COL863: Quantum Computation and Information

Ragesh Jaiswal, CSE, IIT Delhi

Administrative Information

Administrative Information

- Instructor
  - Ragesh Jaiswal
  - *Email*: `rjaiswal@cse.iitd.ac.in`
  - *Office*: SIT Building, Room no. 403

Administrative Information

- Grading Scheme
  1. *Quizzes* (announced) : 25%
  2. *Minor 1 and 2*: 20% each.
  3. *Major*: 35%
- Policy on cheating:
  - Anyone found using unfair means in the course will receive an **F** grade.

Administrative Information

- Textbook: Quantum Computation and Quantum Information by *Michael A. Nielsen and Isaac L. Chuang*.
- Gradescope: A paperless grading system. Use the course code **74525Z** to register in the course on Gradescope. Use only your IIT Delhi email address to register on Gradescope.
- Course webpage: `http://www.cse.iitd.ac.in/~rjaiswal/Teaching/2021/COL863`.
  - The site will contain course information, references, problems. Please check this page regularly.

Introduction

- What are *Quantum computation* and *Quantum Information*?

Introduction

- What are *Quantum computation* and *Quantum Information*?
  - The study of information processing tasks that can be done using *quantum mechanical systems*.
- What is *quantum mechanics*?

Introduction

- What are *Quantum computation* and *Quantum Information*?
  - The study of information processing tasks that can be done using *quantum mechanical systems*.
- What is *quantum mechanics*?
  - Mathematical framework for constructing physical theories.

- What should you expect to know by the end of the course?
  - Mathematical framework of for designing quantum algorithms and information processing.
  - Examples where quantum information processing systems have gone beyond classical ones.
    - Factoring, discrete logarithm, superdense coding, quantum search...

Introduction

- What should you expect to know by the end of the course?
  - Mathematical framework of for designing quantum algorithms and information processing.
  - Examples where quantum information processing systems have gone beyond classical ones.
    - Factoring, discrete logarithm, superdense coding, quantum search...
- This is not a Quantum Mechanics course!
  - We will start and build from a purely mathematical abstraction without going into the details of how the mathematical framework was arrived at or why such a framework might be reasonable.

- Church-Turing Thesis
  - Any algorithmic process can be simulated using a Turing Machine.

- Church-Turing Thesis
  - Any algorithmic process can be simulated using a Turing Machine.
- Extended or strong Church-Turing Thesis
  - Any algorithmic process can be simulated efficiently using a Turing Machine.

- Church-Turing Thesis
  - Any algorithmic process can be simulated using a Turing Machine.
- Extended or strong Church-Turing Thesis
  - Any algorithmic process can be simulated efficiently using a Turing Machine.
- Extended or strong Church-Turing Thesis (randomized version)
  - Any algorithmic process can be simulated efficiently using a probabilistic Turing Machine.

- Church-Turing Thesis
  - Any algorithmic process can be simulated using a Turing Machine.
- Extended or strong Church-Turing Thesis
  - Any algorithmic process can be simulated efficiently using a Turing Machine.
- Extended or strong Church-Turing Thesis (randomized version)
  - Any algorithmic process can be simulated efficiently using a probabilistic Turing Machine.
- What about quantum mechanical processes? Can they be simulated efficiently by Turing Machines?

- Church-Turing Thesis
  - Any algorithmic process can be simulated using a Turing Machine.
- Extended or strong Church-Turing Thesis
  - Any algorithmic process can be simulated efficiently using a Turing Machine.
- Extended or strong Church-Turing Thesis (randomized version)
  - Any algorithmic process can be simulated efficiently using a probabilistic Turing Machine.
- What about quantum mechanical processes? Can they be simulated efficiently by Turing Machines?
  - There are examples where this is not known.
  - So, quantum computation may be the (only) candidate counterexample to the extended Church-Turing Thesis.

- Shannon's noiseless channel coding theorem
  - Quantifies the physical resources required to store the output of an information source.
- Shannon's noisy channel coding theorem
  - Quantifies the amount of information that is possible to reliably transmit through a noisy channel.
- What is the quantum analogue of the physical resource for encoding information? Qubit
- Some surprising results:
  - Superdense coding: Two classical bits can be communicated using a single quantum bit.
  - Distributed quantum computation: Quantum computers can require exponentially less communication to solve certain problems compared to classical computers.

- Private key cryptography
  - It is assumed that Alice and Bob share a secret key and protocols are designed using this assumption.

- Private key cryptography
  - It is assumed that Alice and Bob share a secret key and protocols are designed using this assumption.
  - Main issue: How do Alice and Bob share a secret key?
  - Quantum key distribution (Weisner,1960; Bennett and Brassard, 1984): Alice and Bob can communicate over a quantum channel to share a secret key even in presence of an adversary.

- Private key cryptography
  - It is assumed that Alice and Bob share a secret key and protocols are designed using this assumption.
  - Main issue: How do Alice and Bob share a secret key?
  - Quantum key distribution (Weisner,1960; Bennett and Brassard, 1984): Alice and Bob can communicate over a quantum channel to share a secret key even in presence of an adversary.
- Public key cryptography:
  - Alice and Bob both have a pair of public-private keys.
  - Messages are encoded using public key (that everyone knows) and can be decoded using the corresponding private key (that only the owner knows).
  - Such protocols exist. However, some popular ones become insecure if efficient algorithms for factoring and discrete logarithm problems are built.
  - Quantum algorithms: There are efficient quantum algorithms for both discrete logarithm and factoring.

- What is a qubit?
  - Qubit is to quantum computation as bit is to classical computation.
- Classical bit can be realised in real physical systems. Does it hold for qubits?
  - Yes but with a lot of *ifs* and *buts*. People would not have started talking about this concept if it were completely imaginary.
  - Since we do not have the expertise to go deeper into how qubits can be realised, we will treat it as a mathematical object.

- What is a qubit?
  - Qubit is to quantum computation as bit is to classical computation.
- Classical bit can be realised in real physical systems. Does it hold for qubits?
  - Yes but with a lot of *ifs* and *buts*. People would not have started talking about this concept if it were completely imaginary.
  - Since we do not have the expertise to go deeper into how qubits can be realised, we will treat it as a mathematical object.
- Okay ... the classical bit has two states 0 and 1 (and that is pretty much the full description of the bit). Is qubit similar?

- 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 be in a superposition or linear combination of states:

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

    where α and β are complex numbers.

- 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 $|x\rangle$.

End