Quantum Computing
Lecture 5

Anuj Dawar

Applications of Quantum Information

Some Applications

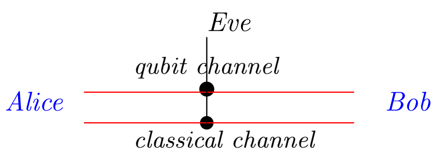
We look at some applications of the encoding of information in quantum states.

- *Quantum Cryptography*, or more accurately *Quantum Key Distribution*.
- *Superdense Coding*.
- *Quantum Teleportation*

These do not rely on *quantum computation* as such, but the properties of information encoded in quantum states: *superposition* and *entanglement*.

Quantum Key Distribution

A protocol for *quantum key distribution* was described by Bennett and Brassard in 1984 (and is known as BB84).



The protocol does not provide the means of transmitting an arbitrary message.

At the end of the protocol, there is a *random* sequence of bits that is shared between *Alice* and *Bob* but unknown to any third party.

Assumptions

The BB84 protocol relies on the following assumptions:

- *Alice* has a source of random (classical) bits.
- *Alice* can produce *qubits* in states $|0\rangle$ and $|1\rangle$.
- *Alice* can apply a *Hadamard operator* H to the qubits.
- *Bob* can measure incoming qubits
  - either in the basis $|0\rangle$, $|1\rangle$;
  - or in the basis $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

These conditions are satisfied, for instance, by a system based on polarised photons.

The Protocol

Alice sends *Bob* a stream of qubits.

For each qubit, before sending it, she

- *randomly* chooses a bit $|0\rangle$ or $|1\rangle$;
- *randomly* either applies H to the qubit or not; and
- sends it to *Bob*.

So, *Bob* receives a random sequence of qubits, each of which is in one of the four states:

$$|0\rangle, |1\rangle, H|0\rangle, H|1\rangle$$

The Protocol–contd.

- For each qubit, *Bob* *randomly* chooses either the basis $|0\rangle$, $|1\rangle$ or the basis $H|0\rangle$, $H|1\rangle$ and measures the qubit in the chosen basis.
- *Bob* announces (over the classical channel) which basis he used for each measurement.
- *Alice* tells *Bob* which measurements were made in the correct basis.
- The qubits which were measured in the wrong basis are discarded, while the rest form a shared key.

Attacks

Why not announce the bases for all qubits before transmission, thus avoiding the loss of half the bits?

> This allows *Eve* to intercept, measure and re-transmit the bits.

Why not wait until *Bob* has received all the qubits, then have *Alice* announce the basis for each one before *Bob* measures them?

- Requires *Bob* to store the qubits—currently technically difficult.
- If *Bob* can store the qubits, then *Eve* can too and then she can retransmit after measurement.

If we could fix the basis before hand, this could be used to transmit a *fixed* (rather than random) message.

Attack 2

What happens if *Eve* intercepts the qubits, measures each one randomly in either the basis $|0\rangle$, $|1\rangle$ or the basis $H|0\rangle, H|1\rangle$ and then retransmits it?

For half of the bits *that are shared between* Alice *and* Bob, *Eve* will have measured them in the wrong basis.

Moreover, these bits will have changed state, and so for approx. $\frac{1}{4}$ of the *shared* bits, the value measured by *Bob* will be different to the one encoded by *Alice*.

Alice and *Bob* can choose a random sample of their shared bits and publically check their values against each other and detect the presence of an eavesdropper.

Attack 3

Could *Eve* intercept the qubits, make a copy *without measuring them* and re-transmit to *Bob* and then wait for the basis to be announced?

> *No Cloning Theorem:*
> There is no *unitary operation* U which for an arbitrary state ψ gives
> $$U|\psi 0\rangle = |\psi\psi\rangle.$$

Exercise: Prove the no-cloning theorem.

Key Distribution

Quantum key distribution relies on nothing more than

- linear superposition of states; and
- change of basis.

In particular, it does not rely on *entanglement*.

We next look at some applications of entanglement.

Bell States

Entanglement based protocols generally rely on using the following four states of a two-qubit system, known as the *Bell states*.

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

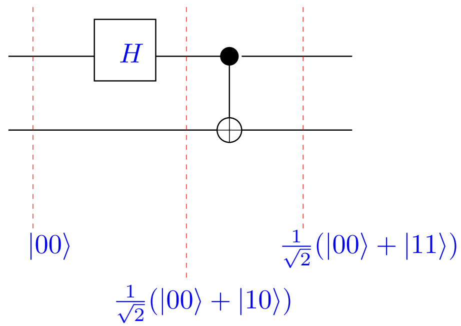
$$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \quad \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

These form an orthonormal basis for $\mathbb{C}^4$, known as the *Bell basis*.

Note that, in each of the states, measuring either qubit in the computational basis yields $|0\rangle$ or $|1\rangle$ with equal probability, but after the measurement, the other bit is determined.

Generating Bell States

We can generate the Bell states from the computational basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ using the following circuit:



Superdense Coding

In general, it is impossible to extract more than one classical bit of information from a single qubit.

However, if *Alice* and *Bob* is each in possession of one qubit of a pair in a known Bell state

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Then *Alice* can perform an operation *solely* on her own qubit, and then send it to *Bob* to convey two bits of information.

Superdense Coding 2

Generating *Bell states* from $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with only operations on the first qubit.

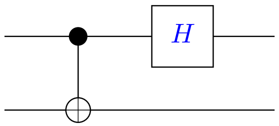
$$(X \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$

$$(Z \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$((ZX) \otimes I)\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Superdense Coding 3

Once he has both qubits, *Bob* can convert back to the computational basis using the circuit.



After this, a measurement in the computational basis yields the two bits that *Alice* intended to convey.

Quantum Teleportation

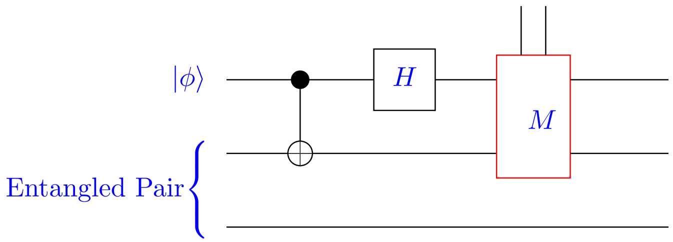
The *superdense coding* protocol allows *Alice* to send *Bob* two classical bits by transmitting a single qubit, *provided they already share an entangled pair*.

Conversely, the *quantum teleportation* protocol allows *Alice* to send *Bob* a qubit, by sending just *two classical bits* along a classical channel, *provided they already share an entangled pair*.

Contrast this with the *no-cloning theorem*, which tells us that we cannot make a copy of a qubit.

Quantum Teleportation 2

Alice has a state $|\phi\rangle$ that she wishes to transmit to *Bob*. The two already share a pair of qubits in state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.



Quantum Teleportation 3

Alice conveys to *Bob* the result of her measurement. Say the qubit in Bob's possession is in state $|\theta\rangle$, then:

- If *Alice* measures $|00\rangle$, then $|\phi\rangle = |\theta\rangle$.
- If *Alice* measures $|01\rangle$, then $|\phi\rangle = X|\theta\rangle$.
- If *Alice* measures $|10\rangle$, then $|\phi\rangle = Z|\theta\rangle$.
- If *Alice* measures $|11\rangle$, then $|\phi\rangle = XZ|\theta\rangle$.

Thus, *Bob* performs the appropriate operation and now has a qubit whose state is exactly $|\phi\rangle$.