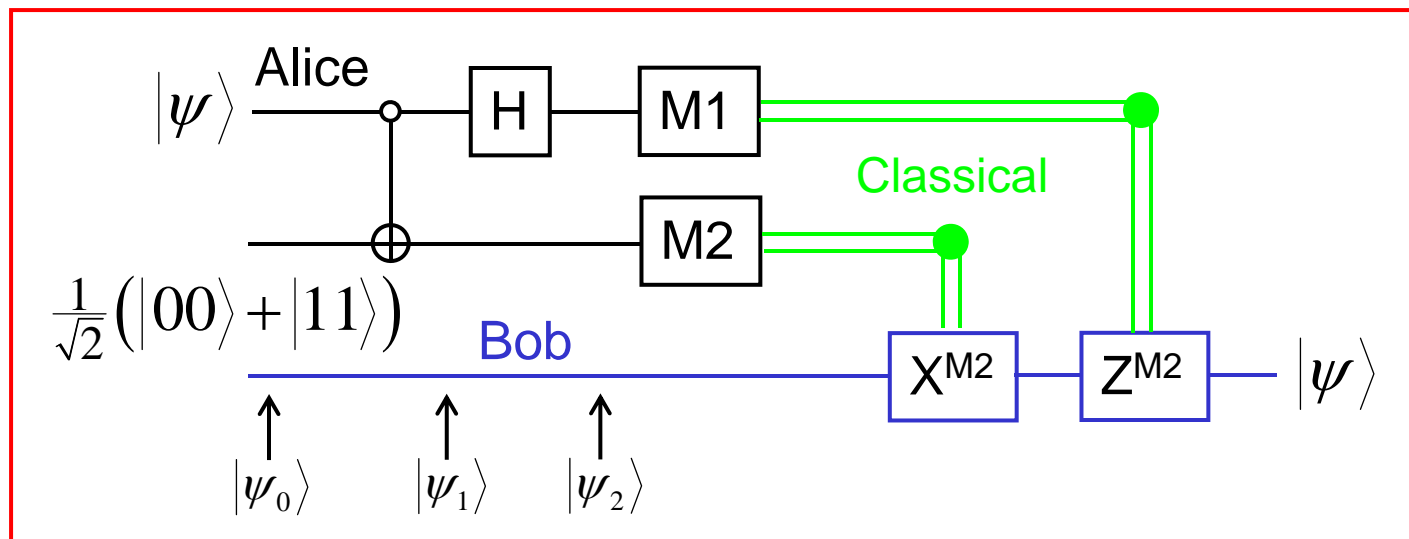


Advanced Quantum Physics

Lecture 23



David Ritchie

www.sp.phy.cam.ac.uk/~dar11/pdf

Section 6: Quantum Information



6.1 Quantum bits, gates and circuits

6.2 Teleportation

6.3 Quantum computing

6.4 Quantum cryptography

Recommended book:

“Quantum computation and quantum information”

M A Nielsen and I L Chuang

Quantum bits

- Quantum computation and quantum information are built on the idea of the qubit.
- This is analogous to the bit in conventional computing but uses the properties of superpositions of quantum mechanical states.
- A classical bit has a state – either 0 or 1
- The qubit also has states $|0\rangle$ or $|1\rangle$.
- But the qubit can also be in other linear combination or *superposition* states:

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

where α and β are complex numbers.

- So the qubit is a vector in a two-dimensional complex vector space where $|0\rangle$ and $|1\rangle$ form an orthonormal basis.
- With conventional computers we can examine a bit to see if it is in state 0 or 1 but, with quantum states we cannot get such precise information.

Quantum bits (2)

- If we examine a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ to find its quantum state
- We either get the result 0 with probability $|\alpha|^2$ or 1 with probability $|\beta|^2$ where $|\alpha|^2 + |\beta|^2 = 1$.
- So the qubit is a *unit* vector in a two-dimensional complex vector space.
- The dichotomy between the unobservable state of a qubit and the observations that are possible makes it difficult to intuitively understand the quantum system but is crucial to quantum information.
- However it is possible to manipulate qubits to give measurable results which depend on the properties of the state.
- Qubits can have a number of physical realisations, for example:
 - The polarisation of a photon.
 - The alignment of a spin in a magnetic field
 - Two states of an electron in an atom.

Quantum bits (3)

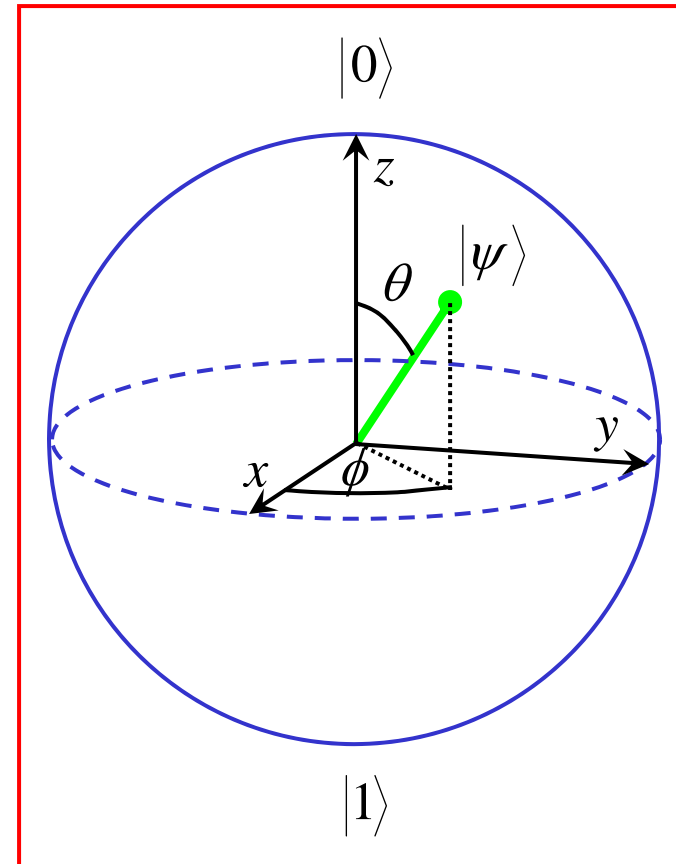
- We can represent the qubit in a geometrical way.
- Since $|\alpha|^2 + |\beta|^2 = 1$ we can write for real θ, ϕ, γ :

$$|\psi\rangle = e^{i\gamma} \left(\cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi} \sin\left(\frac{\theta}{2}\right)|1\rangle \right)$$

- And since the phase factor has no observable effects we can write:

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

- θ and ϕ define a point on the unit 3D sphere, known as a Bloch sphere - this is a useful representation of a qubit.
- If the qubit is in state $|0\rangle$ it is represented by a vector pointing in the $+z$ direction then $\theta = 0$, if it is state $|1\rangle$ then $\theta = \pi$ and the vector points in the $-z$ direction.



Bloch sphere
representation of a qubit

Two qubits

- Consider two qubits.
- If we had two classical bits then there would be 4 possible states :
00,01,10,11
- Two qubits have 4 possible basis states: $|00\rangle, |01\rangle, |10\rangle, |11\rangle$
- A pair of qubits can also exist in superpositions of these four states.

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

- In a similar way to a single qubit, a measurement x resulting in one of the values 00,01,10,11 occurs with a probability $|\alpha_x|^2$.
- So if you measure just the first qubit and get the value 0, with a probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$ then you have a post measurement state:

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$$

- The wavefunction has collapsed into this state as a result of the measurement – in line with postulate no. 4 (lecture 1).

Bell states

- The following are known as the *Bell* states:

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

- Consider the first state, if you measure the first qubit there are two possible results:

- 0 with probability $\frac{1}{2}$ leaving the post measurement state: $|\psi'\rangle = |00\rangle$

- 1 with probability $\frac{1}{2}$ and a post measurement state: $|\psi'\rangle = |11\rangle$

- The measurement of the second qubit always gives the same result as that of the first –measurement outcomes are correlated and the single particle states are *entangled*.


- J S Bell used similar arguments to show that the measurement correlations in this state are stronger than could ever exist between classical systems.

Quantum gates

- Classical computers contain many logic gates – the simplest is the NOT gate where: $0 \rightarrow 1, 1 \rightarrow 0$

- For a quantum system if we have a process $|0\rangle \rightarrow |1\rangle, |1\rangle \rightarrow |0\rangle$ this does not tell us what happens to the superposition of the two states.

- In fact the quantum NOT gate acts linearly: $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|1\rangle + \beta|0\rangle$ and can be represented by the matrix:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ acting on: } \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad \text{so} \quad X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$


- To represent quantum gates in this way by a matrix U , the only condition is that U must be unitary: $UU^\dagger = 1$

- There are several other useful single qubit gates:

- The Z gate: $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ leaves $|0\rangle$ unchanged and flips the sign of $|1\rangle$ to give $-|1\rangle$.
so: $\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|0\rangle - \beta|1\rangle$

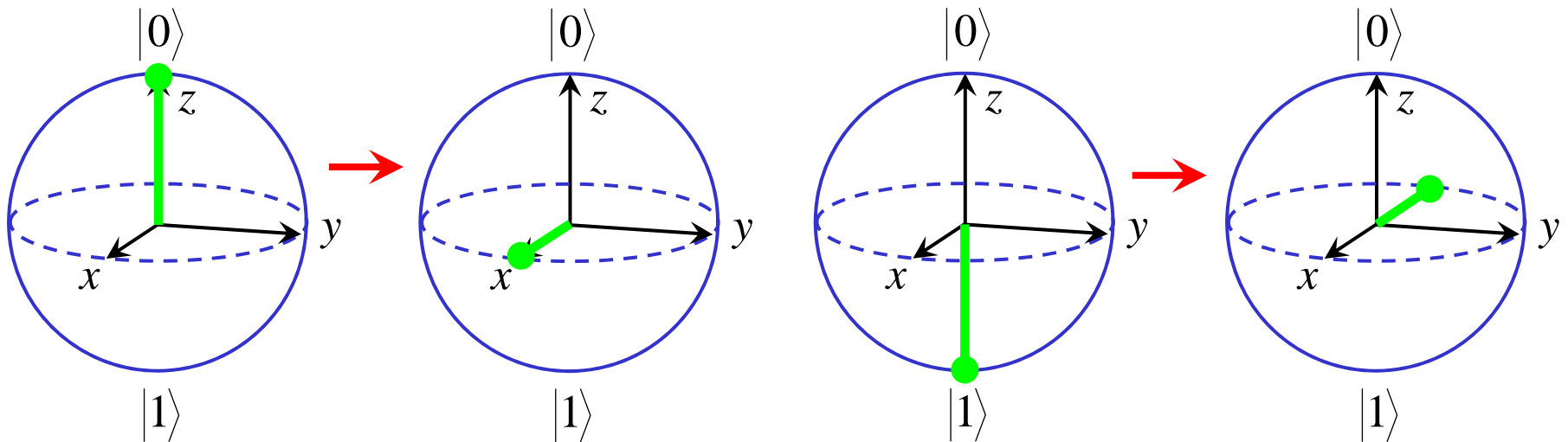
Quantum gates (2)

•The *Hadamard* gate: $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

transforms:

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

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



•This operation corresponds to a rotation of $\frac{\pi}{2}$ about the y-axis followed by a rotation of π about the x-axis.

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

Quantum gates (3)

- An arbitrary unitary 2x2 matrix can be written in the following way:

$$U = e^{i\alpha} \begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{-i\beta/2} \end{bmatrix} \begin{bmatrix} \cos\left(\frac{\gamma}{2}\right) & -\sin\left(\frac{\gamma}{2}\right) \\ \sin\left(\frac{\gamma}{2}\right) & \cos\left(\frac{\gamma}{2}\right) \end{bmatrix}$$

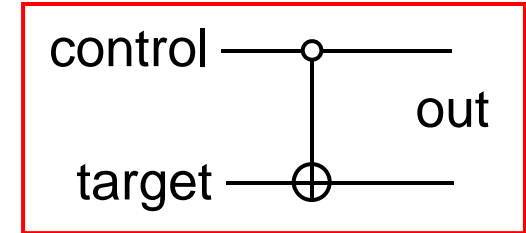
- This is the product of two rotations and a phase shift.
- So any quantum gate can be defined in terms of a small set of operations giving the appropriate values of α, β, γ .
- In classical logic gates any function on bits can be computed with the use of NAND gates alone – this type acts as a *universal* gate.
- The prototypical multi-qubit logic gate is the controlled-not or CNOT gate.
- This gate has two input qubits, known as the control qubit and the target qubit, the action of the gate is:
- If the control qubit is set to 0 the target qubit is left alone, if the control qubit is set to 1 the target qubit is flipped, so with $|control, target\rangle$:

$$|00\rangle \rightarrow |00\rangle, \quad |01\rangle \rightarrow |01\rangle, \quad |10\rangle \rightarrow |11\rangle, \quad |11\rangle \rightarrow |10\rangle$$

Quantum gates (4)

- From the last slide for the CNOT gate:

$$|00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |01\rangle, |10\rangle \rightarrow |11\rangle, |11\rangle \rightarrow |10\rangle$$



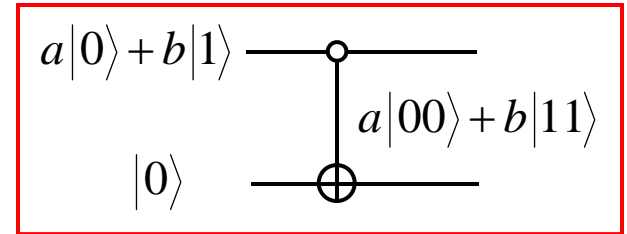
- We can represent the two qubit states as 4x1 vectors and the CNOT gate as a 4x4 matrix,

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \quad U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

- Again the requirement that probability is conserved means that: $U_{CN} U_{CN}^\dagger = I$
- The unitary requirement means that quantum gates are always reversible – the action of one quantum gate can always be undone by another.
- Classical gates are not reversible – there is an irretrievable loss of information.
- Any multiple qubit logic gate may be made from single qubit gates and the CNOT gate – the quantum parallel of NAND gate universality.

Qubit copying?

- Let us try to copy a qubit in the unknown state $|\psi\rangle = a|0\rangle + b|1\rangle$ by using it as the control input for a CNOT gate with target input $|0\rangle$.



- The input state of the two qubits may be written:

$$[a|0\rangle + b|1\rangle]|0\rangle = a|00\rangle + b|10\rangle$$

- The CNOT gate negates the second (target) qubit when the first (control) qubit is 1. The output is thus $a|00\rangle + b|11\rangle$.
- Have we successfully copied $|\psi\rangle$ and created $|\psi\rangle|\psi\rangle$?
- When $|\psi\rangle = |0\rangle$ or $|\psi\rangle = |1\rangle$ this is correct – we are able to use quantum circuits to copy classical information.
- However for a general state $|\psi\rangle = a|0\rangle + b|1\rangle$ we have:

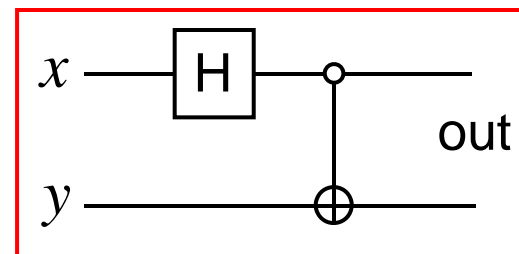
$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle$$

and unless $ab = 0$ we find that the copying circuit does not copy the input quantum state.

It is impossible to copy a quantum state – the ‘*no-cloning theorem*’.

Circuit to create Bell states

- A circuit with two qubit input (x, y) .
- A Hadamard gate acts on x and then feeds the control input of a CNOT.
- The other input qubit, y , forms the target input of the CNOT gate.
- The output of the circuit is the output of the CNOT gate.



- The Hadamard gate puts qubit x into a superposition:

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

- This superposition state then controls the CNOT gate and $|xy\rangle$ becomes:

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

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

- These are the Bell states.

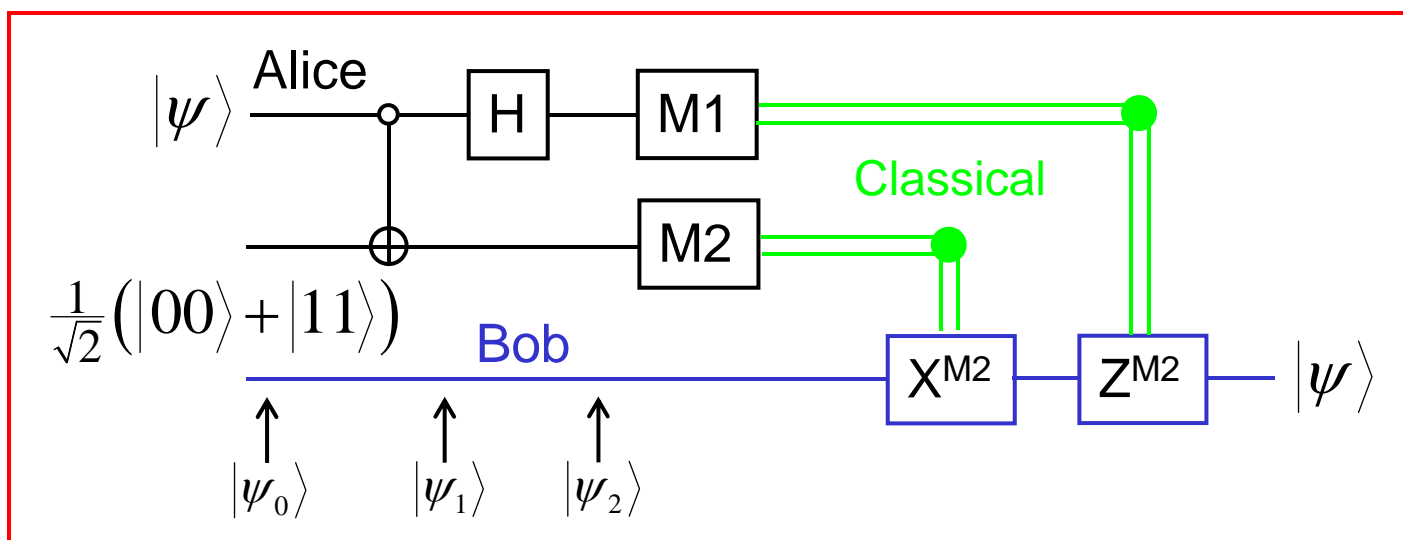
Quantum teleportation

- This is a technique for transferring quantum states – even where there is no quantum communication channel between the sender (Alice) and receiver (Bob)*.
- Alice and Bob generate a Bell state comprising two entangled qubits.
- Each takes one of the two qubits with them.
- Some time later Alice wishes to deliver another qubit $|\psi\rangle$ to Bob but she doesn't know the state of the qubit and the laws of quantum mechanics prevents her finding out as she only has a single copy.
- In addition to this she can only send classical information.
- Even if Alice knows what $|\psi\rangle$ is precisely it would take an infinite amount of classical information (since it can take values in a continuous space) to describe this state.
- Quantum teleportation is a way of using the entangled Bell state to send the state $|\psi\rangle$ to Bob using only a small amount of classical communication.

*Proposed by C H Bennett et al Phys Rev Lett 70, 1895 (1993)

Quantum teleportation (2)

- To send the qubit:
- Alice interacts $|\psi\rangle$ with her half of the entangled Bell state.
- She then measures the two qubits she has and obtains one of 4 possible classical results 00,01,10,11.
- Alice sends this information to Bob who depending on the message undertakes one of four different operations on his half of the Bell state and as a consequence recovers the state $|\psi\rangle$.
- We can describe this process with a circuit:



Quantum teleportation (3)

•If the state to be teleported is: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ where α and β are unknown.

•The input to the circuit is:

$$|\psi_0\rangle = |\psi\rangle \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}} [\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)]$$

where the first 2 qubits in each term belong to Alice and the third to Bob.

•Alice puts her qubits through a CNOT gate with $|\psi\rangle$ fed into the control input and her qubit from the entangled state the target qubit.

$$|\psi_1\rangle = \frac{1}{\sqrt{2}} [\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)]$$

$ control, target\rangle$	
$ 00\rangle$	$\rightarrow 00\rangle$
$ 01\rangle$	$\rightarrow 01\rangle$
$ 10\rangle$	$\rightarrow 11\rangle$
$ 11\rangle$	$\rightarrow 10\rangle$

•Alice sends the first qubit through a Hadamard gate:

$$|\psi_2\rangle = \frac{1}{2} [\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]$$

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

Quantum teleportation (4)

•The last slide: $|\psi_2\rangle = \frac{1}{2} [\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]$

•Which can be written:

$$|\psi_2\rangle = \frac{1}{2} \left[\begin{aligned} &|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) \\ &+ |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle) \end{aligned} \right]$$

remembering the first 2 qubits in each term belong to Alice, the third to Bob.

•If Alice now performs a measurement and obtains the result $|00\rangle$ then Bob's qubit is in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ similarly:

$$|01\rangle \Rightarrow (\alpha|1\rangle + \beta|0\rangle), \quad |10\rangle \Rightarrow (\alpha|0\rangle - \beta|1\rangle), \quad |11\rangle \Rightarrow (\alpha|1\rangle - \beta|0\rangle)$$

•If Alice tells Bob the outcome of her measurements then he knows which state his qubit is in and he can recover $|\psi\rangle$ by applying the appropriate quantum gate.

$$|00\rangle \Rightarrow (\alpha|0\rangle + \beta|1\rangle) = |\psi\rangle, \quad |01\rangle \Rightarrow X(\alpha|1\rangle + \beta|0\rangle) = |\psi\rangle,$$

$$|10\rangle \Rightarrow Z(\alpha|0\rangle - \beta|1\rangle) = |\psi\rangle, \quad |11\rangle \Rightarrow ZX(\alpha|1\rangle - \beta|0\rangle) = |\psi\rangle$$

$$Z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$$

$$X(\alpha|0\rangle + \beta|1\rangle) = \alpha|1\rangle + \beta|0\rangle$$

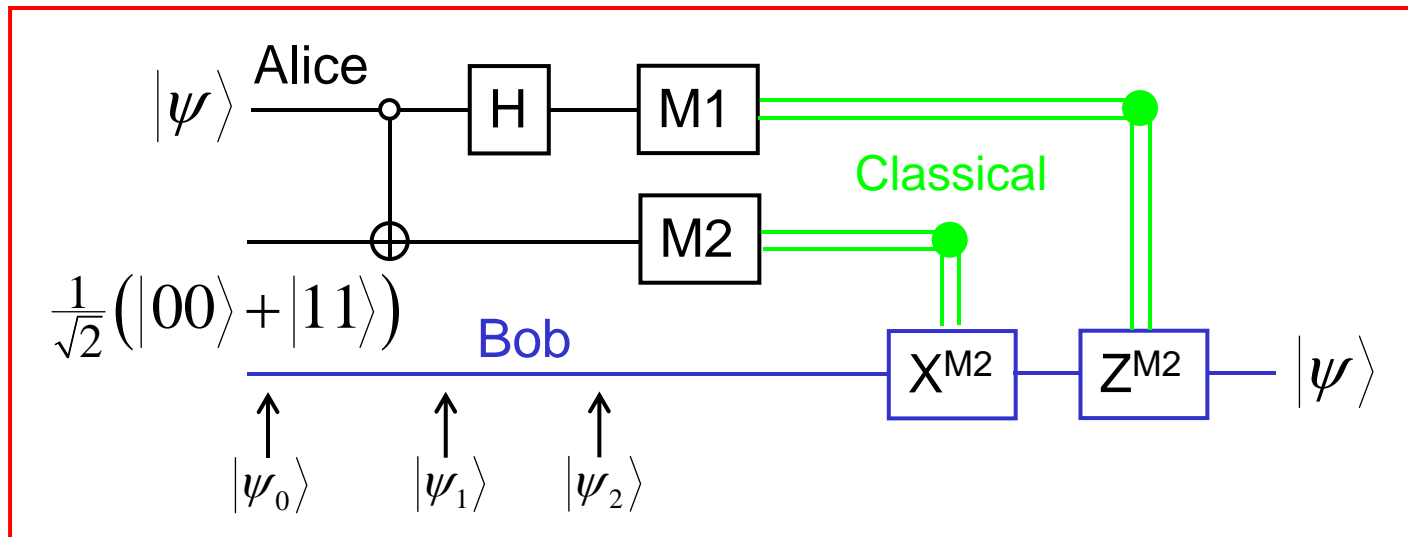
Quantum teleportation (5)

- This result does not imply that information is transferred faster than the speed of light – Alice must transmit her measurement result to Bob over a classical communication link.
- This technique also appears to create a copy of the state $|\psi\rangle$ -but the original $|\psi\rangle$ no longer exists!
- Teleportation was first demonstrated using light by Bouwmeester et al, Nature **390**, 575 (1997).
- Recent results have demonstrated teleportation of atomic states, M Rieble et al Nature **429**, 734 (2004) & M D Barrett et al Nature **429**, 737 (2004).

Lecture 23 - Summary

- Qubits – analogous to bits in computing but use superposition of quantum states. Representation in terms of a Bloch sphere.
- Two qubits, Bell states and entanglement.
- Quantum gates: NOT, Hadamard and CNOT gates.
- Qubit copying is not possible – the *no-cloning* theorem.
- A quantum gate circuit comprising a Hadamard gate and a CNOT gate is used to create Bell states.
- Quantum teleportation – a technique for transferring quantum states.

Lecture 23



The End!!

(www.sp.phy.cam.ac.uk/~dar11/pdf)