

---

## Preface

The twentieth century witnessed the birth of revolutionary ideas in the physical sciences. These ideas began to shake the traditional view of the universe dating back to the days of Newton, even to the days of Galileo. Albert Einstein is usually identified as the creator of the *relativity theory*, a theory that is used to model the behavior of the huge macrosystems of astronomy. Another new view of the physical world was supplied by *quantum physics*, which turned out to be successful in describing phenomena in the microworld, the behavior of particles of atomic size.

Even though the first ideas of automatic information processing are quite old, I feel justified in saying that the twentieth century also witnessed the birth of computer science. As a mathematician, by the term “computer science”, I mean the more theoretical parts of this vast research area, such as the theory of formal languages, automata theory, complexity theory, and algorithm design. I hope that readers who are used to a more flexible concept of “computer science” will forgive me. The idea of a computational device was crystallized into a mathematical form as a *Turing machine* by Alan Turing in the 1930s. Since then, the growth of computer science has been immense, but many problems in newer areas such as complexity theory are still waiting for a solution.

Since the very first electronic computers were built, computer technology has grown rapidly. An observation by Gordon Moore in 1965 laid the foundations for what became known as “Moore’s Law” – that computer processing power doubles every eighteen months. How far can this technical process go? How efficient can we make computers? In light of the present knowledge, it seems unfair even to attempt to give an answer to these questions, but some estimate can be given. By naively extrapolating Moore’s law to the future, we learn that sooner or later, each bit of information should be encoded by a physical system of subatomic size! Several decades ago such an idea would have seemed somewhat absurd, but it does not seem so anymore. In fact, a system of seven bits encoded subatomically has been already implemented [37]. These small systems can no longer be described by classical physics, but rather quantum physical effects must be taken into consideration.

When thinking again about the formalization of a computer as a Turing machine, rewriting system, or some other classical model of computation, one

realizes that the concept of *information* is usually based on strings over a finite alphabet. This strongly reflects the idea of classical physics in the following sense: each member of a string can be represented by a physical system (storing the members in the memory of an electronic computer, writing them on sand, etc.) that can be in a certain *state*; i.e., contain a character of the alphabet. Moreover, we should be able to identify different states reliably. That is, we should be able to make an *observation* in such a way that we become convinced that the system under observation represents a certain character.

In this book, we typically identify the alphabet and the distinguishable states of a physical system that represent the information. These identifiable states are called *basis states*. In quantum physical microsystems, there are also basis states that can be identified and, therefore, we could use such microsystems to represent information. But, unlike the systems of classical physics, these microsystems are also able to exist in a *superposition* of basis states, which, informally speaking, means that the state of such a system can also be a combination of basis states. We will call the information represented by such microsystems *quantum information*. One may argue that in classical physics it is also possible to speak about combinations of basis states: we can prepare a *mixed* state which is essentially a probability distribution of the basis states. But there is a difference between the superpositions of quantum physics and the probability distributions of classical physics: due to the *interference effects*, the superpositions cannot be interpreted as mixtures (probability distributions) of the basis states.

Richard Feynman [30] pointed out in 1982 that it appears to be extremely difficult by using an ordinary computer to simulate efficiently how a quantum physical system evolves in time. He also demonstrated that, if we had a computer that runs according to the laws of quantum physics, then this simulation could be made efficiently. Thus, he actually suggested that a *quantum computer* could be essentially more efficient than any traditional one.

Therefore, it is an interesting challenge to study *quantum computation*, the theory of computation in which traditional information is replaced by its quantum physical counterpart. Are quantum computers more powerful than traditional ones? If so, what are the problems that can be solved more efficiently by using a quantum computer? These questions are still waiting for answers.

The purpose of this book is to provide a good introduction to quantum computation for beginners, as well as a clear presentation of the most important presently known results for more advanced readers. The latter purpose also includes providing a bridge (from a mathematician's point of view) between quantum mechanics and the theory of computation: it is not only my personal experience that the language used in research articles on these topics is completely different.

Chapter 1, especially Section 1.4, includes the most basic knowledge for the presentation of quantum systems relevant to quantum computation.

Chapter 2 is divided as follows: Turing machines, as well as their probabilistic counterparts, are introduced in Section 2.1 as traditional models of computation. For a reader interested in the research on quantum computation but having little knowledge of the theory of computation, this section is designed to also include the basic definitions of complexity theory. In Section 2.2, the knowledge on quantum systems is deepened and the quantum counterparts of the computational models are presented. Sections 2.1 and 2.2 are intended for a reader who has a solid background in quantum mechanics, but little previous knowledge on classical computation theory. A reader who is well aware of the theory of computation may skip Section 2.1 as well: for such a reader the knowledge in Sections 2.2 and 2.3 (excluding the first subsection) is sufficient to follow this book. In Section 2.3, we represent Boolean and quantum circuits (as an extension of the concept of reversible circuits) as models of computation. Because of their descriptiveness, circuits are used throughout this book to present quantum algorithms.

Chapter 3 is devoted to a complete representation of Shor's famous factorization algorithm. The instructions in Chapter 3 will help the reader to choose which sections may, according to reader's background, be skipped. Chapter 4 is closely connected to Chapter 3, and can be seen as a representation of a structural but not straightforward extension of Shor's algorithm.

Chapter 5 is written to introduce Grover's method for obtaining a quadratic speedup in quantum computation (with respect to classical computation) in a very basic form, whereas in Chapter 6, we represent a method for obtaining lower bounds for quantum computation in a restricted quantum circuit model.

Chapters 7 and 8 are appendices intended for a beginner, but Chapter 7 is also suitable for a reader who has a strong background in computer science and is interested in quantum computation. Chapter 8 is composed of various different topics in mathematics, since it has already turned out that, in the area of quantum computation, many mathematical disciplines, seemingly separate from each other, are useful. Moreover, my personal experience is that a basic education on computer science and physics very seldom covers all the areas in Chapter 8.

This book is concentrated mainly on quantum algorithms but other interesting topics, such as quantum information theory, quantum communication, quantum error-correcting, and quantum cryptography, are not covered. Therefore, for additional reading, we can warmly recommend [32] by Josef Gruska. Book [32] also contains a large number of references to works on quantum computing. A reader who is more oriented to physics may also see [70] and [71] by C. P. Williams and S. H. Clearwater. It may also be useful to follow the Los Alamos preprint archive at <http://xxx.lanl.gov/archive/quant-ph> to learn about the new developments in quantum computing. The Los Alamos

preprint archive contains a large number of articles on quantum computing since 1994, and includes many articles referred to in this book.

**Acknowledgements.** My warmest thanks go to Professors Grzegorz Rozenberg and Arto Salomaa for encouraging me to write this book, and to Professor Juhani Karhumäki and Turku Centre for Computer Science for providing excellent working conditions during the writing period. This work has been supported by the Academy of Finland under grants 14047 and 44087. I am also indebted to Docent P. J. Lahti, V. Halava, and M. Rönkä for their careful revision work on parts of this book. Thanks also go to Dr. Hans Wössner for a fruitful cooperation.

Turku, Finland, February 2001

*Mika Hirvensalo*

# Contents

<b>1. Introduction</b> .....	1
1.1 A Brief History of Quantum Computation .....	1
1.2 Classical Physics .....	2
1.3 Probabilistic Systems .....	4
1.4 Quantum Mechanics .....	7
<b>2. Devices for Computation</b> .....	13
2.1 Classical Computational Models .....	13
2.1.1 Turing Machines .....	13
2.1.2 Probabilistic Turing Machines .....	16
2.1.3 Multitape Turing Machines .....	20
2.2 Quantum Information .....	21
2.2.1 Quantum Bits .....	22
2.2.2 Quantum Registers .....	24
2.2.3 More on Quantum Information .....	27
2.2.4 Quantum Turing Machines .....	30
2.3 Circuits .....	34
2.3.1 Boolean Circuits .....	34
2.3.2 Reversible Circuits .....	36
2.3.3 Quantum Circuits .....	38
<b>3. Fast Factorization</b> .....	41
3.1 Quantum Fourier Transform .....	41
3.1.1 General Framework .....	41
3.1.2 Hadamard-Walsh Transform .....	43
3.1.3 Quantum Fourier Transform in $\mathbb{Z}_n$ .....	44
3.1.4 Complexity Remarks .....	49
3.2 Shor's Algorithm for Factoring Numbers .....	50
3.2.1 From Periods to Factoring .....	50
3.2.2 Orders of the Elements in $\mathbb{Z}_n$ .....	52
3.2.3 Finding the Period .....	54
3.3 The Correctness Probability .....	56
3.3.1 The Easy Case .....	56
3.3.2 The General Case .....	57

3.3.3	The Complexity of Shor’s Factorization Algorithm . . . .	61
3.4	Excercises . . . . .	62
<b>4.</b>	<b>Finding the Hidden Subgroup</b> . . . . .	<b>63</b>
4.1	Generalized Simon’s Algorithm . . . . .	64
4.1.1	Preliminaries . . . . .	64
4.1.2	The Algorithms . . . . .	65
4.2	Examples . . . . .	69
4.2.1	Finding the Order . . . . .	69
4.2.2	Discrete Logarithm . . . . .	69
4.2.3	Simon’s Original Problem . . . . .	70
4.3	Excercises . . . . .	70
<b>5.</b>	<b>Grover’s Search Algorithm</b> . . . . .	<b>73</b>
5.1	Search Problems . . . . .	73
5.1.1	Satisfiability Problem . . . . .	73
5.1.2	Probabilistic Search . . . . .	74
5.1.3	Quantum Search with One Query . . . . .	76
5.2	Grover’s Amplification Method . . . . .	79
5.2.1	Quantum Operators for Grover’s Search Algorithm . . . . .	79
5.2.2	Amplitude Amplification . . . . .	80
5.2.3	Analysis of Amplification Method . . . . .	84
5.3	Utilizing Grover’s Search Method . . . . .	87
5.3.1	Searching with Unknown Number of Solutions . . . . .	87
<b>6.</b>	<b>Complexity Lower Bounds for Quantum Circuits</b> . . . . .	<b>91</b>
6.1	General Idea . . . . .	91
6.2	Polynomial Representations . . . . .	92
6.2.1	Preliminaries . . . . .	92
6.2.2	Bounds for the Representation Degrees . . . . .	96
6.3	Quantum Circuit Lower Bound . . . . .	98
6.3.1	General Lower Bound . . . . .	98
6.3.2	Some Examples . . . . .	101
<b>7.</b>	<b>Appendix A: Quantum Physics</b> . . . . .	<b>103</b>
7.1	A Brief History of Quantum Theory . . . . .	103
7.2	Mathematical Framework for Quantum Theory . . . . .	105
7.2.1	Hilbert Spaces . . . . .	107
7.2.2	Operators . . . . .	108
7.2.3	Spectral Representation of Self-adjoint Operators . . . . .	109
7.2.4	Spectral Representation of Unitary Operators . . . . .	111
7.3	Quantum States as Hilbert Space Vectors . . . . .	115
7.3.1	Quantum Time Evolution . . . . .	116
7.3.2	Observables . . . . .	118
7.3.3	The Uncertainty Principles . . . . .	121

7.4	Quantum States as Operators .....	125
7.4.1	Density Matrices .....	126
7.4.2	Subsystem States .....	130
7.4.3	More on Time Evolution .....	135
7.4.4	Representation Theorems .....	136
7.5	Exercises .....	144
<b>8.</b>	<b>Appendix B: Mathematical Background .....</b>	<b>145</b>
8.1	Group Theory .....	145
8.1.1	Preliminaries .....	145
8.1.2	Subgroups, Cosets .....	146
8.1.3	Factor Groups .....	147
8.1.4	Group $\mathbb{Z}_n^*$ .....	149
8.1.5	Group Morphisms .....	151
8.1.6	Direct Product .....	153
8.2	Fourier Transforms .....	154
8.2.1	Characters of Abelian Groups .....	154
8.2.2	Orthogonality of the Characters .....	156
8.2.3	Discrete Fourier Transform .....	158
8.2.4	The Inverse Fourier Transform .....	160
8.2.5	Fourier Transform and Periodicity .....	161
8.3	Linear Algebra .....	161
8.3.1	Preliminaries .....	161
8.3.2	Inner Product .....	164
8.4	Number Theory .....	167
8.4.1	Euclid's Algorithm .....	167
8.4.2	Continued Fractions .....	168
8.5	Shannon Entropy and Information .....	175
8.5.1	Entropy .....	175
8.5.2	Information .....	179
8.6	Exercises .....	181
	<b>References .....</b>	<b>182</b>
	<b>Index .....</b>	<b>187</b>