COL7160 : Quantum Computing

Lecture 1: Introduction

Instructor: Rajendra Kumar **Scribe:** Poojan Shah

1 What is Quantum Computing ?

One of the main motivations behind quantum computing is to predict the behaviour of a system of n particles interacting with each other according to quantum mechanics. We believe that doing so, in its full generality, classically requires $\exp(\Omega(n))$ time and space. To describe an n particle quantum system, where each particle can be in a superposition of 2^n basis states, we need to keep track of 2^n complex numbers which make up the *wave function* of the particles :

$$|\Psi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$$

whose evolution is given by *Schrodinger's* equation, where H is a $2^n \times 2^n$ matrix called the *Hamiltonian* of the system :

$$\frac{d}{dt}|\Psi\rangle = -iH|\Psi\rangle$$

Even accurately simulating the properties of $n \approx 500$ particle systems consumes large resources. How can we speed up or approximate these complex calculations?

2 A Brief History of Quantum Computing

The initial ideas for quantum computing can be traced back to the physicist Richard Feynman. In an invited talk in Physics of Computation Conference 1981 titled "Simulating Physics with Computers", he pointed out some key points :

1. Probabilisitic computers cannot simulate quantum mechanics efficiently.
2. Any efficient simulation of quantum mechanics must be quantum mechanical in nature itself.

> *"... nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical. By golly, it's a wonderful problem, because it doesn't look so easy ... "*

More of Feynman's ideas can be found in chapter 6 of the book [Fey96], which also contains an excellent account of classical computation from the lense of physics. David Deutsch formulated the *quantum turing machine* in [Deu85]. Bennet and Brassard showed how to use the laws of quantum mechanics to perform information theoretically secure key distribution in [BB84], which is now known as the famous BB84 protocol. A provable quantum speedup over all possible classical algorithms under an *black box oracle* model was shown by Bernstein and Vazirani in [BV93]. This speedup was only a polynomial speedup. Simon proposed a problem in [Sim94] in which a quantum algorithm had a provably exponential speedup over all possible quantum algorithms under a similar oracle model. After these were two major results in quantum algorithms : Shor's algorithm for factoring numbers in polynomial time using quantum computers [Sho94] which breaks the security of the widely used RSA public key cryptosystem [RSA78] and Grover's algorithm for unstructured search in square root of input size time [Gro96].

3 Looking Forward

We live in one of three possible world :

1. Quantum mechanics is wrong and factoring is hard.

2. There exists an efficient classical algorithm for factoring.

3. Quantum computers are provably more powerful than classical computers.

Today several government agencies and tech companies are in a *race* to build quantum computers that can do computational tasks faster than classical computers. But there are several engineering hurdles to be overcome yet. We are currently between classical simulators and full fledged quantum computers. We have quantum systems that have 100s or even 1000s of qubits, but they still succumb to too much noise, so complex computation is still a challenge (No examples of factoring of large numbers yet!). As computer scientists, the following areas are where we may contribute :

1. Developing new quantum algorithms for computational problems and improving old quantum algorithms to be less bulky.

2. Error correction : software solution to handle noise from hardware.

3. Complexity Theory : identifying problems for which we do not believe there are efficient quantum algorithms.

4. Quantum / Post-Quantum Cryptography.

References

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems & Signal Processing*, pages 175–179, 1984. Scan of the original 1984 paper; published in TCS 560 (2014) as well.

[BV93] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. In *Proceedings of the 25th Annual ACM Symposium on Theory of Computing (STOC)*, pages 11–20, 1993.

[Deu85] David Deutsch. Quantum theory, the church–turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. Series A*, 400:97–117, 1985.

[Fey96] Richard P. Feynman. *Feynman's Lectures on Computation.* Addison-Wesley, Reading, MA, 1996.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, STOC '96, page 212–219, New York, NY, USA, 1996. Association for Computing Machinery.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[Sho94] Peter W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[Sim94] D.R. Simon. On the power of quantum computation. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 116–123, 1994.