COL866: Quantum Computation and Information

Ragesh Jaiswal, CSE, IIT Delhi

Introduction

- What is a qubit? Quantum analogue of classical bit.
- Classical bit can be realised in real physical systems. Does it hold for qubits? We will work with yes.
- The classical bit has two states 0 and 1. Is qubit similar?
  - Yes and no. A qubit can be in states $|0\rangle$ and $|1\rangle$. However, these are not the only two states of the qubit.
  - A qubit can also be in a superposition or linear combination of states such as: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex numbers.
- Then is it true that there are infinitely many possible states for a qubit?
  - Yes this is true.
- Can all these infinitely many states be recognised or measured? In other words, can one determine the state of a qubit (i.e., α, β)?
  - No. A measurement results in either 0 or 1 as output.
  - For a qubit in state $\alpha|0\rangle + \beta|1\rangle$, the probability of 0 is $|\alpha|^2$ and 1 is $|\beta|^2$ (*Note that this means* $|\alpha|^2 + |\beta|^2 = 1$)
  - Measurements changes the state of the qubit. If the measurement results in $x \in \{0, 1\}$, then the post-measurement state is $|x\rangle$.

- What is a qubit? Quantum analogue of classical bit.
- Classical bit can be realised in real physical systems. Does it hold for qubits? We will work with yes.
- The classical bit has two states 0 and 1. Is qubit similar?
  - Summary: The state of a qubit is a *unit* vector in a two-dimensional complex vector space with $|0\rangle$ and $|1\rangle$ as the orthonormal basis (interpreted as computational basis states).

- What is a qubit? Quantum analogue of classical bit.
- Classical bit can be realised in real physical systems. Does it hold for qubits? We will work with yes.
- The classical bit has two states 0 and 1. Is qubit similar?
  - Summary: The state of a qubit is a *unit* vector in a two-dimensional complex vector space with $|0\rangle$ and $|1\rangle$ as the orthonormal basis (interpreted as computational basis states).
- Doesn't this mean that a qubit can encode infinite amount of information?
  - This is tricky. Even though α and β may encode a lot of information, the information available to us is only through a measurement and we can only extract a single bit of information from a measurement.
  - However, note that nature keeps track of α, β.

- What is a qubit? Quantum analogue of classical bit.
- Classical bit can be realised in real physical systems. Does it hold for qubits? We will work with yes.
- The classical bit has two states 0 and 1. Is qubit similar?
  - Summary: The state of a qubit is a *unit* vector in a two-dimensional complex vector space with $|0\rangle$ and $|1\rangle$ as the orthonormal basis (interpreted as computational basis states).
- Doesn't this mean that a qubit can encode infinite amount of information? No
- What about multiple qubit systems?
  - A two qubit system can be written as a superposition of computational basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$:

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

- What is a qubit? Quantum analogue of classical bit.
- Classical bit can be realised in real physical systems. Does it hold for qubits? We will work with yes.
- The classical bit has two states 0 and 1. Is qubit similar?
  - Summary: The state of a qubit is a *unit* vector in a two-dimensional complex vector space with $|0\rangle$ and $|1\rangle$ as the orthonormal basis (interpreted as computational basis states).
- Doesn't this mean that a qubit can encode infinite amount of information? No
- What about multiple qubit systems?
  - A two qubit system can be written as a superposition of computational basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$:

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

  - Can individual qubits be measured? Yes
  - What is the probability that the measurement output of the first qubit is 0?

- What is a qubit? Quantum analogue of classical bit.
- Classical bit can be realised in real physical systems. Does it hold for qubits? We will work with yes.
- The classical bit has two states 0 and 1. Is qubit similar?
  - Summary: The state of a qubit is a *unit* vector in a two-dimensional complex vector space with $|0\rangle$ and $|1\rangle$ as the orthonormal basis (interpreted as computational basis states).
- Doesn't this mean that a qubit can encode infinite amount of information? No
- What about multiple qubit systems?
  - A two qubit system can be written as a superposition of computational basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$:

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

  - Can individual qubits be measured? Yes
  - What is the probability that the measurement output of the first qubit is 0? $|\alpha_{00}|^2 + |\alpha_{01}|^2$
  - What is the post-measurement state of the system given that the measurement output of the first qubit is 0?

- What is a qubit? Quantum analogue of classical bit.
- Classical bit can be realised in real physical systems. Does it hold for qubits? We will work with yes.
- The classical bit has two states 0 and 1. Is qubit similar?
  - Summary: The state of a qubit is a *unit* vector in a two-dimensional complex vector space with $|0\rangle$ and $|1\rangle$ as the orthonormal basis (interpreted as computational basis states).
- Doesn't this mean that a qubit can encode infinite amount of information? No
- What about multiple qubit systems?
  - A two qubit system can be written as a superposition of computational basis states $|00\rangle, |01\rangle, |10\rangle, |11\rangle$:

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

  - Can individual qubits be measured? Yes
  - What is the probability that the measurement output of the first qubit is 0? $|\alpha_{00}|^2 + |\alpha_{01}|^2$
  - What is the post-measurement state of the system given that the measurement output of the first qubit is 0? $|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$

- What is a qubit? Quantum analogue of classical bit.
- Classical bit can be realised in real physical systems. Does it hold for qubits? We will work with yes.
- The classical bit has two states 0 and 1. Is qubit similar?
  - Summary: The state of a qubit is a *unit* vector in a two-dimensional complex vector space with $|0\rangle$ and $|1\rangle$ as the orthonormal basis (interpreted as computational basis states).
- Doesn't this mean that a qubit can encode infinite amount of information? No
- What about multiple qubit systems?
  - An n-qubit system is a unit vector in a 2^n-dimensional complex vector space with computational basis states $|00...0\rangle, ... |11...1\rangle$.

- What is a qubit? Quantum analogue of classical bit.
- Classical bit can be realised in real physical systems. Does it hold for qubits? We will work with yes.
- The classical bit has two states 0 and 1. Is qubit similar?
  - Summary: The state of a qubit is a *unit* vector in a two-dimensional complex vector space with $|0\rangle$ and $|1\rangle$ as the orthonormal basis (interpreted as computational basis states).
- Doesn't this mean that a qubit can encode infinite amount of information? No
- What about multiple qubit systems?
  - An n-qubit system is a unit vector in a 2^n-dimensional complex vector space with computational basis states $|00...0\rangle, ... |11...1\rangle$.
- How do a system of qubits evolve or chage? Computation over classical bit systems can be expressed in terms of circuits. Can we do something similar for qubit systems?

- What is a qubit? Quantum analogue of classical bit.
- Classical bit can be realised in real physical systems. Does it hold for qubits? We will work with yes.
- The classical bit has two states 0 and 1. Is qubit similar?
    - Summary: The state of a qubit is a *unit* vector in a two-dimensional complex vector space with $|0\rangle$ and $|1\rangle$ as the orthonormal basis (interpreted as computational basis states).
- Doesn't this mean that a qubit can encode infinite amount of information? No
- What about multiple qubit systems?
    - An n-qubit system is a unit vector in a 2^n-dimensional complex vector space with computational basis states $|00...0\rangle, ... |11...1\rangle$.
- How do a system of qubits evolve or chage? Computation over classical bit systems can be expressed in terms of circuits. Can we do something similar for qubit systems?
    - Yes. The Quantum counterpart of classical circuits are called quantum circuits that has quantum gates.

- What is a qubit? Quantum analogue of classical bit.
- Classical bit can be realised in real physical systems. Does it hold for qubits? We will work with yes.
- The classical bit has two states 0 and 1. Is qubit similar?
  - Summary: The state of a qubit is a *unit* vector in a two-dimensional complex vector space with $|0\rangle$ and $|1\rangle$ as the orthonormal basis (interpreted as computational basis states).
- Doesn't this mean that a qubit can encode infinite amount of information? No
- What about multiple qubit systems?
  - An n-qubit system is a unit vector in a 2^n-dimensional complex vector space with computational basis states $|00...0\rangle, \ldots |11...1\rangle$.
- How do a system of qubits evolve or chage? Computation over classical bit systems can be expressed in terms of circuits. Can we do something similar for qubit systems? Quantum circuit

Quantum Circuit

- Single qubit gates:
  There is only one single-input logical gate in the classical setting, the NOT gate. What could be a quantum version of such a gate?
  - The general state of a qubit is expressed as $\alpha|0\rangle + \beta|1\rangle$. The quantum version of NOT gate does the following conversion:
    $$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|1\rangle + \beta|0\rangle$$
    This is known as the X gate.
  - The general state of a qubit can be written using matrix notation as $\left[\begin{smallmatrix}\alpha \\ \beta\end{smallmatrix}\right]$. The X gate operating on the qubit can then be interpreted as a simple matrix multiplication where $X \equiv \left[\begin{smallmatrix}0 & 1 \\ 1 & 0\end{smallmatrix}\right]$.
  - In general single-qubit gates can be expressed as 2×2 complex matrices. Can any 2×2 matrix represent a valid single-qubit gate?

- Single qubit gates:
  There is only one single-input logical gate in the classical setting, the `NOT` gate. What could be a quantum version of such a gate?
  - The general state of a qubit is expressed as $\alpha|0\rangle + \beta|1\rangle$. The quantum version of `NOT` gate does the following conversion:

    $$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|1\rangle + \beta|0\rangle$$

    This is known as the X gate.
  - The general state of a qubit can be written using matrix notation as $\left[\begin{smallmatrix}\alpha\\ \beta\end{smallmatrix}\right]$. The X gate operating on the qubit can then be interpreted as a simple matrix multiplication where $X \equiv \left[\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right]$.
  - In general single-qubit gates can be expressed as 2×2 complex matrices. Can any 2×2 matrix represent a valid single-qubit gate? No
    - Is $\left[\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right]$ a valid single-qubit gate?

- Single qubit gates:
  There is only one single-input logical gate in the classical setting, the `NOT` gate. What could be a quantum version of such a gate?
  - The general state of a qubit is expressed as $\alpha|0\rangle + \beta|1\rangle$. The quantum version of `NOT` gate does the following conversion:
  $$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|1\rangle + \beta|0\rangle$$
  This is known as the X gate.
  - The general state of a qubit can be written using matrix notation as $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$. The X gate operating on the qubit can then be interpreted as a simple matrix multiplication where $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.
  - In general single-qubit gates can be expressed as 2×2 complex matrices. Can any 2×2 matrix represent a valid single-qubit gate? No
    - Is $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$ a valid single-qubit gate? No
    - In general, if the state after applying the gate is $\alpha'|0\rangle + \beta'|1\rangle$, then $|\alpha'|^2 + |\beta'|^2 = 1$.
    - A necessary condition to ensure this is that the matrix is unitary. That is, $U^\dagger U = I$.
    - This also happens to be a sufficient condition for any quantum gate.
    - One implication of this fact is that there can be infinitely many single-qubit gates.

- Single qubit gates: Frequently used gates
  - X gate: Analogue of classical `NOT` gate with matrix representation

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

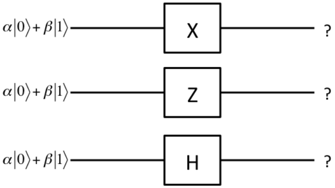
  - Z gate: Matrix representation:

$$Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

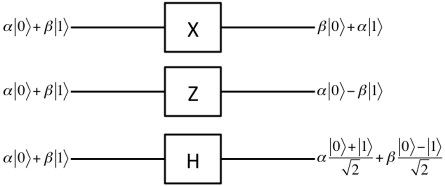
  - H gate: Called Hadamard gate with matrix representation:

$$H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

- Single qubit gates: Frequently used gates
  - X gate: Analogue of classical NOT gate with matrix representation $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.
  - Z gate: Matrix representation: $Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
  - H gate: Called Hadamard gate with matrix representation: $H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.



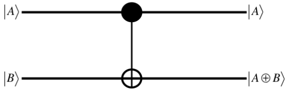
- Single qubit gates: Frequently used gates
  - X gate: Analogue of classical NOT gate with matrix representation $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.
  - Z gate: Matrix representation: $Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
  - H gate: Called Hadamard gate with matrix representation: $H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.



- 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?

- 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
    - `NAND` gate is irreversible. That is one cannot obtain A and B from $A \wedge B$.
    - Quantum gates are constrained to be reversible.
    - Unitary gates (operations using unitary matrices) are invertible and hence reversible.

- 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.



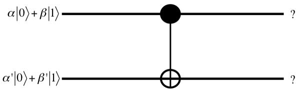
    - More precisely, the matrix representing the gate is given by

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

- 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

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

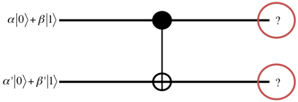
    - Question: What is the output of the following circuit?



- 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?



End