The Complexity of Quantum Computation

Takashi Mihara
School of Information Science
Japan Advanced Institute of Science and Technology

January 16, 1997

Abstract

In this thesis, we show some results on the complexity and algorithms based on a quantum Turing machine, which is a new type of computing model proposed in 1980's.

In Chapter 1, we describe backgrounds and motivations of studying quantum computers. In 1985, Deutsch proposed a computing model involving a superposition of physical states, which is one of inherent properties of quantum physics, as a quantum Turing machine (QTM) and in 1993, Bernstein and Vazirani mathematically formalized the QTM. After that, some results have indicated that the QTM may be more powerful than ordinary computers.

In Chapter 2, we describe elementary definitions and notations. We define Turing machines (TMs) that are standard theoretical models of computing devices. A QTM is defined based on these models. Since the execution of the QTM is evolved by unitary matrices, it is also a model of reversible computation. Therefore, in this chapter, we also describe the definition of a reversible Turing machine that was proposed by Bennett.

In Chapter 3, we review several models of quantum computers. A quantum computer was firstly proposed as a QTM by Deutsch. His quantum computer, for the first time, involves inherent properties of quantum physics as the computational principles. Nowadays, many computer scientists study the complexity and algorithms based on his model. However, since there are other quantum computing models such as quantum circuits and quantum cellular automata, we also describe these models briefly. Finally, we summarize the realizabilities of quantum computers.

In Chapter 4, we define typical complexity classes based on TMs and complexity classes based on QTMs. Moreover, we also show the relationships between complexity classes.

In Chapter 5, we discuss methods to find the periods of functions efficiently. Some techniques for solving problems efficiently on QTMs have been proposed. Especially, the most well-known techniques, a quantum Fourier transform and a quantum iterating method, have been used. A *quantum Fourier transform* is a quantum version of discrete Fourier transforms and can efficiently obtain some properties of functions. By this technique, we show that the periods in some kinds of periodic functions, $f(x) = f(x + r)$ and $x = f^r(x)$ for a period r, can be found in polynomial time with bounded error probability on QTMs. Some of the functions proposed as pseudo-random generators are also included in these functions.

In Chapter 6, we discuss quantum search algorithms for a table search. A *quantum iterating method* is a method to increase the probability of accepting states by using an algorithm repeatedly. By this technique, we show that for an unsorted table T of n items and a query item q, there is a quantum search algorithm that finds a pair of indices (j, k) corresponding to two

successive items, $T[j]$ and $T[k]$, which satisfy that $T[j] \leq q \leq T[k]$, in expected time $O(n^{1/2})$ with bounded error probability. As a special case, this algorithm can find the minimum or the maximum value of T in expected time $O(n^{1/2})$ with bounded error probability. Moreover, we also show that QTMs can solve some problems in computational geometry more efficiently than ordinary computers.

In Chapter 7, we investigate the relationships between the computational complexity and quantum physics. Although NP-complete problems appear in many situations, nobody knows whether ordinary computers can efficiently solve these problems or not. On the other hand, the problem of measurement is one of the most interesting problems in physics and nobody can explain sufficiently what happens when we measure yet. Here, we propose the following two assumptions on measurement: (i) Assumption Π_1 : a superposition of physical states is preserved after measurements and all of the states in the superposition can be measured in time proportional to the number of the states in the superposition, and (ii) Assumption Π_2 : we can measure the existence of a specific physical state C in a given superposition with certainty in polynomial time if the state C exists in the superposition. Then, we show that there is a QTM that solves the satisfiability problem (SAT) in $O(2^{n/4})$ time under Assumption Π_1 and there is a QTM that solves SAT in $n^{O(1)}$ time under Assumption Π_2, where n is the length of an instance of SAT. SAT is a typical NP-complete problem.

In Chapter 8, we denote some concluding remarks and a future work.

Finally, in Appendix A, we summarize the fundamental parts of quantum physics needed to understand quantum computers.

Key Words: **quantum computation, quantum Turing machine, quantum complexity class, periodic function, pseudo-random generator, quantum search algorithm, NP-complete problem, satisfiability problem**