only they know.
⇒ They have shared a private key

Alternatively, Alice can now share 2 qubits of information with a single bit, as follows: (note that the first bit did not carry any information, because

they always agree to share the same state).

A and B have shared the state

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$
$$\quad A\ B \qquad\quad A\ B$$

By manipulating her qubit, Alice can drive the total system to one of 4 possible orthonormal states (which can be distinguished by a measurement on the full system).

Message 1, A does nothing, $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

2, Phase flip: $|0\rangle \to |0\rangle$, $|1\rangle \to -|1\rangle$, $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$

3, Not gate: $|0\rangle \to |1\rangle$, $|1\rangle \to |0\rangle$, $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

4, First Not gate then phase flip

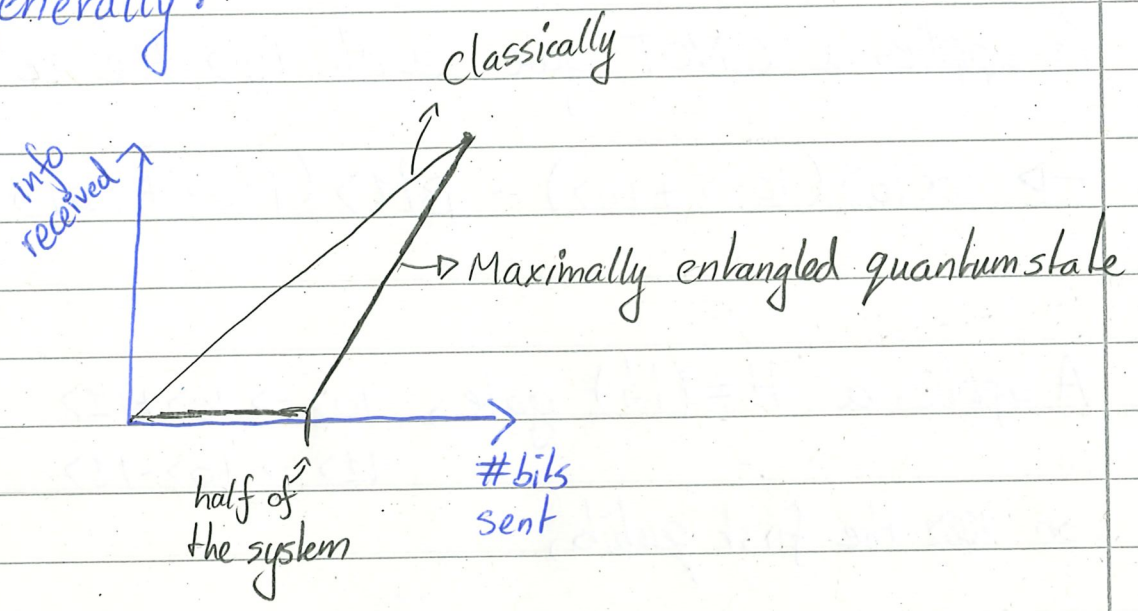
$$\to \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Alice now sends her qubit to Bob as well. By measuring the total system Bob receives one of the 4 messages.

The information is not accessible locally. Eve may intercept the second qubit, but

her measurements will convey no info.

generally:



Quantum information is "locally inaccessible." It is encoded in the entanglement.

Quantum Teleportation

A and B again share a maximally entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

A wants to send $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to B, but she doesn't know the state and can only communicate classically

Full system: $\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)$ (A, A B)

A applies a CNOT gate with $|\psi\rangle$ the control

$\rightarrow \alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)$

A applies a $H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ gate, $|0\rangle \rightarrow |0\rangle + |1\rangle$
$|1\rangle \rightarrow |0\rangle - |1\rangle$
on the first qubits,

$\rightarrow \alpha(|0\rangle + |1\rangle)(00 + 11) + \beta(0 - 1)(10 + 01)$

$= 00(\alpha 0 + \beta 1) + 01(\alpha 1 + \beta 0)$
$+ 10(\alpha 0 - \beta 1) + 11(\alpha 1 - \beta 0)$

A measures here 2 qubits.

If she finds $|00\rangle$, Bob should do nothing with his qubit. It is $|\psi\rangle$!

If $|01\rangle$, B should do a Not gate
if $|10\rangle$, B should do a phase flip
if $|11\rangle$, B should first do a Not
then do a Phase flip.

B has "received" $|\psi\rangle$, which has been destroyed on Alice's side