Project Proposal CSCI 5622

Introduction to Quantum Algorithms

Paramjot Singh and Laksh Advani

November 2017

Introduction

The idea of a quantum computer was first proposed in 1981 by Nobel laureate Richard Feynman, who pointed out that accurately and efficiently simulating quantum mechanical systems would be impossible on a classical computer, but that a new kind of machine, a computer itself "built of quantum mechanical elements which obey quantum mechanical laws" [1], might one day perform efficient simulations of quantum systems. Classical computers are inherently unable to simulate such a system using sub-exponential time and space complexity due to the exponential growth of the amount of data required to completely represent a quantum system. Quantum computers, on the other hand, exploit the unique, non-classical properties of the quantum systems from which they are built, allowing them to process exponentially large quantities of information in only polynomial time. Of course, this kind of computational power could have applications to a multitude of problems outside quantum mechanics, and in the same way that classical computation quickly branched away from its narrow beginnings facilitating simulations of Newtonian mechanics, the study of quantum algorithms has diverged greatly from simply simulating quantum physical systems to impact a wide variety of fields, including information theory, cryptography, language theory, and mathematics.

Background

Probably the most widely known development in quantum computation was Peter Shor's 1997 publication of a quantum algorithm for performing prime factorization of integers in essentially polynomial time [2]. Shor's algorithm was a monumental discovery not only because it provides exponential speedup over the fastest classical algorithms, but because a number of algorithms for public-key cryptography, including the commonly used RSA algorithm, depend on the fact that there is no known efficient classical algorithm to factor integers into prime numbers [3]. Shor demonstrated that the realization of a full-scale quantum computer would have the potential to provide a truly significant increase in computing speed, at the same time pointing out the possible implications of such an increase in computational power to the field of cybersecurity. For both reasons, Shor's discovery sparked a great deal of interest in the design of quantum algorithms and computers that endures today.

In addition to Shor's algorithm, there is a wealth of other interesting and important algorithms that have been developed for quantum computers. One of those algorithms will be described in detail in this project in order to better elucidate the study of quantum computing theory and quantum algorithm design. This algorithm we'll be explaining is a good model for our current understanding of quantum computation as many other quantum algorithms use similar techniques to achieve their results, whether they be algorithms to solve linear systems of equations [4], or quickly compute discrete logarithms. Shor, for example, credits one of these algorithms as the inspiration for his own [2].

The algorithm that will be explored in our project is Lov Grover's quantum database search [5]. Grover's algorithm searches for a specified entry in an unordered database, employing an important technique in quantum algorithm design known as amplitude amplification to achieve a polynomial speedup over the best classical algorithms. In fact, Grover's algorithm is optimal for any quantum algorithm for performing such a search [6]. Of course, searching for an unique element in an unordered set can be generalized to apply to a wide variety of problems in computer science, such as the problem of boolean satisfiability (SAT). Determining whether there exists a set of truth values that satisfy a given set of clauses is equivalent to searching for an element, the set of truth values, that satisfies a certain condition, the set of clauses, in an unordered search space, the set of all 2n possible truth assignments of n boolean variables. Although this algorithm does not provide an extreme increase in efficiency over its classical counterparts, the speedup is still certainly significant with large input.

Objectives

We propose to review and understand the concepts of quantum algorithms and how are they implemented. In this review we'll achieve following two goals mainly:

1. Understand the quantum computing and implementation of quantum algorithms.
2. Explanation of Lov Grover's quantum database search algorithm.

Under the first goal, we'll be exploring how Quantum computers employ the laws of quantum mechanics to provide a vastly different mechanism for computation than that available from classical machines. Fortunately for computer scientists interested in the field of quantum computing, a deep knowledge of quantum physics is not a prerequisite for understanding quantum algorithms, in the same way that one need not know how to build a processor in order to design classical algorithms. However, it is still important to be familiar with the basic concepts that differentiate quantum mechanical systems from classical ones in order to gain a better intuitive understanding of the mathematics of quantum computation, as well as of the algorithms themselves.

Under the second part of our goal we'll talk about how Grover's algorithm takes advantage of qubits(quantum bit) and implements performs a search over an unordered set items to find the unique element that satisfies some condition. While currently the best classical algorithm for a search over an unordered set takes O(N) time. But, Grover's algorithm outperforms with a quadratic speedup and requires only O(√N) time to perform search using quantum computer [6].

Schedule

The schedule for the whole project is as below:

Timeline	Tasks achieved
13 Nov - 18 Nov	Initial investigation and understanding basics of quantum physics
19 Nov - 25 Nov	Reading about Quantum algorithms and write-up
26 Nov - 02 Dec	Understanding Grover’s Algorithm and write-up
03 Nov - 09 Dec	Creating final project presentation

Above schedule will mostly be the benchmark for our project, although there might be few minor changes in schedule due to unplanned factors, such as hitting roadblock while researching, etc.

References

[1] R. P. Feynman, “Simulating Physics with Computers,”
International Journal of Theoretical Physics

[2] P. W. Shor, “Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer,”

[3] R. L. Rivest, A. Shamir et al., “A method for obtaining digital signatures and public-key cryptosystems,”

[4] A. Harrow, A. Hassidim et al., “Quantum Algorithm for Linear Systems of Equations,”
Physical Review Letters

[5] L. K. Grover, “A fast quantum mechanical algorithm for database search,” in
Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing

[6] C. Zalka, “Grover’s quantum searching algorithm is optimal,”
Physical Review A

[7] Emma Strubell, “An introduction to Quantum Algorithms”,
COS498 – Chawathe

[8] Grover’s Algorithm, “Wikipedia”, https://en.wikipedia.org/wiki/Grover's_algorithm

[9] Quantum Algorithms, “Algorithms by Dasgupta, Papadimitriou and Vazirani”,