PREFACE

Come forth into the light of things.
Let Nature be your teacher.

W. Wordsworth (1770–1850)

A simplified view of the history of computing shows that computing was thought of mainly as mental processes in the 19th century; it is thought of mainly as machine processes in the 20th century, and it will be thought of mainly as Nature processes in the 21st century.

We cannot tell, of course, how much of this vision will be true. Currently, we see vigorous, interesting and, we expect, very important attempts to go much deeper than before into Nature in order to discover its potential for information processing. In this way we also hope to deepen our understanding of Nature. Perhaps the two areas of greatest potential are quantum computing and molecular computing.

The amount of theoretical research and experimental developments in quantum computing grows rapidly. At the same time, interest grows within the science and technology community, especially in physics and theoretical computing, and this interest in turn gives rise to a need for a systematic presentation and summary of the main concepts, methods and achievements through textbooks and courses. This book is addressed to this need.

There has long been a tradition in computing to look into the natural world for inspiration. There have been many attempts to understand, mimic and harness information processing tools and power of the brain. Already finite automata have been developed as an abstraction of neurons activities. Neural networks represent another model inspired by the brain. Information processing of genetic mechanisms is a further source of inspiration. All these attempts are of interest and importance. However, the current attempts in molecular and quantum computing seem to go even deeper into Nature in the quest of exploring its information processing potential.

Our world is quantum mechanical. It is therefore natural, necessary, interesting and important to explore the foundations and potentials of quantum information processing. At the same time, we must explore the technologies and methods that allow the experimental realization of quantum information processing systems.

Quantum computing is a very new, fascinating, promising and puzzling scientific adventure in which we witness a merging and mutual influence of two of the most significant developments in science and technology of the 20th century—quantum mechanics and computing. An adventure that may lead not only to **the** computer revolution, but also to a new scientific and technological basis for information processing in the 21st century.

> *It has been known, but not realized enough, from the birth of modern quantum mechanics theory that the most basic processes of Nature are actually quantum information processing processes and that amount of information processing going on everywhere around us in a tiny portion of matter and time is incomparably larger than all information processing classical technology has ever provided. In addition, it has not been realized, till the birth of modern quantum information processing research, that information processing capabilities of Nature cannot be matched by classical information processing tools, and due to severe limitations on retrieval of information from quantum to classical world, it has not been clear at all whether and how we can harness enormous information processing power of Nature for classical information processing.*

At the same time, as it is often the case with the very fundamental and powerful theories and ideas, the very basic concepts of quantum computing are surprisingly simple and elegant even though they seem to deal with mysterious and puzzling phenomena. Moreover, the technical—mathematical—tools needed to present an introduction to quantum computing are mostly those that are included in basic science education. The book demonstrates and utilizes this fact in a way that is readable and understandable by the broad science and technology community.

It is hard to foresee exactly where the research and development in quantum computing will take us. However, we can safely say that something important will come out and that quantum computing is a challenge not only for informatics and physics—theoretical and also experimental — but also for science, technology and society in general.

For informatics as a science, quantum computing may bring the most radical change in its main research aims, scope and paradigms. Indeed, so far informatics has been developed, largely, with the global aims of serving current and foreseeable information processing technology. Quantum computing (with molecular computing) is perhaps the first significant challenge, chance and necessity for informatics to free itself from this short-term role of the servant of technology and to start to concentrate more on its most basic long-term aims: to study the laws and limitations of the information processing world, to contribute to the development of new global theories and to deepen our understanding of various worlds: for example physical, biological, and chemical.

For informatics as a technology, the development of quantum information processing technologies can make a revolutionary contribution to the potential and security of information processing and communication systems.

For theoretical physics, quantum computing can be seen as a new challenge and also as an important new source of aims, stimuli, scientific methods and paradigms for dealing with one of the most basic problems of current science (physics). Namely, how to deepen and extend one of the most basic, powerful and fascinating theory in physics—quantum theory. It also brings an opportunity to understand more the role of information as an important resource and fundamental concept in physics and for the understanding of the physical world.

For experimental physics, especially for atomic physics and quantum optics, large needs of quantum computing to store, communicate and process quantum information faithfully bring radically new challenges of astounding complexity and importance.

The merging of insights, methodologies and research paradigms from quantum physics and theoretical computing has been vital for the development of quantum computing and it is expected to be even more so in the future. Historically the first ideas of quantum computing came from people in physics with knowledge of research paradigms, concepts and methods of theoretical computing. However, some key results, and actually the main "apt killers", came from the people in computing making use of only very basic concepts of quantum physics. The results obtained so far in quantum computing demonstrate that currently even the people in theoretical computing or physics with rudimentary knowledge of other areas still have a chance to make significant contributions to the field. However, in the future, one could expect a growing need for a thorough knowledge of both of the areas behind quantum computing.

In this book, very basic concepts, models, methods and results of quantum computing are presented in a systematic way. Emphasis is much more on computational aspects, models, methods and problems than on the details of the underlying physics or on technological features which are of (enormous) importance for implementation of quantum information processing systems. The book is therefore primarily oriented towards readers with a computing/mathematics background, but should also be of interest, use, and importance to those with a background in physics and other areas of science and technology. The book assumes very little knowledge of physics and presents quantum computing concepts, models, and methods in a systematic and quite abstract way. The very basic concepts from quantum physics and from its mathematical model—Hilbert spaces—are dealt with in the introductory chapter and also in the Appendix.

The book consists of eight chapters, an extensive Appendix, a list of literature and a detailed index.

The introductory chapter, *Fundamentals*, presents, quite informally, the basic ideas and concepts of quantum computing, including the description of some basic experiments and principles of quantum mechanics and also of elements of Hilbert spaces. The chapter starts with a thorough discussion of why to consider quantum computing and provides an introduction of basic ideas of quantum computing via a comparison of quantum and randomized computing on the level of Turing machines. It also deals in some detail with the concept of reversibility in classical computing.

The second chapter, *Elements*, presents a very detailed treatment of such basic concepts of quantum computing as quantum states, bits, registers, gates, networks and evolutions. Special attention is given to the quantum entanglement, the key inherently quantum resource of quantum information processing. Quantum registers, evolution of their states and measurements, are also discussed and demonstrated. A variety of examples of quantum gates and networks is provided and the universality of quantum gates is dealt with in detail.

The third chapter, *Algorithms*, presents the basic results concerning the design of efficient quantum algorithms. A variety of important quantum algorithms is presented, starting with pioneering algorithms for simple promise problems and including Shor's integer factorization and discrete logarithm computation algorithms, Grover's search algorithm and algorithms for related search and counting problems. A general framework to design efficient quantum algorithms is also presented and illustrated. Finally, a framework is introduced to show lower bounds for quantum algorithms and limitations of quantum computers to speed-up some computations.

The fourth chapter, *Automata*, presents and analyses quantum versions of several basic models of computing: finite automata, Turing machines and cellular automata. These models bring new insights into quantum computing and at the same time a variety of new specific automata-theoretic problems.

In the fifth chapter, *Complexity*, several key problems concerning complexity of quantum computation and communication are dealt with: design of efficient universal quantum Turing machines, basic quantum time and space computational complexity classes and their mutual relations as well as their relation to classical computational complexity classes, and quantum communication complexity. Finally, computational power of nonlinear quantum mechanics is shortly discussed.

In the sixth chapter, *Cryptography*, at first several quantum key generation protocols are presented and their security is analysed. In addition, several quantum protocols for such fundamental problems as bit commitment and oblivious transfer, or for two-party communication are presented. Very important, but tricky, complex and deep questions concerning security of cryptographic protocols are dealt with in detail. This includes a proof of unconditional security for quantum key generation as well as the proof of impossibility of such security for quantum bit commitment protocols. Finally, quantum teleportation, superdense coding and some of their applications are described. These areas of quantum information processing are already of more than theoretical interest. Especially in quantum cryptography, experimental progress has been formidable and one has good reason to expect significant applications in the near future.

The seventh chapter, *Processors*, starts with the presentation of very early ideas on how to design quantum processors. It then analyses several key problems one encounters in attempts to build quantum processors. These include: decoherence and inaccuracies and several ways how to cope with these problems: quantum stabilization and error-correction methods for making storage and communication of quantum information feasible; quantum fault tolerant techniques for making (long) processing of quantum information feasible.

Finally, several basic problems are pointed out which a technology has to be able to deal with well in order to create a potential base for the design of (experimental) quantum processors.

In the last chapter, *Information*, several quantum information theory and communication problems are dealt with. These include the development of the quantum counterparts of the basic concepts of the classical information theory, quantum data compression, communication through noiseless and noisy channels and capacities of quantum channels. Entanglement creation, manipulation, concentration, distillation and quantification concepts, protocols and results are also presented and analysed.

The *Appendix* has five parts: In the first part, several basic problems concerning quantum physics are briefly and informally introduced and discussed. In the second part, there is a more detailed presentation of the basic concepts and results of Hilbert space theory related to quantum computing. In the third part a short survey of the basic concepts and main results of computational complexity theory is provided for those less familiar with the topic. In the fourth part additional exercises are listed. Finally, in the last part, additional historical and bibliographical references are provided.

The idea of writing this book came up quite naturally with my attempt to write an additional, on web only, chapter on quantum computing, as a supplementary chapter 12, to my book *Foundations of Computing*, 1997. The writing went well and manuscript soon got much too big just for a chapter. In addition, I have realized the attractiveness of the subject for computing people and its maturity which already allows, in spite of the very short history of the field, a systematic presentation of its main concepts and results of clearly lasting importance.

Naturally, the book is only an introduction to quantum computing, written from one perspective, that of computing. Several subjects that are dealt with only briefly in this book, such as design of quantum algorithms, quantum cryptography, quantum information, quantum error-correcting codes, quantum fault tolerant computing and quantum entanglement would already merit monographs. In addition, many subjects requiring more expertise in quantum physics, and at the same time not central for an introduction to the main problems of current quantum computing, have been covered only briefly, or not at all.

Referencing. A large effort has been made so that results and ideas presented are properly credited and referenced. This has been a hard task because the field develops very fast. This is therefore to apologize for all omissions, imperfections or even misclaims and to ask those feeling that an addition or correction should be done along these lines to let me know and I will try to do that on the book web pages.

Acknowledgements. I have started to work on this book while visiting University Paris VI, in 1997, and, especially, University of Nice, Laboratoire d'Informatique Signaux et Systèmes at Sophia-Antipolis, during long stays in 1997 and 1998, within the PAST program. Excellent conditions provided by these universities and help by many people there, especially by Irène Guessarian and Bruno Martin are much appreciated.

I have also to acknowledge excellent conditions, full understanding and support provided by Faculty of Informatics, Masaryk University, Brno and also support of GAČR, Grant 201/98/0369 and of the Slovak Literary Agency.

This is also to thank Vladimír Bužek, Patrick Cegielski, Vladimír Černý, Christop Dürr, Ru̱siņš Freivalds, Mika Hirvensalo, Juraj Hromkovič, Bernd Kirsig, Manfred Kudlek, Bruno Martin, Michele Mosca, Jozef Nagy, Masanao Ozawa, Pavol Petrovič, Jiří Rosický, Martin Stanek, Mark-Oliver Stehr, John Watrous and Thomas Worsch for reading, correcting and commenting onearlier drafts of this book or its parts. Special thanks go to V. Bužek for discussions and also advice and help. Support of the Roland Volmar team is also acknowledged.

Expertise and helpfulness of our TeX and LaTeX expert Petr Sojka was most useful and is much appreciated. Appreciated also is help with figures, index and manuscript checking by Robert Batůšek, Petr Tobola and especially by Petr Macháček.

Finally, very smooth cooperation with David Hatter from McGraw-Hill and his continuous, but very enjoyable and constructive, wisdom, pressure, understanding and help, has been very much appreciated during the whole process of the manuscript preparation. Cooperation with Steve Gardiner and his production staff is also to appreciated.

Using the book as the textbook. The following is a possible structure of a one semester course: (1) Introduction (1.1–1.3, 1.7); (2) Hilbert spaces basics (1.4, 9.2); (3) Quantum principles (1.5–1.6 + Appendix 9.1) or Computational complexity (Appendix 9.3); (4) Quantum bits, registers, gates and networks (2.1–2.3); (5) Basic quantum algorithms (3.1); (6) Shor's algorithms I (3.2); (7) Search algorithms (3.3); (8) Quantum algorithms design methodologies and limitations (3.4 and 3.5); (9) Quantum finite automata and Turing machines (4.1 and 4.2); (10) Quantum key generation (6.1 and 6.2); (11) Quantum cryptographic protocols and teleportation (6.3 and 6.4); (12) Quantum error correction codes (7.2–7.4); (13) Quantum fault-tolerant methods (7.5); (14) Quantum processors (7.1 and 7.6); (15) Quantum information theory (8.1–8.2); (16) Quantum entanglement theory (8.3–8.4).

Additional subjects: quantum computational complexity (5.1–5.4), quantum cellular automata (4.3).

29 April 1999 Jozef Gruska