G53NSC and G54NSC
Non-Standard Computation

Dr. Alexander S. Green

23rd of February 2010

Introduction

- Last week we looked at multiple qubits and Entanglement
- Today, we are going to look at some simple quantum algorithms:
- Superdense Coding
- Quantum Teleportation
- Deutsch's algorithm
- Deutsch-Jozsa

Bell states

- Quantum Teleportation and Superdense coding make use of Bell states, and the Bell measurement
- We only looked at one Bell state last week, but there are four of them:

$$|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad |\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$$
$$|\Psi_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad |\Psi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

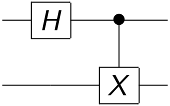
- Just like $|00\rangle$, $|01\rangle$, $|10\rangle$ and $|11\rangle$ they form an orthonormal basis in the four dimensional complex Hilbert space
- That means we could describe any 2-qubit state in terms of the four Bell states...
- and use the Bell states as are measurement basis, instead of the Computational base states
- However, we don't need to make things complicated...

Bell measurements

- We're used to thinking of things in the computational basis
- Instead of measuring in a different basis, we are able to do a unitary operation that can be thought of as a change of basis...
- and the measurement we do is still in the computational basis
- The operation that takes the Bell basis into the computational basis, followed by a measurement of both qubits, is known as a Bell measurement

Bell measurements

- The following circuit takes the computational basis into the Bell basis



- The inverse of this circuit takes the Bell basis back into the computational basis...
- Measuring both qubits after this would perform a Bell measurement
- Entanglement means the Bell states have some interesting properties
- Being able to change into the Bell basis means we can easily take advantage of these properties

Part I

Superdense Coding

Superdense coding

- If you have a single qubit in an arbitrary state, how much information can you get from it?
- No matter what unitary operations you do to it, the only information you can gain is from a measurement...
- A measurement only gives you a single Bit of information
- So, the transfer of a single qubit only transfers a single bit of information
- However, superdense coding makes use of a Bell state to transfer two bits of information, whilst only a single qubit changes hands
- The sender has two classical bits of information, and one member of a pair of entangled qubits
- The reciever has the other qubit from the entangled pair
- The sender encodes the classical information, and can send it to the receiver jut by giving them the single qubit they started with.

Superdense coding protocol

- The sender and receiver have a single qubit each from the two qubit state $|\Psi_{00}\rangle$
- The sender does a different unitary operation depending on the Bits that they want to encode...
  - for 00 they don't do anything
  - for 01 they do a Pauli-X rotation
  - for 10 they do a Pauli-Z rotation
  - for 11 they do a Pauli-X rotation and a Pauli-Z rotation
- The sender can now *send* their qubit to the receiver
- All the receiver has to do is a Bell measurement, and they will have the two Bits that the sender wanted to send them

Superdense coding

- Lets look at how this works...
- The sender and receiver share the state $|\Psi_{00}\rangle$
- What happens when we do a Pauli-X or Pauli-Z rotation on the first qubit in this pair?

$$Pauli - X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Pauli - Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

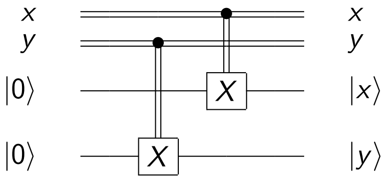
- Pauli-X has the effect of negating the base states $|0\rangle$ and $|1\rangle$
- Pauli-Z has the effect of adding a negative (relative) phase to the $|1\rangle$ base state

Superdense coding

- What happens when we apply the operations for each possible pair of bits we wish to send?
- For 00 we do nothing, so the two qubits are in the state $|\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- For 01 we have Pauli-X applied to the first qubit: $X_0 |\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\Psi_{01}\rangle$
- For 10 we have Pauli-Z applied to the first qubit: $Z_0 |\Psi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\Psi_{10}\rangle$
- For 11 we have a Pauli-X and a Pauli-Z applied to the first qubit: $Z_0(X_0 |\Psi_{00}\rangle) = Z_0 |\Psi_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\Psi_{11}\rangle$
- The qubit is then given to the receiver...
- With both qubits in their possesion, the receiver is able to perform a Bell measurement and extract the original encoded Bits

Deriving superdense coding

- It is possible to derive the circuit for superdense coding from a circuit that simply *copies* two Bits:



- The double wires represent classical bits
- Currently the sender would require access to both qubits
- Before starting the derivation, lets looks at some equivalences

Equivalent circuits

- For arbitrary U, and its inverse U^{-1}

$$-\boxed{U}-\boxed{U^{-1}}- \quad = \quad -\!-\!-\!-\!- \qquad (a)$$

- E.g. Hadamard and Controlled-X are self-inverse (a_H) and (a_C)
-

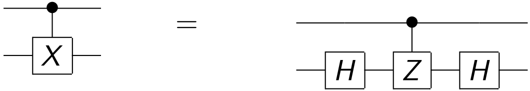
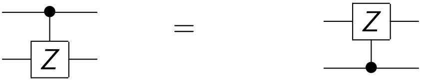
$$-\boxed{H}-\boxed{X}-\boxed{H}- \quad = \quad -\boxed{Z}- \qquad (b)$$

-

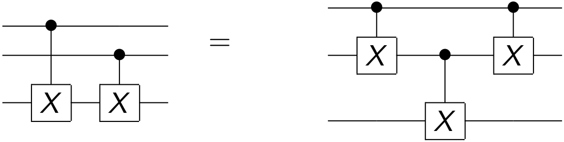
$$-\boxed{H}-\boxed{Z}-\boxed{H}- \quad = \quad -\boxed{X}- \qquad (c)$$

- (c) is derivable from (a_H) and (b)

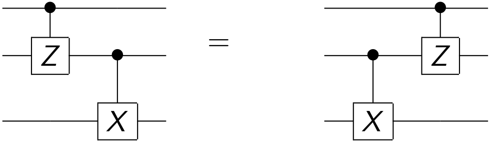
Equivalent circuits

-  (d)
- (d) is derivable from (a_H) and (c)
-  (e)

Equivalent circuits

- 

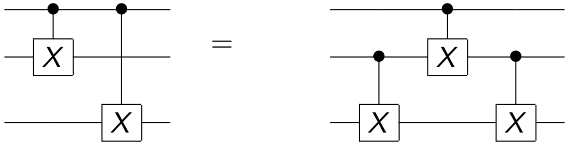
  (f)

- 

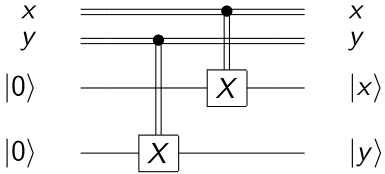
  (g)

- (d), (f), and (g) still hold if the top control wire is a classical wire

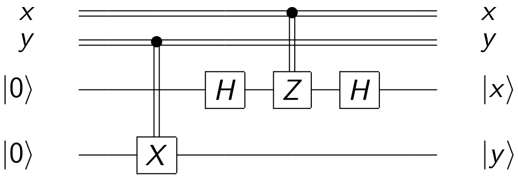
Equivalent circuits

-  (h)

Derivation of superdense coding

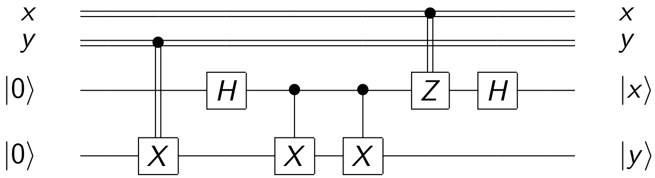
- 

- Using (d):

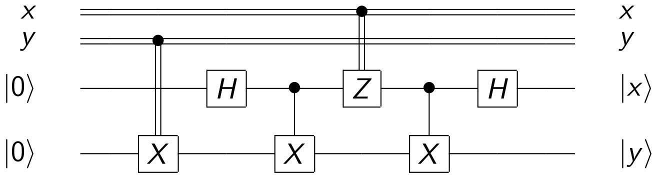


Derivation of superdense coding

- Using (a_C):

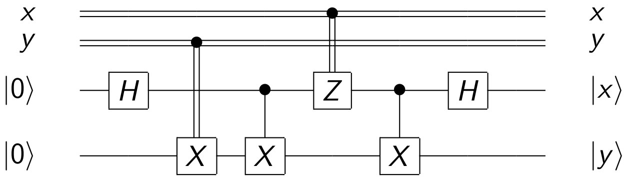


- Using (g):

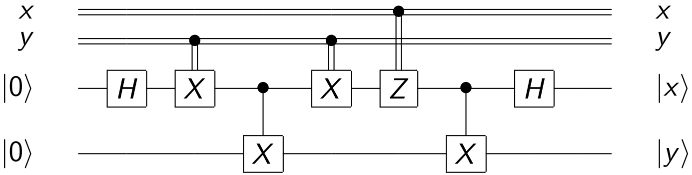


Derivation of superdense coding

- Sliding the Hadamard to the front:

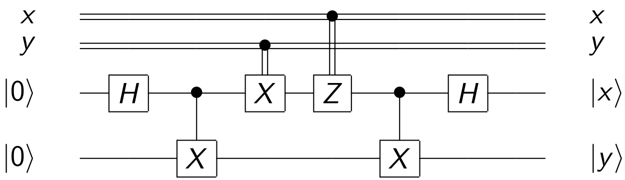


- Using (f):

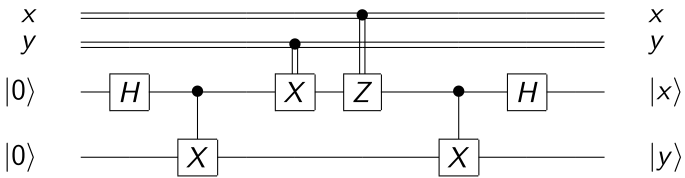


Derivation of superdense coding

- The first controlled-X will act as identity:



- Spreading it all out a little:



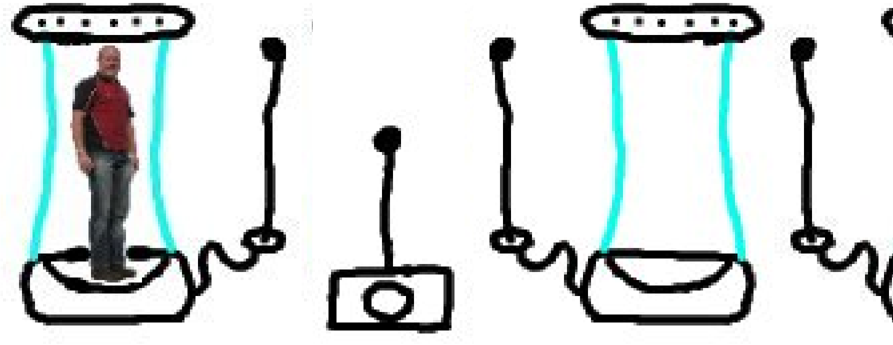
- This is the circuit that describes the superdense coding protocol that we looked at earlier

Part II

Quantum Teleportation

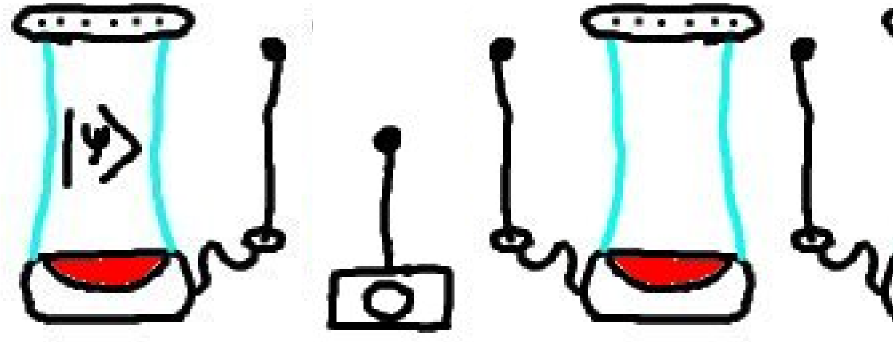
Teleportation

- What is teleportation?



Quantum Teleportation

- What is quantum teleportation?



Quantum Teleportation

- Quantum teleportation allows us to transfer the state of an aribtrary qubit to another qubit
- It makes use of an entangled pair of qubits in order to achieve this
- It doesn't break the no-cloning theorem as the state of the original qubit is lost in the process
- We shall look at teleportation in terms of a sender and a reciever
  - We shall call the sender Alice
  - We shall call the reciever Bob
- If Alice and Bob share an entangled pair of qubits, then it is possible for Alice to teleport Bob an arbitrary qubit using purely classical communication...
- In fact, only two Bits of classical information need to be sent

Quantum teleportation

- Lets look at the protocol in more detail
- Alice and Bob have one qubit each from an entangled pair of qubits in the state $|\Psi_{00}\rangle$
- Alice also has a qubit in an arbitrary state $\alpha|0\rangle + \beta|1\rangle$ that she wishes to send to Bob
- However, Alice is only able to send Bob classical information
- Alice can use quantum teleportation to achieve her goal
- Alice must perform a Bell measurement on the two qubits in her possesion...
- collapsing them into one of the base states $|00\rangle$, $|01\rangle$, $|10\rangle$, or $|11\rangle$
- If Alice sends Bob the classical results of this measurement $(00, 01, 10$, or $11)$ then he is able to reconstruct the original state $\alpha|0\rangle + \beta|1\rangle$ with unitary operations on the single qubit in his possesion

Quantum teleportation

- Lets look at the state of the qubits, with subscripts to denote who they belong to
- The qubit Alice wishes to send is in the arbitrary state $|\psi\rangle_a = \alpha |0\rangle_a + \beta |1\rangle_a$
- The Bell state shared by Alice and Bob is in the state $|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)$
- We can write the combined state as $|\psi\rangle_a |\Psi\rangle_{AB} = (\alpha |0\rangle_a + \beta |1\rangle_a)\frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)$
- Lets see what happens to this state if we apply a Bell measurement to the first two qubits
- We can think of the Bell measurement in terms of the circuit introduced earlier
- First, a controlled-X is applied to the two qubits, then a Hadamard rotation is applied to the first qubit, and finally both the qubits are measured

Quantum teleportation

- We have the overall state:
  $|\psi\rangle_a |\Psi\rangle_{AB} = (\alpha |0\rangle_a + \beta |1\rangle_a) \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)$
- The controlled-X will change the state to:
  $\alpha |0\rangle_a \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)$
  $+\beta |1\rangle_a \frac{1}{\sqrt{2}}(|1\rangle_A |0\rangle_B + |0\rangle_A |1\rangle_B)$
- The Hadamard will change this to:
  $\alpha \frac{1}{\sqrt{2}}(|0\rangle_a + |1\rangle_a) \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)$
  $+\beta \frac{1}{\sqrt{2}}(|0\rangle_a - |1\rangle_a) \frac{1}{\sqrt{2}}(|1\rangle_A |0\rangle_B + |0\rangle_A |1\rangle_B)$
- $= \alpha \frac{1}{2}((|0\rangle_a + |1\rangle_a) |0\rangle_A |0\rangle_B + (|0\rangle_a + |1\rangle_a) |1\rangle_A |1\rangle_B)$
  $+\beta \frac{1}{2}((|0\rangle_a - |1\rangle_a) |1\rangle_A |0\rangle_B + (|0\rangle_a - |1\rangle_a) |0\rangle_A |1\rangle_B)$
- $= \alpha \frac{1}{2}(|0\rangle_a |0\rangle_A |0\rangle_B + |1\rangle_a |0\rangle_A |0\rangle_B + |0\rangle_a |1\rangle_A |1\rangle_B + |1\rangle_a |1\rangle_A |1\rangle_B) + \beta \frac{1}{2}(|0\rangle_a |1\rangle_A |0\rangle_B - |1\rangle_a |1\rangle_A |0\rangle_B + |0\rangle_a |0\rangle_A |1\rangle_B - |1\rangle_a |0\rangle_A |1\rangle_B)$

Quantum teleportation

- $= \alpha\frac{1}{2}|0\rangle_a|0\rangle_A|0\rangle_B + \beta\frac{1}{2}|0\rangle_a|0\rangle_A|1\rangle_B$
  $+\beta\frac{1}{2}|0\rangle_a|1\rangle_A|0\rangle_B + \alpha\frac{1}{2}|0\rangle_a|1\rangle_A|1\rangle_B$
  $+\alpha\frac{1}{2}|1\rangle_a|0\rangle_A|0\rangle_B - \beta\frac{1}{2}|1\rangle_a|0\rangle_A|1\rangle_B$
  $-\beta\frac{1}{2}|1\rangle_a|1\rangle_A|0\rangle_B + \alpha\frac{1}{2}|1\rangle_a|1\rangle_A|1\rangle_B$
- $= \frac{1}{2}|0\rangle_a|0\rangle_A(\alpha|0\rangle_B + \beta|1\rangle_B)$
  $+\frac{1}{2}|0\rangle_a|1\rangle_A(\alpha|1\rangle_B + \beta|0\rangle_B)$
  $+\frac{1}{2}|1\rangle_a|0\rangle_A(\alpha|0\rangle_B - \beta|1\rangle_B)$
  $+\frac{1}{2}|1\rangle_a|1\rangle_A(\alpha|1\rangle_B - \beta|0\rangle_B)$
- What happens if Alice now measures her qubits?

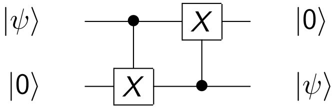
Quantum teleportation

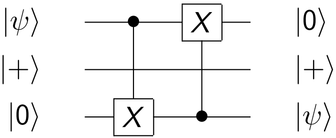
- We are left with one of the following four states, each with probability $\frac{1}{4}$:
  - 00 leaves the state $\alpha\left|0\right\rangle_B + \beta\left|1\right\rangle_B$
  - 01 leaves the state $\alpha\left|1\right\rangle_B + \beta\left|0\right\rangle_B$
  - 10 leaves the state $\alpha\left|0\right\rangle_B - \beta\left|1\right\rangle_B$
  - 11 leaves the state $\alpha\left|1\right\rangle_B - \beta\left|0\right\rangle_B$
- The original qubit state $\left|\psi\right\rangle$ can be recovered from any of these states:
  - if Bob receives 00 then he already has the teleported state
  - if Bob receives 01 then he needs to apply a Pauli-X to recover the teleported state
  - if Bob receives 10 then he needs to apply a Pauli-Z to recover the teleported state
  - if Bob receives 11 then he needs to apply a Pauli-X and a Pauli-Z to recover the teleported state

Quantum teleportation

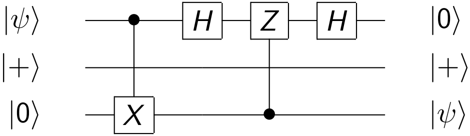
- What about the no-cloning theorem?
- Have we cloned the original state $|\psi\rangle$?
- No! Alice's qubits are in one of the computational base states
- Teleportation is able to transfer an arbitrary state, not copy it
- In doing the teleportation, we have also lost the entanglement that Alice and Bob shared
- It is possible to think of this in terms of a resource, that we have used up
- Like superdense coding, we are able to derive the quantum teleportation circuit from a classical circuit.

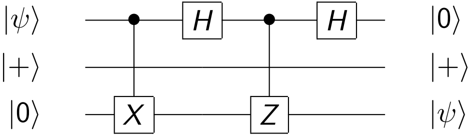
Deriving teleportation

- The following circuit transfers the state of the first qubit to the second qubit:
- 

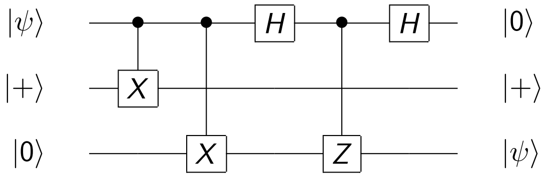
- We know we need an extra qubit for the Bell state, so lets introduce that
- 

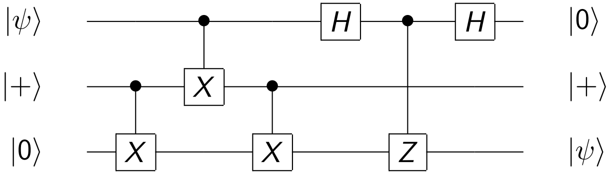
Deriving teleportation

- Using (d)
- 

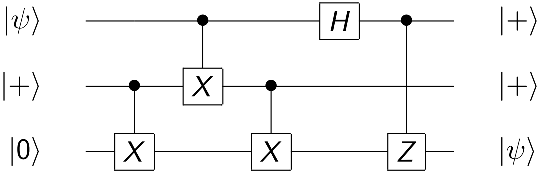
- Using (e)
- 

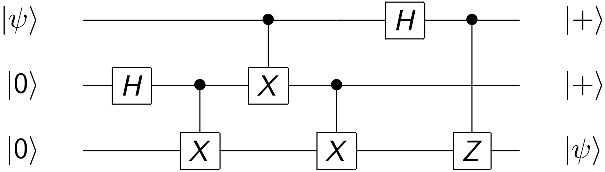
Deriving teleportation

- Pauli-X is the identity on $|+\rangle$
- 

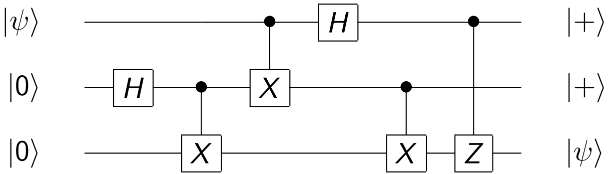
- Using (h)
- 

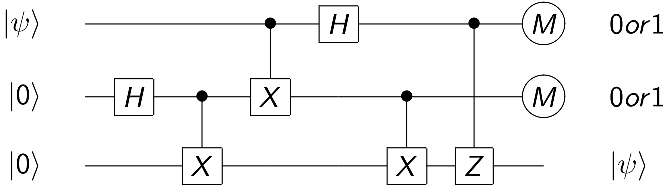
Deriving teleportation

- removing the last Hadamard changes the output state
- 

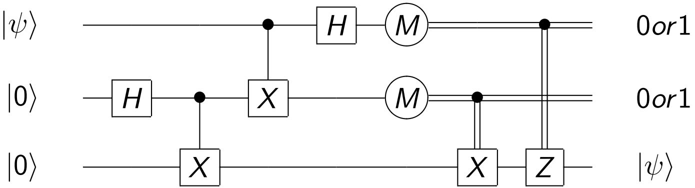
- adding a hadamard at the begining changes the input state
- 

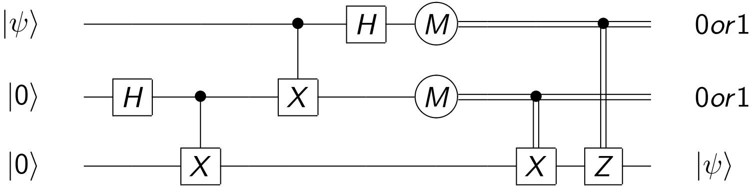
Deriving teleportation

- Sliding the controlled-X and Hadamard around
- 

- Introducing measurement
- 

Deriving teleportation

- Measurement commutes over controls
- 

- Spacing it out a little
- 

- This is the circuit for quantum teleportation

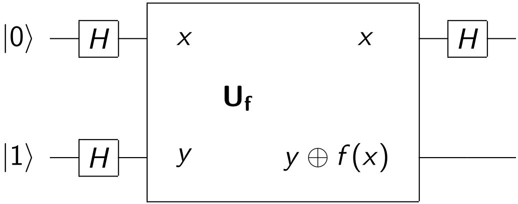
Part III

Deutsch's Algorithm

Deutsch's Algorithm

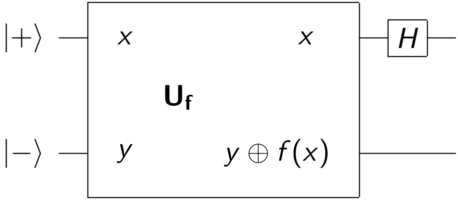
- Deutsch's algorithm is possibly the simplest algorithm that solves a problem *faster* than on a classical computer
- It involves being given a Boolean function (E.g. $f :: Bool \rightarrow Bool$) and being asked whether the function is balanced, or constant
- If the function is balanced, then it returns *False* and *True* for half the inputs each
- If the function is constant, then it always returns the same result, no matter what the input is
- If I was to give you a function f, and ask you if it was constant or balanced, how many times would you have to evaluate that function?
- Using Deutsch's algorithm, we are able to define a quantum computation that only evaluates the function once, and will return the correct answer with absolute certainty
- (albeit over a quantum state)

Deutsch's algorithm

- The following circuit implements Deutsch's algorithm
- 

- We can see what happens if we run this circuit for different functions f
- The first two Hadamard gates take the inputs to $|+\rangle$ and $|-\rangle$

Deutsch's algorithm

- 

- What are the outputs for each function $f :: Bool \rightarrow Bool$
  - $(f = \lambda x \rightarrow False)$ leaves the state as $|+-\rangle$
  - $(f = \lambda x \rightarrow True)$ negates both qubits leaving $-|+-\rangle$
  - $(f = \lambda x \rightarrow x)$ negates the second qubit when the top qubit is $|1\rangle$, leaving $|--\rangle$
  - $(f = \lambda x \rightarrow \neg\, x)$ negates the second qubit when the top qubit is $|0\rangle$, leaving $-|--\rangle$
- What do we notice about the output state when f is constant, or when f is balanced?

Deutsch's algorithm

- When f is constant, we're left with the states $\pm|+-\rangle$
- When f is balanced, we're left with the states $\pm|--\rangle$
- What effect does the final Hadamard have on these states?
- $\pm|+-\rangle$ is taken to $\pm|0-\rangle$
- $\pm|--\rangle$ is taken to $\pm|1-\rangle$
- The $\pm$ is a global phase, so doesn't effect measurement
- So, measuring the first qubit gives us exactly 0 if f is constant, and exactly 1 if f is balanced
- We'll start to see next week that many quantum algorithms have a similar strucutre to this

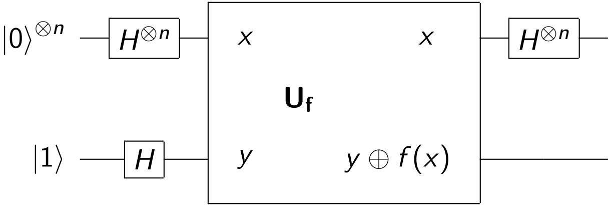
Part IV

Deutsch-Jozsa

Deutsch-Jozsa

- The Deutsch-Jozsa algorithm is a generalisation of Deutsch's algorithm, to Boolean functions with an arbitrary number of input arguments, but only a single Boolean output
- As long as the function is guaranteed to be either balanced, or constant, then the Deutsch-Jozsa algorithm can tell you with certainty which type it is...
- and only has to evaluate the function once
- (albeit over a quantum state)
- Classically, in the worst case, you would have to evaluate the function once more than for half the possible inputs

Deutsch-Jozsa

- The following circuit implements Deutsch-Jozsa:
- 

- It is very similar to Deutsch's algorithm...
- requiring one more qubit than the number of inputs to the Boolean function

Remember...

- Remember, labs are on Thursday, 15:00 to 17:00
- The labs this week will look again at the algorithms introduced in this lecture.
- Next week, we shall be looking at a more complicated quantum algorithm...
- known as Grover's algorithm
- or Grover's quantum unsorted database searching algorithm
- Thank you