Quantum Algorithms, Spring 2022: Lecture 1

Chandan Anand, Vishal Anand

January 19, 2022

1 Introduction

Computer is a physical device which processes information by executing algorithms, well-defined procedures, with finite description, for realizing that information processing task. An information-processing task can always be translated into a physical task. Hence, we can say information is physical.

Fundamental unit of classical computation is bits. Two possible discrete state either 0 or 1.

2 Irreversibility

Computational complexity deals with space and time to solve a computational problem. Another important computational resource is energy. Energy consumption in computation is deeply linked to the reversibility of the computation i.e. NAND gate, takes two input bits and produces a single output bit. This gate is intrinsically irreversible because, given the output of the gate, the input is not uniquely determined. NOT gate takes only a single input and negates the values of data in its input. This means that we can always construct the input bit from its output bit, hence NOT gate is reversible.

3 Entropy

Entropy is a measure of disorder, with systems having more disorder means less entropy. According to second law of thermodynamics, the entropy of isolated systems left to spontaneous evolution cannot decrease. Here entropy is defined as a state function of the system which we can calculate.

When viewed in terms of information theory, the entropy state function is the amount of information in the system that is needed to fully specify the microstate of the system. To capture this idea of information entropy of a state of a system, we have so called, Shannon entropy of the system. When we calculate this for AND gates, we find that this entropy, decreases which is in violation with 2nd law of thermodynamics. This issue was resolved when we consider not only the information processing device as system, but the device plus the environment as the system.

4 Landauer's Principle

Rolf Landauer pointed out in 1961 that

> A fundamental limit on the heat produced when erasing a bit of information has been confirmed in a fully quantum system by **?**].

Landauer's principle provides connection between irreversibility and energy consumption: Suppose a computer erases a single bit of information. The amount of energy dissipated into the environment is at least $(ln2)k_BT$, where k_B is Boltzmann's constant, and T is the temperature of the environment in which our computer is being kept.
OR
Suppose a computer erases a single bit of information. The entropy of the environment increases by at least k_Bln2, where k_B is Boltzmann's constant.

5   Maxwell's Demon

In 1871, James Clerk Maxwell proposed an idea which may break second law of thermodynamics. He conducted a thought experiment in which he envisioned a gas cylinder with two part. A demon reduce entropy of gas cylinder by individually separate passing fast and slow molecules into one half to another half of the cylinder. When a fast molecule approaches from the left side the demon opens a door between the partition, allowing the molecule through and then close the door. By doing this many times the total entropy of the cylinder can be decreased, in apparent violation of the second law of thermodynamics.

This Maxwell's demon paradox lies in the fact that the demon must perform measurements on the molecules moving between partitions. To determine gas molecule velocity must stores in the demon's memory. Because any memory is finite the demon must eventually begin erasing information from its memory, in order to have space for new measurement results. By Landauer's principle, erasing information increases the total entropy of system (demon, gas cylinder and environment).

Classical computer work on the principle of classical physics. However, nature phenomena more precisely explain by quantum physics. Physics of sub atomic particle is way different from classical physics. So, it is Obviousness Quantum Computer work on the principle on quantum physics.

6   Church-Turing Thesis

It states a computer problem can be solved on any computer that we could hope to build, if and only if it can be solved on a very simple 'machine', Turing machine.

Any algorithmic process can be simulated efficiently using a probabilistic Turing machine.

7   David Deutsch

Computing devices build on the principle of quantum physics can offer a strong version of this thesis. Computing machine resembling universal quantum computing could in principle be built and would have many remarkable properties not reproducible by any standard turing machine.

8   Richard Feynman

There is plenty of room at the bottom. **?**]

Above put a question that can we simulate physics on computer?
Quantum physics would be hard to simulate. For quantum physics numbers of variable: exponential in the size of the system. System of 50 electron: 2^{50} variables.

9   Quantum Algorithms

In quantum computing, a quantum algorithm is an algorithm which runs on a realistic model of quantum computation, the most commonly used model being the quantum circuit model of computation.

10   Shor's Algorithms

Factorize large number into prime numbers. Exponentially factor than the best classical algorithms (factoring is believed to be in NP.) **?**] Shor's algorithm solves the discrete logarithm problem and the integer factorization problem in polynomial time, whereas the best known classical algorithms take super-polynomial time.

11 Grover's Algorithms

Search for a solution out of N potential solution. **?**] Grover's algorithm searches an unstructured database (or an unordered list) with N entries, for a marked entry, using only $O(\sqrt{N})O(\sqrt{N})$ queries instead of the $O(N)O(N)$ queries required classically.

12 Quantum Simulation

Efficient quantum algorithms exist for quantum simulation (simulation physical system that are quantum mechanics in nature.)**?**]
Quantum simulators permit the study of quantum system in a programmable fashion. In this instance, simulators are special purpose devices designed to provide insight about specific physics problems. Quantum simulators may be contrasted with generally programmable "digital" quantum computers, which would be capable of solving a wider class of quantum problems.

To simulate a quantum system for time t with accuracy ϵ a quantum computer takes time $\mathcal{O}\left(t + \log \frac{1}{\epsilon}\right)$. **?**]

13 Quantum Linear Systems

Solves a quantum version of $Ax = b$ in a time exponentially faster than classical. **?**] In 2009 Aram Harrow, Avinatan Hassidim, and Seth Lloyd, formulated a quantum algorithm for solving linear systems. The algorithm estimates the result of a scalar measurement on the solution vector to a given linear system of equations. It can lead to many quantum machine learning (QML) algorithm. **?**]

14 Ground State Preparation

Quantum algorithm exist for finding ground state of Hamiltonian.**?**]

$\mathcal{O}\left(\frac{1}{\delta} \frac{1}{\langle 0||\psi\rangle}\right)$ eigenvalue gap between ground state.

Companies having quantum computers - Google(Cirq), IBM(Qiskit), Microsoft(#Q), D-Wave, IONQ...etc.

NISQ - Noisy Intermediate Scale Quantum device QEC - Quantum Error Correction.
Cross entropy benchmarks to check algorithms.

NISQ Algorithms -

- Useful NISQ algorithm ground state preparation, optimization.

- Contrived problem (Quantum Supremacy)