ITIS 6260/8260 Quantum Computing

Lecture 2: Quantum entanglement and quantum gates

Yongge Wang

UNC Charlotte, USA

January 4, 2019

Outline

Outline

Outline

Bloch Sphere

- For a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, we have $|\alpha|^2 + |\beta|^2 = 1$. Thus we can also write it as

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

  where θ, ϕ, and γ are real numbers.
- Since $e^{i\gamma}$ has no observable effects, we can just write

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

Bloch Sphere

- For a qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, we have $|\alpha|^2 + |\beta|^2 = 1$. Thus we can also write it as

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

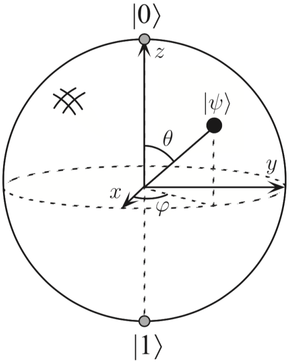
  where θ, ϕ, and γ are real numbers.
- Since $e^{i\gamma}$ has no observable effects, we can just write

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

Bloch Sphere

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

where θ and ϕ define a point on the three-dimensional sphere (Bloch sphere):



Two Qubits

- For a pair of photons, we have four basis states:

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

- a general state of two photons is:

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

where $\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}$ are complex numbers with $\sum_{i,j} |\alpha_{ij}|^2 = 1$.

Two Qubits

- For a pair of photons, we have four basis states:

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

- a general state of two photons is:

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

where $\alpha_{00}, \alpha_{01}, \alpha_{10}, \alpha_{11}$ are complex numbers with $\sum_{i,j} |\alpha_{ij}|^2 = 1$.

Measuring multiple-qubits systems

- For a two photon system, we may choose to measure the first photon and leave the second photon unmeasured

$$s = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

Measuring multiple-qubits systems

- Rewrite s as

$$s = |0\rangle \otimes (a|0\rangle + b|1\rangle) + |1\rangle \otimes (c|0\rangle + d|1\rangle)$$

or

$$s = |0\rangle \otimes |v\rangle + |1\rangle \otimes |w\rangle$$

where $\otimes$ is the tensor product of quantum states (a state that is expressed independently–no entanglement)

Measuring multiple-qubits systems

- Then if we use the measurement M to measure the first photon, what is the outcome possibility? and what is the impact on the second photon?
- According to the general rule of quantum mechanics, the outcome of the measuring is $|0\rangle$ and $|1\rangle$ with probabilities $\langle v|v\rangle$ and $\langle w|w\rangle$ respectively.
- If the outcome is $|0\rangle$, then the final state of the first photon is $|0\rangle$ and the final state of the second photon is $|v\rangle/\sqrt{\langle v|v\rangle}$
- This is interesting. If the first photon is light year apart from the second photon, the second photon still changes its state!

Measuring multiple-qubits systems

- Then if we use the measurement M to measure the first photon, what is the outcome possibility? and what is the impact on the second photon?
- According to the general rule of quantum mechanics, the outcome of the measuring is $|0\rangle$ and $|1\rangle$ with probabilities $\langle v|v\rangle$ and $\langle w|w\rangle$ respectively.
- If the outcome is $|0\rangle$, then the final state of the first photon is $|0\rangle$ and the final state of the second photon is $|v\rangle/\sqrt{\langle v|v\rangle}$
- This is interesting. If the first photon is light year apart from the second photon, the second photon still changes its state!

Measuring multiple-qubits systems

- Then if we use the measurement M to measure the first photon, what is the outcome possibility? and what is the impact on the second photon?
- According to the general rule of quantum mechanics, the outcome of the measuring is $|0\rangle$ and $|1\rangle$ with probabilities $\langle v|v\rangle$ and $\langle w|w\rangle$ respectively.
- If the outcome is $|0\rangle$, then the final state of the first photon is $|0\rangle$ and the final state of the second photon is $|v\rangle/\sqrt{\langle v|v\rangle}$
- This is interesting. If the first photon is light year apart from the second photon, the second photon still changes its state!

Measuring multiple-qubits systems

- Then if we use the measurement M to measure the first photon, what is the outcome possibility? and what is the impact on the second photon?
- According to the general rule of quantum mechanics, the outcome of the measuring is $|0\rangle$ and $|1\rangle$ with probabilities $\langle v|v\rangle$ and $\langle w|w\rangle$ respectively.
- If the outcome is $|0\rangle$, then the final state of the first photon is $|0\rangle$ and the final state of the second photon is $|v\rangle/\sqrt{\langle v|v\rangle}$
- This is interesting. If the first photon is light year apart from the second photon, the second photon still changes its state!

Measuring multiple-qubits systems

- the physical interpretation of this is beyond the scope of this class
- the final state of the second photon depends on our choice of measurement to perform on the first photon
- Cryptographic implication: Alice tries to measure photon one, Bob is close to photon two. Could this measurement by Alice send some signal to Bob by Alice's choice of what to measure?
- the good news is that Alice can choose what to measure, but cannot control the outcome. Thus a simple argument could be used to show that Bob's measurement result is independent of Alice's choice. In words, Alice cannot use her choice of measurement to send a signal to Bob.

Measuring multiple-qubits systems

- the physical interpretation of this is beyond the scope of this class
- the final state of the second photon depends on our choice of measurement to perform on the first photon
- Cryptographic implication: Alice tries to measure photon one, Bob is close to photon two. Could this measurement by Alice send some signal to Bob by Alice's choice of what to measure?
- the good news is that Alice can choose what to measure, but cannot control the outcome. Thus a simple argument could be used to show that Bob's measurement result is independent of Alice's choice. In words, Alice cannot use her choice of measurement to send a signal to Bob.

Measuring multiple-qubits systems

- the physical interpretation of this is beyond the scope of this class
- the final state of the second photon depends on our choice of measurement to perform on the first photon
- Cryptographic implication: Alice tries to measure photon one, Bob is close to photon two. Could this measurement by Alice send some signal to Bob by Alice's choice of what to measure?
- the good news is that Alice can choose what to measure, but cannot control the outcome. Thus a simple argument could be used to show that Bob's measurement result is independent of Alice's choice. In words, Alice cannot use her choice of measurement to send a signal to Bob.

Measuring multiple-qubits systems

- the physical interpretation of this is beyond the scope of this class
- the final state of the second photon depends on our choice of measurement to perform on the first photon
- Cryptographic implication: Alice tries to measure photon one, Bob is close to photon two. Could this measurement by Alice send some signal to Bob by Alice's choice of what to measure?
- the good news is that Alice can choose what to measure, but cannot control the outcome. Thus a simple argument could be used to show that Bob's measurement result is independent of Alice's choice. In words, Alice cannot use her choice of measurement to send a signal to Bob.

Entanglement

- Entanglement is the ability of quantum systems to exhibit correlations between states within a superposition.
- Imagine two qubits, each in the state $|0\rangle + |1\rangle$. We can entangle the two qubits such that the measurement of one qubit is always correlated to the measurement of the other qubit.

Entanglement

- Entanglement is the ability of quantum systems to exhibit correlations between states within a superposition.
- Imagine two qubits, each in the state $|0\rangle + |1\rangle$. We can entangle the two qubits such that the measurement of one qubit is always correlated to the measurement of the other qubit.

Two Qubits

- If we measure two qubits $|\alpha\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$ at the same time, the probability to get the output $|ij\rangle$ is $|\alpha_{ij}|^2$.
- If we only measure the first qubit, the probability to get output $|0\rangle$ is $|\alpha_{00}|^2 + |\alpha_{01}|^2$, and the post-measurement state will be:

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

Two Qubits

- If we measure two qubits $|\alpha\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$ at the same time, the probability to get the output $|ij\rangle$ is $|\alpha_{ij}|^2$.
- If we only measure the first qubit, the probability to get output $|0\rangle$ is $|\alpha_{00}|^2 + |\alpha_{01}|^2$, and the post-measurement state will be:

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

Bell state or EPR pair

- An important two qubit state is the Bell state or EPR pair $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$
- Measure any qubit, it has 50% probability to get 0 or 1
- However, measure any qubit will fix the state of the other qubit.

Bell state or EPR pair

- An important two qubit state is the Bell state or EPR pair $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$
- Measure any qubit, it has 50% probability to get 0 or 1
- However, measure any qubit will fix the state of the other qubit.

Bell state or EPR pair

- An important two qubit state is the Bell state or EPR pair $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$
- Measure any qubit, it has 50% probability to get 0 or 1
- However, measure any qubit will fix the state of the other qubit.

Multiple Qubits

- Consider a 3 bit qubit register. An equally weighted superposition of all possible states would be denoted by

$$|\phi\rangle = \frac{1}{\sqrt{8}}|000\rangle + \frac{1}{\sqrt{8}}|001\rangle + \cdots + \frac{1}{\sqrt{8}}|111\rangle$$

- An n qubit register can represent the numbers 0 through $2^n - 1$ simultaneously.
- For entangled n qubits, we need 2^n complex numbers to represent them
- if the state of n photons can be expressed separately, then we say that this is a product state
- any state that is not a product state is called an entangled state
- entanglement is the essential difference of quantum mechanics from classical physics

Multiple Qubits

- Consider a 3 bit qubit register. An equally weighted superposition of all possible states would be denoted by

$$|\phi\rangle = \frac{1}{\sqrt{8}}|000\rangle + \frac{1}{\sqrt{8}}|001\rangle + \cdots + \frac{1}{\sqrt{8}}|111\rangle$$

- An n qubit register can represent the numbers 0 through $2^n - 1$ simultaneously.
- For entangled n qubits, we need 2^n complex numbers to represent them
- if the state of n photons can be expressed separately, then we say that this is a product state
- any state that is not a product state is called an entangled state
- entanglement is the essential difference of quantum mechanics from classical physics

Multiple Qubits

- Consider a 3 bit qubit register. An equally weighted superposition of all possible states would be denoted by

$$|\phi\rangle = \frac{1}{\sqrt{8}}|000\rangle + \frac{1}{\sqrt{8}}|001\rangle + \cdots + \frac{1}{\sqrt{8}}|111\rangle$$

- An n qubit register can represent the numbers 0 through $2^n - 1$ simultaneously.
- For entangled n qubits, we need 2^n complex numbers to represent them
- if the state of n photons can be expressed separately, then we say that this is a product state
- any state that is not a product state is called an entangled state
- entanglement is the essential difference of quantum mechanics from classical physics

Multiple Qubits

- Consider a 3 bit qubit register. An equally weighted superposition of all possible states would be denoted by

$$|\phi\rangle = \frac{1}{\sqrt{8}}|000\rangle + \frac{1}{\sqrt{8}}|001\rangle + \cdots + \frac{1}{\sqrt{8}}|111\rangle$$

- An n qubit register can represent the numbers 0 through $2^n - 1$ simultaneously.
- For entangled n qubits, we need 2^n complex numbers to represent them
- if the state of n photons can be expressed separately, then we say that this is a product state
- any state that is not a product state is called an entangled state
- entanglement is the essential difference of quantum mechanics from classical physics

Multiple Qubits

- Consider a 3 bit qubit register. An equally weighted superposition of all possible states would be denoted by

$$|\phi\rangle = \frac{1}{\sqrt{8}}|000\rangle + \frac{1}{\sqrt{8}}|001\rangle + \cdots + \frac{1}{\sqrt{8}}|111\rangle$$

- An n qubit register can represent the numbers 0 through $2^n - 1$ simultaneously.
- For entangled n qubits, we need 2^n complex numbers to represent them
- if the state of n photons can be expressed separately, then we say that this is a product state
- any state that is not a product state is called an entangled state
- entanglement is the essential difference of quantum mechanics from classical physics

Multiple Qubits

- Consider a 3 bit qubit register. An equally weighted superposition of all possible states would be denoted by

$$|\phi\rangle = \frac{1}{\sqrt{8}}|000\rangle + \frac{1}{\sqrt{8}}|001\rangle + \cdots + \frac{1}{\sqrt{8}}|111\rangle$$

- An n qubit register can represent the numbers 0 through $2^n - 1$ simultaneously.
- For entangled n qubits, we need 2^n complex numbers to represent them
- if the state of n photons can be expressed separately, then we say that this is a product state
- any state that is not a product state is called an entangled state
- entanglement is the essential difference of quantum mechanics from classical physics

Quantum computers

- A quantum computer contains n qubits.
- if qubits can only be in non-entangled state, then nothing more powerful could be achieved
- The important thing is that these qubits could be entangled. There could be potentially 2^n states, and we could run a function on all these inputs at the same time
- challenges in building quantum computers: how can we restrict many qubits in a controlled environments so that they will not have too much entanglement with outside world and they could sufficiently entangle with each other in a controlled way?

Quantum computers

- A quantum computer contains n qubits.
- if qubits can only be in non-entangled state, then nothing more powerful could be achieved
- The important thing is that these qubits could be entangled. There could be potentially 2^n states, and we could run a function on all these inputs at the same time
- challenges in building quantum computers: how can we restrict many qubits in a controlled environments so that they will not have too much entanglement with outside world and they could sufficiently entangle with each other in a controlled way?

Quantum computers

- A quantum computer contains n qubits.
- if qubits can only be in non-entangled state, then nothing more powerful could be achieved
- The important thing is that these qubits could be entangled. There could be potentially 2^n states, and we could run a function on all these inputs at the same time
- challenges in building quantum computers: how can we restrict many qubits in a controlled environments so that they will not have too much entanglement with outside world and they could sufficiently entangle with each other in a controlled way?

Quantum computers

- A quantum computer contains n qubits.
- if qubits can only be in non-entangled state, then nothing more powerful could be achieved
- The important thing is that these qubits could be entangled. There could be potentially 2^n states, and we could run a function on all these inputs at the same time
- challenges in building quantum computers: how can we restrict many qubits in a controlled environments so that they will not have too much entanglement with outside world and they could sufficiently entangle with each other in a controlled way?

Quantum computers

- Traditional computers are based on the AND, OR, NAND circuit gates to manipulate signals
- In quantum computers, we need to define the operations on quantum bits
- The definition of Quantum circuits (Quantum Turing machine) only allows local unitary transformations (unitary transformations on a fixed number of bits).
- a general transformation on n-qubits could be implemented by exponentially many 2-qubits transformations (called quantum gates)
- The goal for quantum algorithm: find polynomial steps of -2-qubits transformations for the target tasks

Quantum computers

- Traditional computers are based on the AND, OR, NAND circuit gates to manipulate signals
- In quantum computers, we need to define the operations on quantum bits
- The definition of Quantum circuits (Quantum Turing machine) only allows local unitary transformations (unitary transformations on a fixed number of bits).
- a general transformation on *n*-qubits could be implemented by exponentially many 2-qubits transformations (called quantum gates)
- The goal for quantum algorithm: find polynomial steps of -2-qubits transformations for the target tasks

Quantum computers

- Traditional computers are based on the AND, OR, NAND circuit gates to manipulate signals
- In quantum computers, we need to define the operations on quantum bits
- The definition of Quantum circuits (Quantum Turing machine) only allows local unitary transformations (unitary transformations on a fixed number of bits).
- a general transformation on n-qubits could be implemented by exponentially many 2-qubits transformations (called quantum gates)
- The goal for quantum algorithm: find polynomial steps of -2-qubits transformations for the target tasks

Quantum computers

- Traditional computers are based on the AND, OR, NAND circuit gates to manipulate signals
- In quantum computers, we need to define the operations on quantum bits
- The definition of Quantum circuits (Quantum Turing machine) only allows local unitary transformations (unitary transformations on a fixed number of bits).
- a general transformation on n-qubits could be implemented by exponentially many 2-qubits transformations (called quantum gates)
- The goal for quantum algorithm: find polynomial steps of -2-qubits transformations for the target tasks

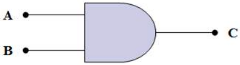
Quantum computers

- Traditional computers are based on the AND, OR, NAND circuit gates to manipulate signals
- In quantum computers, we need to define the operations on quantum bits
- The definition of Quantum circuits (Quantum Turing machine) only allows local unitary transformations (unitary transformations on a fixed number of bits).
- a general transformation on n-qubits could be implemented by exponentially many 2-qubits transformations (called quantum gates)
- The goal for quantum algorithm: find polynomial steps of -2-qubits transformations for the target tasks

Operations on Bits and Qubits - Reversible Logic

Ex.

The AND Gate



Input		Output
A	B	C
0	0	0
0	1	0
1	0	0
1	1	1

In these 3 cases, information is being destroyed

- Due to the nature of quantum physics, the destruction of information in a gate will cause heat to be evolved which can destroy the superposition of qubits. Thus traditional AND gate could not be constructed in quantum computers

Quantum Gates

- Quantum Gates are similar to classical gates, but do not have a degenerate output. i.e. their original input state can be derived from their output state, uniquely. They must be reversible.
- This means that a deterministic computation can be performed on a quantum computer only if it is reversible. Luckily, it has been shown that any deterministic computation can be made reversible (Charles Bennet, 1973).

Quantum Gates

- Quantum Gates are similar to classical gates, but do not have a degenerate output. i.e. their original input state can be derived from their output state, uniquely. They must be reversible.
- This means that a deterministic computation can be performed on a quantum computer only if it is reversible. Luckily, it has been shown that any deterministic computation can be made reversible (Charles Bennet, 1973).

Single qubit gate: Pauli X gate (NOT gate)

- NOT gate: changes $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$?
- The quantum NOT gate acts linearly: change $\alpha|0\rangle + \beta|1\rangle$ to $\alpha|1\rangle + \beta|0\rangle$
- It equates to a rotation of the Bloch sphere around the X-axis by π radians.
- This is defined by the unitary transformation $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Single qubit gate: Pauli X gate (NOT gate)

- NOT gate: changes $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$?
- The quantum NOT gate acts linearly: change $\alpha|0\rangle + \beta|1\rangle$ to $\alpha|1\rangle + \beta|0\rangle$
- It equates to a rotation of the Bloch sphere around the X-axis by π radians.
- This is defined by the unitary transformation $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Single qubit gate: Pauli X gate (NOT gate)

- NOT gate: changes $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$?
- The quantum NOT gate acts linearly: change $\alpha|0\rangle + \beta|1\rangle$ to $\alpha|1\rangle + \beta|0\rangle$
- It equates to a rotation of the Bloch sphere around the X-axis by π radians.
- This is defined by the unitary transformation $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Single qubit gate: Pauli X gate (NOT gate)

- NOT gate: changes $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$?
- The quantum NOT gate acts linearly: change $\alpha|0\rangle + \beta|1\rangle$ to $\alpha|1\rangle + \beta|0\rangle$
- It equates to a rotation of the Bloch sphere around the X-axis by π radians.
- This is defined by the unitary transformation $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

Single qubit gate: Pauli Y gate

- The Pauli Y gate applies a rotation around the Y-axis of the Bloch sphere by π radians.
- It maps $|0\rangle$ to $i|1\rangle$ and $|1\rangle$ to $-i|0\rangle$. It is represented by the Pauli Y matrix:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Single qubit gate: Pauli Y gate

- The Pauli Y gate applies a rotation around the Y-axis of the Bloch sphere by π radians.
- It maps $|0\rangle$ to $i|1\rangle$ and $|1\rangle$ to $-i|0\rangle$. It is represented by the Pauli Y matrix:

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

Single qubit gate: Pauli Z gate

- Z gate is defined by the unitary transformation
  $$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$
- Z gate leaves $|0\rangle$ unchanged, and flips the sign of $|1\rangle$ to give $-|1\rangle$
- It equates to a rotation around the Z-axis of the Bloch sphere by π radians.

Single qubit gate: Pauli Z gate

- Z gate is defined by the unitary transformation
  $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- Z gate leaves $|0\rangle$ unchanged, and flips the sign of $|1\rangle$ to give $-|1\rangle$
- It equates to a rotation around the Z-axis of the Bloch sphere by π radians.

Single qubit gate: Pauli Z gate

- Z gate is defined by the unitary transformation
  $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- Z gate leaves $|0\rangle$ unchanged, and flips the sign of $|1\rangle$ to give $-|1\rangle$
- It equates to a rotation around the Z-axis of the Bloch sphere by π radians.

Single qubit gate: Hadamard gate

- Hadamard gate is a unitary transformation with the effect on basis:

$$H|0\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$$
$$H|1\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$$

In other words,

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- H-gate is also called 'square-root of NOT' since both $H|0\rangle$ and $H|1\rangle$ are 'halfway' between $|0\rangle$ and $|1\rangle$.
- It should also note that $H^2 = I$.

Single qubit gate: Hadamard gate

- Hadamard gate is a unitary transformation with the effect on basis:

$$H|0\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$$
$$H|1\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$$

In other words,

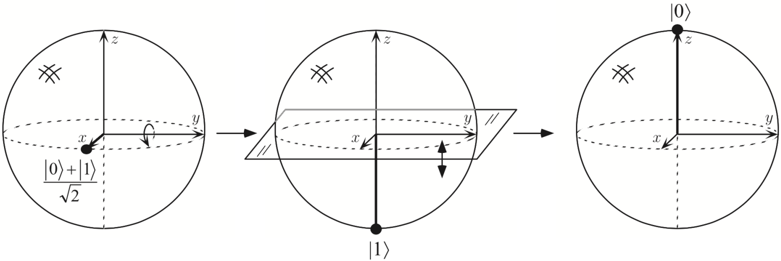
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

- H-gate is also called 'square-root of NOT' since both $H|0\rangle$ and $H|1\rangle$ are 'halfway' between $|0\rangle$ and $|1\rangle$.
- It should also note that $H^2 = I$.

Single qubit gate: Hadamard gate

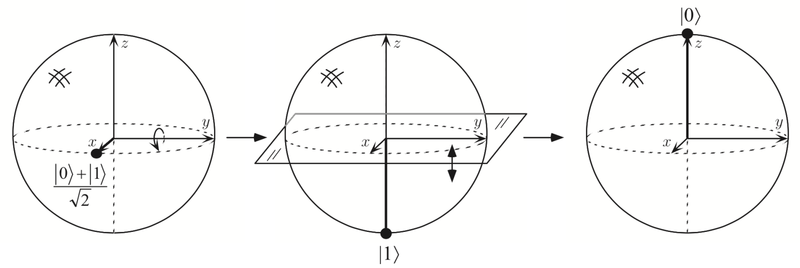
- Hadamard gate is a unitary transformation with the effect on basis:
$$H|0\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$$
$$H|1\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$$
In other words,
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$
- H-gate is also called 'square-root of NOT' since both $H|0\rangle$ and $H|1\rangle$ are 'halfway' between $|0\rangle$ and $|1\rangle$.
- It should also note that $H^2 = I$.

Hadamard gate in Bloch sphere



- Single qubit gates correspond to rotations and reflections of the Bloch sphere.
- The H-operation is a rotation of the sphere about the *y*-axis by 90, followed by a rotation about the *x*-axis by 180

Hadamard gate in Bloch sphere



- Single qubit gates correspond to rotations and reflections of the Bloch sphere.
- The H-operation is a rotation of the sphere about the *y*-axis by 90, followed by a rotation about the *x*-axis by 180

Phase shift

- This phase shift gates leave the basis state $|0\rangle$ unchanged and map $|1\rangle$ to $e^{i\phi}|1\rangle$
- The probability of measuring a $|0\rangle$ or $|1\rangle$ is unchanged after applying this gate, however it modifies the phase of the quantum state.
- This is equivalent to tracing a horizontal circle (a line of latitude) on the Bloch sphere by ϕ radians.
- The matrix representation is $R_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$ where ϕ is the phase shift.
- The common shift gate exampe is the T gate applies a phase of $\pi/4$ and has a matrix representation of $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

Phase shift

- This phase shift gates leave the basis state $|0\rangle$ unchanged and map $|1\rangle$ to $e^{i\phi}|1\rangle$
- The probability of measuring a $|0\rangle$ or $|1\rangle$ is unchanged after applying this gate, however it modifies the phase of the quantum state.
- This is equivalent to tracing a horizontal circle (a line of latitude) on the Bloch sphere by ϕ radians.
- The matrix representation is $R_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$ where ϕ is the phase shift.
- The common shift gate exampe is the T gate applies a phase of $\pi/4$ and has a matrix representation of $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

Phase shift

- This phase shift gates leave the basis state $|0\rangle$ unchanged and map $|1\rangle$ to $e^{i\phi}|1\rangle$
- The probability of measuring a $|0\rangle$ or $|1\rangle$ is unchanged after applying this gate, however it modifies the phase of the quantum state.
- This is equivalent to tracing a horizontal circle (a line of latitude) on the Bloch sphere by ϕ radians.
- The matrix representation is $R_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$ where ϕ is the phase shift.
- The common shift gate exampe is the T gate applies a phase of $\pi/4$ and has a matrix representation of $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

Phase shift

- This phase shift gates leave the basis state $|0\rangle$ unchanged and map $|1\rangle$ to $e^{i\phi}|1\rangle$
- The probability of measuring a $|0\rangle$ or $|1\rangle$ is unchanged after applying this gate, however it modifies the phase of the quantum state.
- This is equivalent to tracing a horizontal circle (a line of latitude) on the Bloch sphere by ϕ radians.
- The matrix representation is $R_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$ where ϕ is the phase shift.
- The common shift gate exampe is the T gate applies a phase of $\pi/4$ and has a matrix representation of $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

Phase shift

- This phase shift gates leave the basis state $|0\rangle$ unchanged and map $|1\rangle$ to $e^{i\phi}|1\rangle$
- The probability of measuring a $|0\rangle$ or $|1\rangle$ is unchanged after applying this gate, however it modifies the phase of the quantum state.
- This is equivalent to tracing a horizontal circle (a line of latitude) on the Bloch sphere by ϕ radians.
- The matrix representation is $R_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$ where ϕ is the phase shift.
- The common shift gate exampe is the T gate applies a phase of $\pi/4$ and has a matrix representation of $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

Bloch's theorem

Hadamard and phase-shift gates form a universal gate set of 1-qubit gates, every 1-qubit gate can be built from them.

Bloch's Theorem

According to Bloch's theorem for solid body rotations in three dimensions, any arbitrary 2×2 unitary matrix may be written as

$$U = e^{i\gamma} \begin{bmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{bmatrix} \begin{bmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} e^{i\beta} & 0 \\ 0 & e^{-i\beta} \end{bmatrix} \quad (6)$$

$$= e^{i\gamma} e^{i\alpha\sigma_z} e^{i\theta\sigma_x} e^{i\beta\sigma_z} , \quad (7)$$

where γ, α, θ, and β are real-valued, and σ_i are the Pauli matrices,

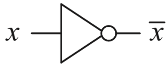
$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (8)$$

$$\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad (9)$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (10)$$

All single qubit operations may conveniently be expressed in terms of spinor rotations. For example, $U_R = \exp(\pi i \sigma_y / 4)$. This will later be useful in connecting such transforms with physical Hamiltonians.

Summary of single qubit gates



$$\alpha|0\rangle + \beta|1\rangle \;—\!\boxed{X}\!—\; \beta|0\rangle + \alpha|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \;—\!\boxed{Z}\!—\; \alpha|0\rangle - \beta|1\rangle$$

$$\alpha|0\rangle + \beta|1\rangle \;—\!\boxed{H}\!—\; \alpha\frac{|0\rangle+|1\rangle}{\sqrt{2}} + \beta\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

Quantum parallelism for $f:\{0,1\}^n \to \{0,1\}$

- Prepare a quantum computer with $n+1$ qubit state $|0\rangle^{\otimes n}|0\rangle$
- Apply Hadamard to the first n qubits independently

$$\begin{aligned} H\otimes \ldots H(|0\rangle \ldots |0\rangle)|0\rangle &= \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle)\ldots(|0\rangle + |1\rangle)|0\rangle \\ &= \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|0\rangle \end{aligned}$$

- Apply the circuit U_f for f to produce the state

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle$$

- Quantum parallelism enables all possible values of the function f to be evaluated simultaneously, even though we apparently only evaluated f once

Quantum parallelism for $f : \{0,1\}^n \to \{0,1\}$

- Prepare a quantum computer with $n+1$ qubit state $|0\rangle^{\otimes n}|0\rangle$
- Apply Hadamard to the first n qubits independently

$$\begin{aligned} H\otimes \ldots H(|0\rangle \ldots |0\rangle)|0\rangle &= \tfrac{1}{\sqrt{2^n}}(|0\rangle+|1\rangle)\ldots(|0\rangle+|1\rangle)|0\rangle \\ &= \tfrac{1}{\sqrt{2^n}}\textstyle\sum_{x\in\{0,1\}^n}|x\rangle|0\rangle \end{aligned}$$

- Apply the circuit U_f for f to produce the state

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle$$

- Quantum parallelism enables all possible values of the function f to be evaluated simultaneously, even though we apparently only evaluated f once

Quantum parallelism for $f : \{0,1\}^n \to \{0,1\}$

- Prepare a quantum computer with $n+1$ qubit state $|0\rangle^{\otimes n}|0\rangle$
- Apply Hadamard to the first n qubits independently

$$\begin{aligned} H\otimes \ldots H(|0\rangle \ldots |0\rangle)|0\rangle &= \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle)\ldots(|0\rangle + |1\rangle)|0\rangle \\ &= \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n} |x\rangle|0\rangle \end{aligned}$$

- Apply the circuit U_f for f to produce the state

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle$$

- Quantum parallelism enables all possible values of the function f to be evaluated simultaneously, even though we apparently only evaluated f once

Quantum parallelism for $f:\{0,1\}^n \to \{0,1\}$

- Prepare a quantum computer with $n+1$ qubit state $|0\rangle^{\otimes n}|0\rangle$
- Apply Hadamard to the first n qubits independently

$$\begin{aligned} H\otimes \ldots H(|0\rangle \ldots |0\rangle)|0\rangle &= \frac{1}{\sqrt{2^n}}(|0\rangle+|1\rangle)\ldots(|0\rangle+|1\rangle)|0\rangle \\ &= \frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|0\rangle \end{aligned}$$

- Apply the circuit U_f for f to produce the state

$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle|f(x)\rangle$$

- Quantum parallelism enables all possible values of the function f to be evaluated simultaneously, even though we apparently only evaluated f once

Quantum parallelism: A simple example

- 3-qubit quantum computer with initial state $|000\rangle = |0\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C$
- perform the transformation $H_A \otimes H_B \otimes I_C$, result is

$$\frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |110\rangle)$$

- if we perform U_{AND} on this state, we get

$$\frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |111\rangle)$$

- Essentially we performed the AND operation on all potential 2^2 inputs in one step
- **NOTE**: This example shows how to simulate classical AND gate with quantum gates: create a 3-qubit input so that the first two qubits simulate the classical input and the third qubit will hold the AND result

Quantum parallelism: A simple example

- 3-qubit quantum computer with initial state $|000\rangle = |0\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C$
- perform the transformation $H_A \otimes H_B \otimes I_C$, result is

$$\frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |110\rangle)$$

- if we perform U_{AND} on this state, we get

$$\frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |111\rangle)$$

- Essentially we performed the AND operation on all potential 2^2 inputs in one step
- **NOTE**: This example shows how to simulate classical AND gate with quantum gates: create a 3-qubit input so that the first two qubits simulate the classical input and the third qubit will hold the AND result

Quantum parallelism: A simple example

- 3-qubit quantum computer with initial state $|000\rangle = |0\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C$
- perform the transformation $H_A \otimes H_B \otimes I_C$, result is

$$\frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |110\rangle)$$

- if we perform U_{AND} on this state, we get

$$\frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |111\rangle)$$

- Essentially we performed the AND operation on all potential 2^2 inputs in one step
- **NOTE**: This example shows how to simulate classical AND gate with quantum gates: create a 3-qubit input so that the first two qubits simulate the classical input and the third qubit will hold the AND result

Quantum parallelism: A simple example

- 3-qubit quantum computer with initial state $|000\rangle = |0\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C$
- perform the transformation $H_A \otimes H_B \otimes I_C$, result is

$$\frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |110\rangle)$$

- if we perform U_{AND} on this state, we get

$$\frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |111\rangle)$$

- Essentially we performed the AND operation on all potential 2^2 inputs in one step
- **NOTE**: This example shows how to simulate classical AND gate with quantum gates: create a 3-qubit input so that the first two qubits simulate the classical input and the third qubit will hold the AND result

Quantum parallelism: A simple example

- 3-qubit quantum computer with initial state $|000\rangle = |0\rangle_A \otimes |0\rangle_B \otimes |0\rangle_C$
- perform the transformation $H_A \otimes H_B \otimes I_C$, result is
$$\frac{1}{2}(|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle)\otimes|0\rangle = \frac{1}{2}(|000\rangle+|010\rangle+|100\rangle+|110\rangle)$$
- if we perform U_{AND} on this state, we get
$$\frac{1}{2}(|000\rangle+|010\rangle+|100\rangle+|111\rangle)$$
- Essentially we performed the AND operation on all potential 2^2 inputs in one step
- **NOTE**: This example shows how to simulate classical AND gate with quantum gates: create a 3-qubit input so that the first two qubits simulate the classical input and the third qubit will hold the AND result

Quantum parallelism: The Deutsch-Jozsa algorithm

- f is a constant if $f(x) = 0$ (or $f(x) = 1$) for all x
- f is a balanced if $f(x) = 0$ for exactly half of the 2^n inputs x.
- Apply Hadamard gate to first n qubit state $|0\cdots 0\rangle$ and to the last qubit state $|1\rangle$ to get the $(n+1)$-qubit state

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} |x\rangle(|0\rangle - |1\rangle)$$

- Apply the circuit U_f for f to this state

$$\begin{aligned} U_f : |x\rangle(|0\rangle - |1\rangle) &\rightarrow |x\rangle(|f(x)\rangle - |f(x) \oplus 1\rangle) \\ &= \begin{cases} |x\rangle(|0\rangle - |1\rangle) & \text{if } f(x) = 0 \\ -|x\rangle(|0\rangle - |1\rangle) & \text{if } f(x) = 1 \end{cases} \\ &= (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle) \end{aligned}$$

Quantum parallelism: The Deutsch-Jozsa algorithm

- f is a constant if $f(x) = 0$ (or $f(x) = 1$) for all x
- f is a balanced if $f(x) = 0$ for exactly half of the 2^n inputs x.
- Apply Hadamard gate to first n qubit state $|0\cdots 0\rangle$ and to the last qubit state $|1\rangle$ to get the $(n+1)$-qubit state

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} |x\rangle(|0\rangle - |1\rangle)$$

- Apply the circuit U_f for f to this state

$$\begin{aligned} U_f : |x\rangle(|0\rangle - |1\rangle) &\to |x\rangle(|f(x)\rangle - |f(x) \oplus 1\rangle) \\ &= \begin{cases} |x\rangle(|0\rangle - |1\rangle) & \text{if } f(x) = 0 \\ -|x\rangle(|0\rangle - |1\rangle) & \text{if } f(x) = 1 \end{cases} \\ &= (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle) \end{aligned}$$

Quantum parallelism: The Deutsch-Jozsa algorithm

- f is a constant if $f(x) = 0$ (or $f(x) = 1$) for all x
- f is a balanced if $f(x) = 0$ for exactly half of the 2^n inputs x.
- Apply Hadamard gate to first n qubit state $|0\cdots 0\rangle$ and to the last qubit state $|1\rangle$ to get the $(n+1)$-qubit state

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} |x\rangle(|0\rangle - |1\rangle)$$

- Apply the circuit U_f for f to this state

$$\begin{aligned} U_f : |x\rangle(|0\rangle - |1\rangle) \quad & \rightarrow |x\rangle(|f(x)\rangle - |f(x)\oplus 1\rangle) \\ & = \begin{cases} |x\rangle(|0\rangle - |1\rangle) & \text{if } f(x) = 0 \\ -|x\rangle(|0\rangle - |1\rangle) & \text{if } f(x) = 1 \end{cases} \\ & = (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle) \end{aligned}$$

Quantum parallelism: The Deutsch-Jozsa algorithm

- f is a constant if $f(x) = 0$ (or $f(x) = 1$) for all x
- f is a balanced if $f(x) = 0$ for exactly half of the 2^n inputs x.
- Apply Hadamard gate to first n qubit state $|0\cdots 0\rangle$ and to the last qubit state $|1\rangle$ to get the $(n+1)$-qubit state

$$\frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} |x\rangle(|0\rangle - |1\rangle)$$

- Apply the circuit U_f for f to this state

$$\begin{aligned} U_f : |x\rangle(|0\rangle - |1\rangle) \quad & \rightarrow |x\rangle(|f(x)\rangle - |f(x) \oplus 1\rangle) \\ & = \begin{cases} \;\; |x\rangle(|0\rangle - |1\rangle) & \text{if } f(x) = 0 \\ -|x\rangle(|0\rangle - |1\rangle) & \text{if } f(x) = 1 \end{cases} \\ & = (-1)^{f(x)} |x\rangle(|0\rangle - |1\rangle) \end{aligned}$$

Quantum parallelism: The Deutsch-Jozsa algorithm (continued)

$$U_f : \frac{1}{\sqrt{2^{n+1}}}\sum_{x\in\{0,1\}^n}|x\rangle(|0\rangle-|1\rangle) \to \frac{1}{\sqrt{2^{n+1}}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle(|0\rangle-|1\rangle)$$

Now apply $H\otimes\cdots\otimes H$ to the above state (that is, first n-qubits).

- Note that $H|x\rangle = \sum_z(-1)^{xz}|z\rangle/\sqrt{2}$ for a single bit x. Thus

$$H^{\otimes n}|x\rangle = \frac{\sum_{z\in\{0,1\}^n}(-1)^{x\cdot z}|z\rangle}{\sqrt{2^{n+1}}}$$

- That is,

$$H^{\otimes n}|\phi\rangle = \sum_z\sum_x \frac{(-1)^{x\cdot z+f(x)}|z\rangle}{\sqrt{2^n}}$$

- Note that the amplitude for the state $|0\rangle^{\otimes n}$ is $\sum_x(-1)^{f(x)}/2^n$

Quantum parallelism: The Deutsch-Jozsa algorithm (continued)

$$U_f : \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} |x\rangle(|0\rangle - |1\rangle) \to \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$$

Now apply $H \otimes \cdots \otimes H$ to the above state (that is, first n-qubits).

- Note that $H|x\rangle = \sum_z (-1)^{xz}|z\rangle/\sqrt{2}$ for a single bit x. Thus

$$H^{\otimes n}|x\rangle = \frac{\sum_{z \in \{0,1\}^n} (-1)^{x \cdot z}|z\rangle}{\sqrt{2^{n+1}}}$$

- That is,

$$H^{\otimes n}|\phi\rangle = \sum_z \sum_x \frac{(-1)^{x \cdot z + f(x)}|z\rangle}{\sqrt{2^n}}$$

- Note that the amplitude for the state $|0\rangle^{\otimes n}$ is $\sum_x (-1)^{f(x)}/2^n$

Quantum parallelism: The Deutsch-Jozsa algorithm (continued)

$$U_f : \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} |x\rangle(|0\rangle - |1\rangle) \to \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$$

Now apply $H\otimes\cdots\otimes H$ to the above state (that is, first n-qubits).

- Note that $H|x\rangle = \sum_z (-1)^{xz}|z\rangle/\sqrt{2}$ for a single bit x. Thus

$$H^{\otimes n}|x\rangle = \frac{\sum_{z\in\{0,1\}^n}(-1)^{x\cdot z}|z\rangle}{\sqrt{2^{n+1}}}$$

- That is,

$$H^{\otimes n}|\phi\rangle = \sum_z \sum_x \frac{(-1)^{x\cdot z + f(x)}|z\rangle}{\sqrt{2^n}}$$

- Note that the amplitude for the state $|0\rangle^{\otimes n}$ is $\sum_x (-1)^{f(x)}/2^n$

Quantum parallelism: The Deutsch-Jozsa algorithm (continued)

- The amplitude for the state $|0\rangle^{\otimes n}$ is $\sum_x (-1)^{f(x)}/2^n$
- If f is constant, then we get the state $\pm|0\cdots0\rangle$
- If f is balanced, then the term $|0\cdots0\rangle$ disappears. Thus measuring each bit individually shows at least one qubit is non-zero

Quantum parallelism: The Deutsch-Jozsa algorithm (continued)

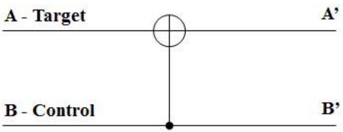
- The amplitude for the state $|0\rangle^{\otimes n}$ is $\sum_x (-1)^{f(x)}/2^n$
- If f is constant, then we get the state $\pm|0\cdots 0\rangle$
- If f is balanced, then the term $|0\cdots 0\rangle$ disappears. Thus measuring each bit individually shows at least one qubit is non-zero

Quantum parallelism: The Deutsch-Jozsa algorithm (continued)

- The amplitude for the state $|0\rangle^{\otimes n}$ is $\sum_x (-1)^{f(x)}/2^n$
- If f is constant, then we get the state $\pm|0\cdots 0\rangle$
- If f is balanced, then the term $|0\cdots 0\rangle$ disappears. Thus measuring each bit individually shows at least one qubit is non-zero

Controlled NOT

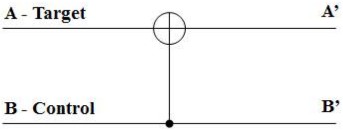
- A gate which operates on two qubits is called a Controlled-NOT (CN) Gate. If the bit on the control line is 1, invert the bit on the target line.
- The CN gate has a similar behavior to the XOR gate with some extra information to make it reversible



Input		Output	
A	B	A'	B'
0	0	0	0
0	1	1	1
1	0	1	0
1	1	0	1

Controlled NOT

- A gate which operates on two qubits is called a Controlled-NOT (CN) Gate. If the bit on the control line is 1, invert the bit on the target line.
- The CN gate has a similar behavior to the XOR gate with some extra information to make it reversible

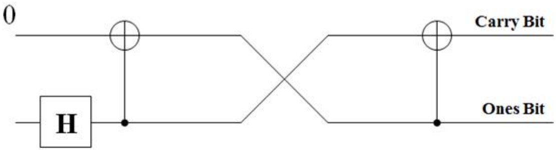


Input		Output	
A	B	A'	B'
0	0	0	0
0	1	1	1
1	0	1	0
1	1	0	1

Example multiplication by 2

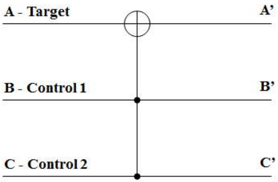
- We can build a reversible logic circuit to calculate multiplication by 2 using CN gates arranged in the following manner:

Input		Output	
Carry Bit	Ones Bit	Carry Bit	Ones Bit
0	0	0	0
0	1	1	0



Controlled Controlled NOT (CCN): Toffoli gate

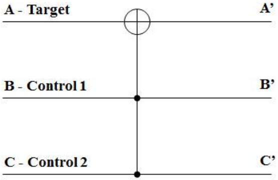
- A gate which operates on three qubits is called a Controlled Controlled NOT (CCN) Gate iff the bits on both of the control lines are 1,then the target bit is inverted.
- $A' = A \oplus (B \wedge C)$



Input			Output		
A	B	C	A'	B'	C'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	0
1	1	1	0	1	1

Controlled Controlled NOT (CCN): Toffoli gate

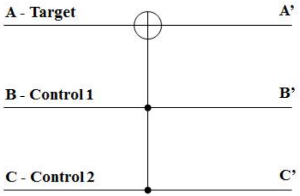
- A gate which operates on three qubits is called a Controlled Controlled NOT (CCN) Gate iff the bits on both of the control lines are 1,then the target bit is inverted.
- $A' = A \oplus (B \wedge C)$



Input			Output		
A	B	C	A'	B'	C'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	0
1	1	1	0	1	1

A Universal Quantum Computer

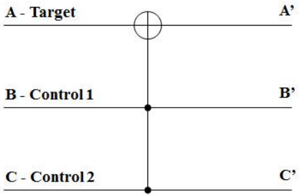
- The CCN gate has been shown to be a universal reversible logic gate as it can be used as a NAND gate.
- When the target input is 1, the target output is a result of a NAND of B and C.



Input			Output		
A	B	C	A'	B'	C'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	0
1	1	1	0	1	1

A Universal Quantum Computer

- The CCN gate has been shown to be a universal reversible logic gate as it can be used as a NAND gate.
- When the target input is 1, the target output is a result of a NAND of B and C.



Input			Output		
A	B	C	A'	B'	C'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	0
1	1	1	0	1	1

Q&A

Q&A?