Seminar 8

Created	@November 1, 2022 4:53 PM
Class	Quantum Computing Fundamentals
Type	Seminar
Reviewed	☐
Date	@November 6, 2022
Materials	week7_concepts.pdf

Introduction to Quantum Algorithms and Protocols

Week 7 | November 6th, 2022

- The parts if the quantum stack that we have seen so far
- Quantum Algorithms and Protocols:
  - What's the difference?
  - What algorithms and protocols do we know of?
- Superdense coding

Computation for Innovation

The problems we face in world require. lot of innovation: many of these innovations require the aid of computation (not enough computation power to make necessary breakthroughs)

- Japan's Fugaku supercomputer is the largest supercomputer in the world. there are some problems that it would take far too long for this computer to even solve

- The key goal of quantum computing is to leverage quantum resources to design quantum algorithms which are able to efficiently solve certain types of problems and approach computation differently.

So far we have been focused on the details of qubits, gates, and more. In today, we will review these parts and start seeing how they apply to quantum algorithms which are really the “computation” in quantum computation

Solving a Problem using Quantum Computer

- Goal: simulate a molecule on a q-computer → you provide input to a classical computer → classical computer converts input into construction for q-computer → q-computer converts the inputs into outputs using q-circuits → Q-computer sends the output back to a classical computer → classical computer shows you the output
- This process can be mapped into the q-stack

Quantum Cirucits:

A Q-circuit is a sequence of quantum gates. these gates work together to produce a target output state. We can organize the components of a q-circuits with the Quantum Circuit Model. This model breaks down the circuit into: States (qubits), Gates, Measurement.

Key: Measurement is random for any superposition states. The closer to |0> a state is, the more likely we measure 0 and similarly applied for 1.

Since the results can be random, we need to completely rerun our circuit many times to understand the state we’re measuring. Once a state is measured the superposition collapses and thus the q-state changes to whatever state is measured.

All of these concepts are the building blocks leading to algorithms and protocols

Introduction to Quantum Algorithms and Protocols:

Algorithms & Protocols (Classical)

Algorithm (recipe) - a specific procedure for solving a computation problem.

Protocol - A set if standard rules that allow electronic devices to communicate with each other

There are many different types of algorithms! For example: “searching algorithms” (finding correct option in a series of values), “sorting algorithms” (grouping a series of

values by a certain criteria), “ranking algorithms” (ordering a series in a particular appealing way).

Protocols are like contracts: Protocols coordinate communication between multiple systems. All parties involved need to agree upon a protocol in order for it work. protocols are like contracts that multiple parties abide by.

Example: “https://” (p stands for protocol):

- Originally developed in order to transfer information across the web; protocols are continuously refined

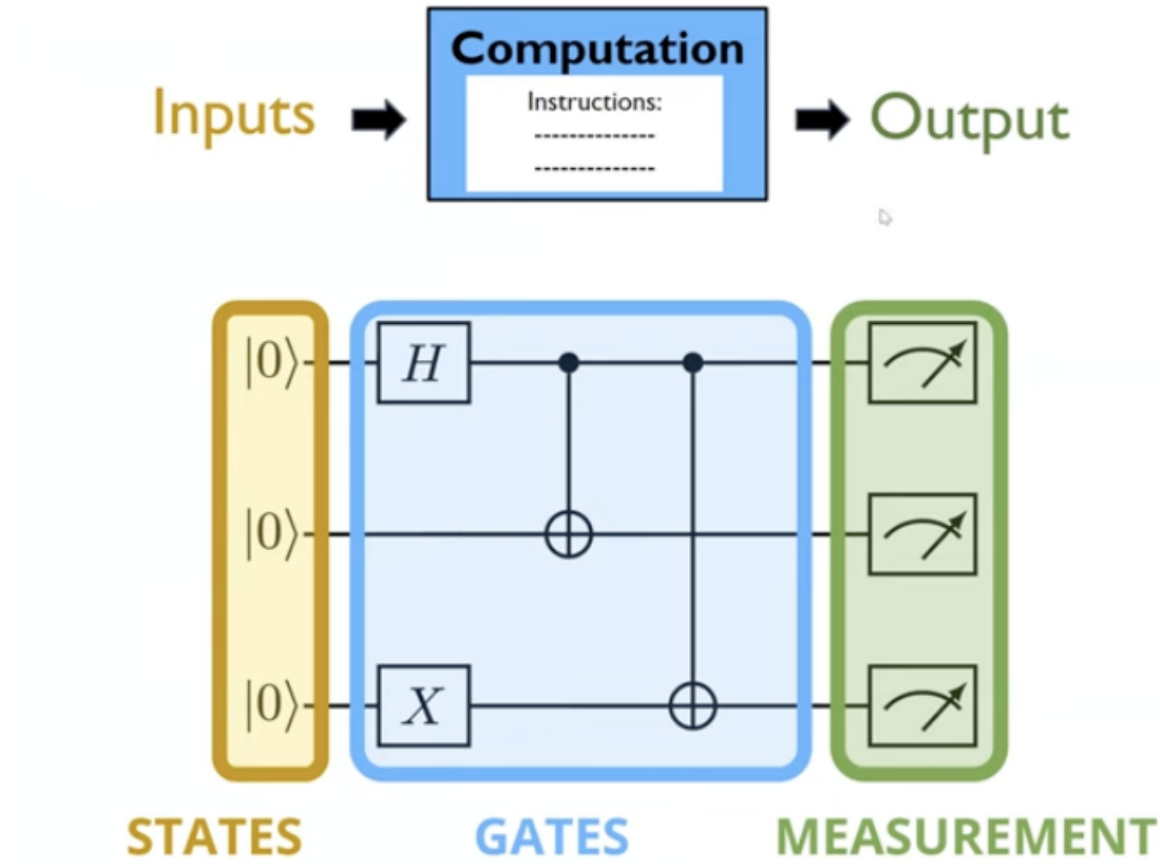
What about quantum algorithms and protocols?

Quantum Protocol:

A set of standard rules that use the properties of quantum physics to allow electronic devices to communicate with each other.

Quantum Algorithm:

Operate in the same exact structure like classical algorithms.



All q-algorithms boil down to quantum circuits, but not every q-circuit is a useful quantum algorithm. Find a q-algorithm that works and find a smart way to translate into the language of gates and circuits.

Useful Quantum Algorithms:

Quantum algorithms won't be useful unless they do something classical algorithms cannot do that also does something of value. They need to leverage our three quantum resources and do something clever with them:

- Superposition
- Entanglement
- Interference

Landscape of Quantum Algorithms

In order for use to be able to execute q-algorithms that cannot be matched classically, we need something called fault tolerance (a q-computer that can correct for errors so that outcome can be error-free).

We are currently in the era of Noisy Intermediate Scale Quantum, NISQ, devices. The art of q-algorithm design is that can we do something that we can't do with a normal computer?

Can we get some sort of quantum advantage using quantum computers?

Since 2019, there have started to be more and more demonstrations of quantum advantage.

As Q-devices get more sophisticated, it is valuable to know what the possible uses are or will be. here are some examples we will explore today:

Destsch-Jozsa:

- Phase Kickback
- Was one of the first q-algorithms that was proven to be significantly better than classical
- The core technique that was used was: Provide a CFX gate with two different superpositions, the control qubit will sneak away with information about both states. This is called a phase kick back. We will learn some information about the target through the control.
- Known Uses: None

Shor's Algorithm:

- QFT
- Factor's numbers efficiently. it was one of the first q-algorithms that's significantly better than classical and is useful.
- The core technique: Fundamentally relies on the Quantum Fourier transform discovered in the same year. It is a q-circuit that creates superpositions with very special properties
- It turns that QFT for 1 qubit is the H gate
- Known Uses: breaking RSA encryption (a world standard)

Grover Serach:

- Amplitude Amplification
- Can search a completely disorganized database more efficiently than any classical algorithm
- Fundamentally relies on amplitude amplification which amplifies the probability of measuring states of one kind
- Known Uses; Searching databases, applications in cryptography, optimization uses

All these algorithms will require fault tolerance to be useful!

Near-Term Algos:

- Hybrid and others
- trying to use q-computers to do something useful (some advantage over classical computers)
- Attempt to use current q-computers to do something useful. The other algorithms require very large and advanced q-computers to get any use out of.
- Concept: Variational Hybrid Algorithm
- Known Uses: Simulation, Machine Learning
- These tend to be classical quantum hybrid approaches where we use the best of classical and quantum computing together to do something nether one could do alone

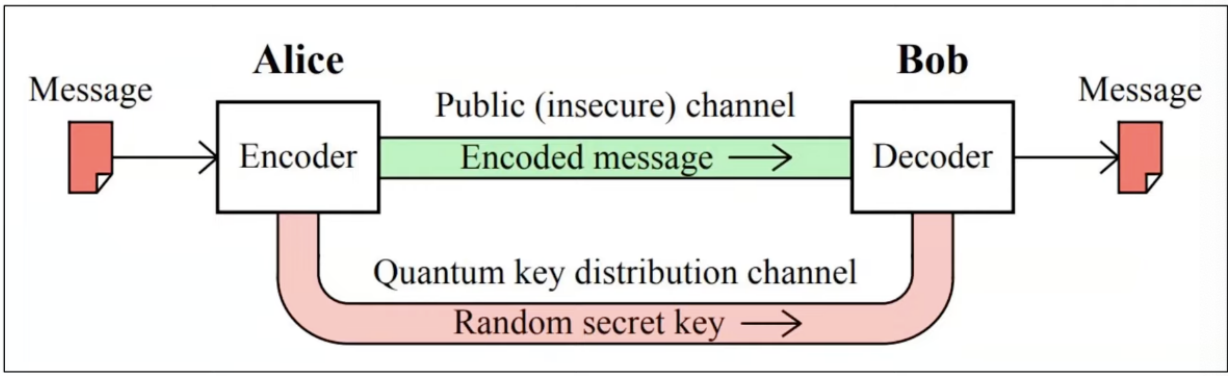
Landscape of Quantum Protocols:

Quantum Teleportation:

- A protocol where we can send a q-state to someone far away using entangled qubits and classical bits
- Known Uses: Quantum Internet, Cryptography
- You need an entangled state, measurement, and classical bits (teleportation can’t be done faster than speed of light since classical bit information are involved)
- Quantum Networking is a subfield of QISE that is about making this a reality, creating a quantum internet

Quantum Key Distribution:

- A protocol where we can establish a way to securely communicate with another person even of there's someone listening in



Superdense Coding:

- A protocol where we can send the equivalent of multiple classical bits with just one quantum bit. It's the ultimate compression scheme
- If you have two parties who are sharing an entangled pair, you can perform operations on one half of the share and you can send that half and the receiver will be able to decode and receive two classical bits of information. You need two qubits in this scheme, but will only need to send one qubit to get two classical bits of information. This is also a secure way to share information.
- You need both of the entangled qubits to get the information. by only having half, you can't get any useful information.
- Known Uses; Quantum Internet, Cryptography