COL863: Quantum Computation and Information

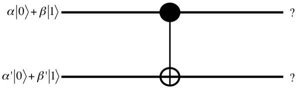
Ragesh Jaiswal, CSE, IIT Delhi

Introduction

- Multiple qubit gates:
  - Claim: We saw that there is a quantum analogue of the classical `NOT` gate. If there is a similar analogue for `NAND` gate, then any classical logic circuit will have a quantum analogue.
  - Why should the above claim hold? `NAND` gate is a universal gate.
  - Does a quantum analogue of `NAND` gate exist? No
  - Is there a reversible gate that is universal for quantum computation? Yes
    - This is called the controlled-NOT gate or `CNOT` gate.
    - More precisely, the matrix representing the gate is given by

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

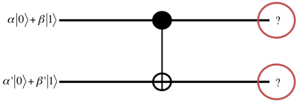
    - Question: What is the output of the following circuit?



- Multiple qubit gates:
  - Claim: We saw that there is a quantum analogue of the classical NOT gate. If there is a similar analogue for NAND gate, then any classical logic circuit will have a quantum analogue.
  - Why should the above claim hold? NAND gate is a universal gate.
  - Does a quantum analogue of NAND gate exist? No
  - Is there a reversible gate that is universal for quantum computation? Yes
    - This is called the controlled-NOT gate or CNOT gate.
    - More precisely, the matrix representing the gate is given by

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

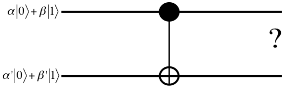
    - Question: What is the output of the following circuit?



- Multiple qubit gates:
  - Claim: We saw that there is a quantum analogue of the classical NOT gate. If there is a similar analogue for NAND gate, then any classical logic circuit will have a quantum analogue.
  - Why should the above claim hold? NAND gate is a universal gate.
  - Does a quantum analogue of NAND gate exist? No
  - Is there a reversible gate that is universal for quantum computation? Yes
    - This is called the controlled-NOT gate or CNOT gate.
    - More precisely, the matrix representing the gate is given by

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

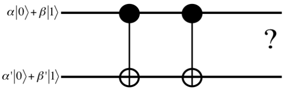
    - Question: What is the output of the following circuit?



- Multiple qubit gates:
  - Claim: We saw that there is a quantum analogue of the classical `NOT` gate. If there is a similar analogue for `NAND` gate, then any classical logic circuit will have a quantum analogue.
  - Why should the above claim hold? `NAND` gate is a universal gate.
  - Does a quantum analogue of `NAND` gate exist? No
  - Is there a reversible gate that is universal for quantum computation? Yes
    - This is called the controlled-NOT gate or `CNOT` gate.
    - More precisely, the matrix representing the gate is given by

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

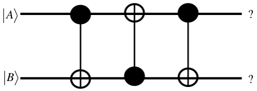
    - Question: What is the output of the following circuit?



- Multiple qubit gates:
  - Claim: We saw that there is a quantum analogue of the classical NOT gate. If there is a similar analogue for NAND gate, then any classical logic circuit will have a quantum analogue.
  - Why should the above claim hold? NAND gate is a universal gate.
  - Does a quantum analogue of NAND gate exist? No
  - Is there a reversible gate that is universal for quantum computation? Yes
    - This is called the controlled-NOT gate or CNOT gate.
    - More precisely, the matrix representing the gate is given by

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

    - Question: What is the output of the following circuit?



- Multiple qubit gates:
  - Claim: We saw that there is a quantum analogue of the classical `NOT` gate. If there is a similar analogue for `NAND` gate, then any classical logic circuit will have a quantum analogue.
  - Why should the above claim hold? `NAND` gate is a universal gate.
  - Does a quantum analogue of `NAND` gate exist? No
  - Is there a reversible gate that is universal for quantum computation? Yes the `CNOT` gate
    - This is called the controlled-NOT gate or `CNOT` gate.
    - More precisely, the matrix representing the gate is given by

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

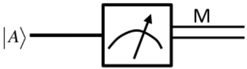
    - Claim: *Any multiple qubit logic gate may be composed from* `CNOT` *and single qubit gates.*

- Multiple qubit gates:
  - Claim: We saw that there is a quantum analogue of the classical NOT gate. If there is a similar analogue for NAND gate, then any classical logic circuit will have a quantum analogue.
  - Why should the above claim hold? NAND gate is a universal gate.
  - Does a quantum analogue of NAND gate exist? No
  - Is there a reversible gate that is universal for quantum computation? Yes the CNOT gate

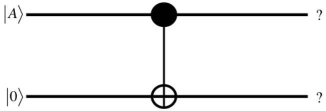
- Measurements:
  - We now have a high-level understanding of how a quantum circuit evolves. What can be obtain or measure from the circuit?
  - We said that we can measure a qubit in the computation basis $|0\rangle$ and $|1\rangle$ which are just one orthonormal basis. Can we measure in some other orthonormal basis?

- Measurements:
  - We now have a high-level understanding of how a quantum circuit evolves. What can be obtain or measure from the circuit?
  - We said that we can measure a qubit in the computation basis $|0\rangle$ and $|1\rangle$ which are just one orthonormal basis. Can we measure in some other orthonormal basis? Yes
    - We can measure in any orthonormal basis $|a\rangle, |b\rangle$. If the state of the qubit can be expressed as $\alpha|a\rangle + \beta|b\rangle$, then the measurement result is a with probability $|\alpha|^2$ and b with probability $|\beta|^2$.
    - One such popular basis is the $|+\rangle, |-\rangle$ basis that are expressed as $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.
    - Question: Express $\alpha|0\rangle + \beta|1\rangle$ in the $|+\rangle, |-\rangle$ basis.

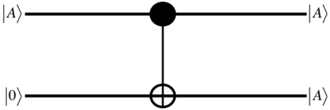
- Measurements:
  - We now have a high-level understanding of how a quantum circuit evolves. What can be obtain or measure from the circuit?
  - We said that we can measure a qubit in the computation basis $|0\rangle$ and $|1\rangle$ which are just one orthonormal basis. Can we measure in some other orthonormal basis? Yes
    - We can measure in any orthonormal basis $|a\rangle, |b\rangle$. If the state of the qubit can be expressed as $\alpha |a\rangle + \beta |b\rangle$, then the measurement result is a with probability $|\alpha|^2$ and b with probability $|\beta|^2$.
    - One such popular basis is the $|+\rangle, |-\rangle$ basis that are expressed as $|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ and $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$.
    - In quantum circuit diagrams, measurement of a qubit is represented as below:



- Some exercises:
  - What is the output of the following circuit?

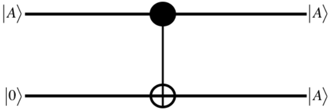


- <u>Some exercises</u>:
  - What is the output of the following circuit?

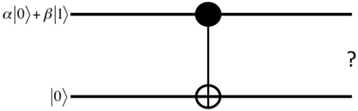


  - So, is the above circuit a qubit-copying circuit?

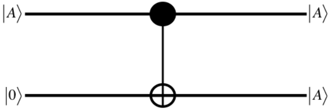
- <u>Some exercises</u>:
  - What is the output of the following circuit?



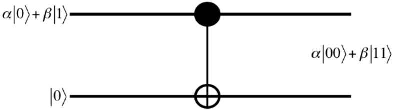
  - So, is the above circuit a qubit-copying circuit? No
    - Consider what happens in the following circuit?



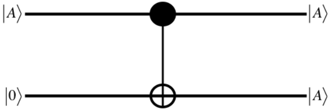
- Some exercises:
  - What is the output of the following circuit?



  - So, is the above circuit a qubit-copying circuit? No
    - Consider what happens in the following circuit?



- Some exercises:
  - What is the output of the following circuit?



  - So, is the above circuit a qubit-copying circuit? No
  - No-Cloning Theorem: It is impossible to copy an unknown quantum state input.

- Some exercises:
  - Let $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ be any unitary matrix representing a single-qubit gate Q. Consider the matrix:

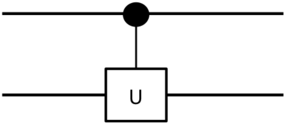
$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & q \\ 0 & 0 & r & s \end{bmatrix}$$

Is this matrix unitary?

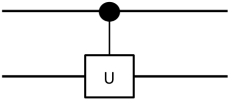
- Some exercises:
  - Let $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ be any unitary matrix representing a single-qubit gate U. Consider the matrix:

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & q \\ 0 & 0 & r & s \end{bmatrix}$$

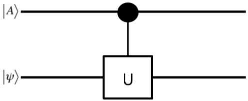
    Is this matrix unitary? Yes
  - So, this is a valid two-qubit quantum gate and is represented as:



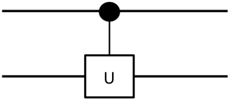
- Some exercises:
  - Let $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ be any unitary matrix representing a single-qubit gate U. Consider the matrix: $M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & q \\ 0 & 0 & r & s \end{bmatrix}$. Is this matrix unitary? Yes
  - So, this is a valid two-qubit quantum gate and is represented as:



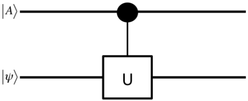
  - Question: Draw the quantum truth table for the circuit below:



- Some exercises:
  - Let $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ be any unitary matrix representing a single-qubit gate U. Consider the matrix: $M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & q \\ 0 & 0 & r & s \end{bmatrix}$. Is this matrix unitary? Yes
  - So, this is a valid two-qubit quantum gate and is represented as:

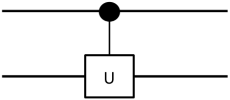


  - Question: Draw the quantum truth table for the circuit below:

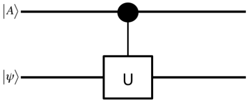


Input qubits	Output qubits
$\|0\rangle \|\psi\rangle$	$\|0\rangle \|\psi\rangle$
$\|1\rangle \|\psi\rangle$	$\|1\rangle U(\|\psi\rangle)$

- Some exercises:
  - Let $\begin{bmatrix} p & q \\ r & s \end{bmatrix}$ be any unitary matrix representing a single-qubit gate U. Consider the matrix: $M = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & q \\ 0 & 0 & r & s \end{bmatrix}$. Is this matrix unitary? Yes
  - So, this is a valid two-qubit quantum gate and is represented as:



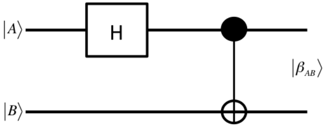
  - Question: Draw the quantum truth table for the circuit below:



Input qubits	Output qubits
$\|0\rangle\ \|\psi\rangle$	$\|0\rangle\ \|\psi\rangle$
$\|1\rangle\ \|\psi\rangle$	$\|1\rangle\ U(\|\psi\rangle)$

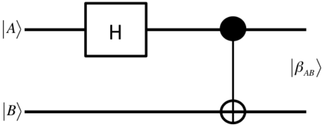
  - This is known as the controlled-U gate. The U gate is conditionally applied to the second qubit.

- Some exercises:
  - What is the output of the following circuit for different input states as shown:



In	Out
$\|00\rangle$	?
$\|01\rangle$	?
$\|10\rangle$	?
$\|11\rangle$	?

- Some exercises:
  - What is the output of the following circuit for different input states as shown:



In	Out
$\|00\rangle$	$\frac{\|00\rangle+\|11\rangle}{\sqrt{2}} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$\frac{\|01\rangle+\|10\rangle}{\sqrt{2}} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$\frac{\|00\rangle-\|11\rangle}{\sqrt{2}} \equiv \|\beta_{10}\rangle$
$\|11\rangle$	$\frac{\|01\rangle-\|10\rangle}{\sqrt{2}} \equiv \|\beta_{11}\rangle$

  - $|\beta_{00}\rangle, |\beta_{01}\rangle, |\beta_{10}\rangle, |\beta_{11}\rangle$ are called Bell states or EPR-pairs or EPR-states (after Bell, Einstein, Podolsky, and Rosen). These exhibit interesting properties as we will see in our first application to quantum-teleportation.

End