Texts in Computer Science

More information about this series at http://www.springer.com/series/3191

Sergei Kurgalin • Sergei Borzunov

Concise Guide to Quantum Computing

Algorithms, Exercises, and Implementations

Springer

Sergei Kurgalin
Digital Technologies
Voronezh State University
Voronezh, Russia

Sergei Borzunov
Digital Technologies
Voronezh State University
Voronezh, Russia

ISSN 1868-0941 ISSN 1868-095X (electronic)
Texts in Computer Science
ISBN 978-3-030-65051-3 ISBN 978-3-030-65052-0 (eBook)
https://doi.org/10.1007/978-3-030-65052-0

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

The role of Computing Science in modern society can hardly be overestimated. The rapid development of physics, chemistry, biology, medicine as well as achievements in economics is based on the developing possibility of solving resource-intensive problems on powerful computing systems. Nevertheless, the exponential complexity of many practically significant problems leads to considerable difficulties even while using a supercomputer.

The approach to computing, fundamentally different from the widely known and available—classical—computing, provides quantum theory. Quantum-mechanical methods of solving problems in some cases provide exponential speedup in comparison with traditional algorithms. The idea of accelerating computational processes by using quantum systems began to develop in many academic and industrial world centers.

Training specialists in the field of computing science, meeting the requirements of time, leads to the need to pay special attention to the basics of quantum computing. In our opinion, there are not enough books describing quantum computing on the methodical level available for future programmers in the educational literature at the present time. The known textbooks on quantum theory in the majority do not contain the data on quantum algorithms and, therefore, are not completely focused on the training of experts in the field of information technology. In this workbook, we made an attempt to fill this gap.

The book was developed over several years using the experience of teaching the quantum theory course at Computer Science Faculty of Voronezh State University. Its content corresponds to Federal State Educational Standards in the areas of Bachelor's Degree "Information Systems and Technologies", "Software Engineering", "Information Security", "Mathematics and Computer Science", Specialist's degree in "Computer Security", and Master's degree in "Information Systems and Technologies".

This workbook is intended for laboratory, practical classes and for independent study. It contains basic theoretical concepts and methods for solving basic types of problems, as well as a large number of explanatory examples. It gives an idea of the quantum computing model, basic operations with qubits and universal elements of quantum schemes, introduces definitions of entangled states, and analyzes the Einstein–Podolsky–Rosen experiment. Much attention is paid to examples of the most important quantum algorithms—the algorithms of phase evaluation and the Fourier quantum transformation.

The workbook offers a large number of problems and exercises of a wide range of complexity for independent solution. All problems, except the simplest ones, are equipped with answers, hints, or solutions. The most difficult problems are highlighted with the character "asterisk" (*), placed before their number. The end of an example in the text is indicated by the symbol □. The book includes a sufficient number of illustrations and diagrams to help visualize the objects being studied and the connections between them. Review questions on theoretical material are formulated to test knowledge.

There are two appendices to the textbook. In *Appendix A*, the system of postulates of quantum theory is formulated. That will help students to fix and systematize knowledge and skills in solving quantum-mechanical problems. *Appendix B* contains a summary of information on Hermitian and unitary transformations, which are known to play a major role in quantum theory and its applications.

Mastering the material requires knowledge of the basics of linear algebra and elementary probability theory. The knowledge of quantum mechanics basics is not strictly necessary.

The authors sought to make the presentation of the material available without losing the rigor of the wording of the statements. Theorems and properties are accompanied by proofs or references to scientific literature.

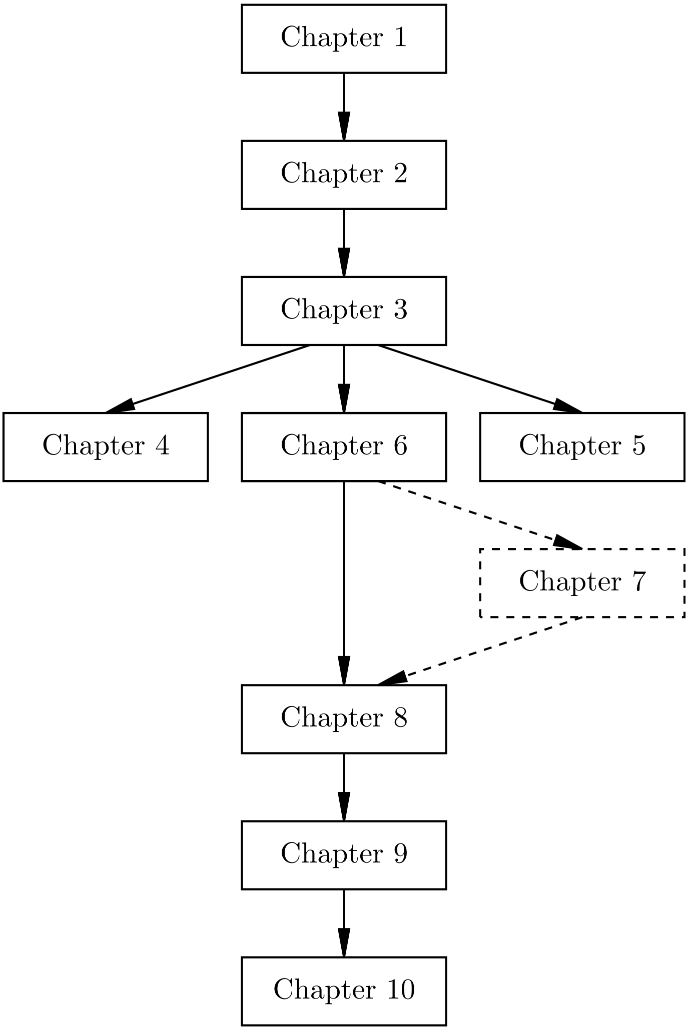
A detailed reference and bibliography aids is one of the distinguishing features of this manual. *References* contains links to educational literature, where the issues discussed in the text of this workbook are covered in detail. In addition, the reference list contains references to fundamental original works in the field of quantum computing. It is hoped that the reading of such articles will allow students to get the skill of working with a steadily increasing flow of information about modern researches in this field.

The workbook is provided with *Name* and *Subject Indices*.

Below you can see the scheme of the chapter information dependence in the form of an oriented graph reflecting the preferable order of covering the academic material. For instance, after having studied Chaps. 1–3, you can move to one of the three Chaps. 4, 5 or 6, whose contents are relatively independent. The dashed border marks Chap. 7, which will be suitable for readers who want to reach a high level of the subject knowledge; this section contains more difficult academic material. This way, after studying Chap. 6, you can either come to Chap. 8, or, for better mastery, study the material of Chap. 7 more thoroughly for better digestion, and only then switch to Chap. 8.

Voronezh, Russia
July 2020

Sergei Kurgalin
Sergei Borzunov



The chapter dependency chart

Acknowledgments

The authors would like to express their grateful acknowledgment to their colleagues Valeria Kaverina, Alexander Klinskikh, Alexey Kornev, Sergei Kurgansky, Peter Meleshenko, Mikhail Semenov, and Sergei Zapryagaev for useful discussions, advice, and critical comments.

We would like to thank Senior Editor Wayne Wheeler from Springer. Editorial Director Aliaksandr Birukou provided continuous and comprehensive support at all stages.

Probably, there are inevitable errors and inaccuracies in the book, all of which remain on the authors' conscience.

Sergei Kurgalin expresses special gratitude to Olga Kurgalina, Alexander Shirokov, and Veronica Shirokova for their constant support during the work on the book.

July 2020

Sergei Kurgalin
Sergei Borzunov

Contents

Notation

$\vert\psi\rangle$	Quantum state, ket vector
$\langle\psi\vert$	Bra vector
$\vert 0\rangle$, $\vert 1\rangle$	Basis quantum states of the qubit
$\vert\psi_1\rangle \otimes \vert\psi_2\rangle$ or $\vert\psi_1\rangle\vert\psi_2\rangle$	Tensor product
$A = (a_{ij})$	Matrix, formed by elements a_{ij}
A^T	Transposed matrix
$A^\dagger$	Hermitian conjugate matrix
M_U	Matrix of a unitary transformation U
δ_{ij}	Kronecker delta
σ_1, σ_2, σ_3	Pauli matrices
α_1, α_2, α_3, β	Dirac matrices
$\lambda_1, \lambda_2, \ldots, \lambda_8$	Gell-Mann matrices
$\{a_1, a_2, \ldots, a_n\}$	The set consisting of the elements $a_1, a_2, \ldots, a_n$
$\mathbb{N} = \{1, 2, 3, \ldots\}$	The set of natural numbers
$\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$	The set of integers
$\mathbb{R} = (-\infty, \infty)$	The set of real numbers
$\mathbb{C} = \mathbb{R} \times \mathbb{R}$	The set of complex numbers
$\mathbb{B} = \{0, 1\}$	Two-element set
$\mathbb{H}$	Hilbert space
$A \Rightarrow B$	The logical implication
$A \Leftrightarrow B$	The logical equivalence
$\forall x(P(x))$	For all x, the statement $P(x)$ is true
$\exists x(P(x))$	There exists such x, that the statement $P(x)$ is true
$[a, b]$	Closed interval $\{x : a \leqslant x \leqslant b\}$
(a, b)	Open interval $\{x : a < x < b\}$
$\mathrm{i} = \sqrt{-1}$	The imaginary unit
z^*	Conjugate of a complex number z
$\sum_{i=1}^{n} a_i$	Sum $a_1 + a_2 + \ldots + a_n$
$\prod_{i=1}^{n} a_i$	Product $a_1 a_2 \ldots a_n$
I	Identity matrix
O	Zero matrix
$[A, B]$	Commutator of matrices A and B

$\{A, B\}$	Anticommutator of matrices A and B
$(a_1, a_2, \ldots, a_n)$	Vector, i.e. an element of the set A^n
$\lfloor x \rfloor$	Floor function of x, that is the greatest integer less or equal to the real x
$x_1 \wedge x_2$	The conjunction of Boolean values x_1 and x_2
$x_1 \vee x_2$	The disjunction of Boolean values x_1 and x_2
$x_1 \rightarrow x_2$	The implication, x_1 implies x_2
$x_1 \leftrightarrow x_2$	The equivalence of x_1 and x_2
$x_1 \oplus x_2$	Addition modulo 2
$x_1 \mid x_2$	Sheffer stroke
$x_1 \downarrow x_2$	Peirce's arrow
$O(g(n))$	The class of functions growing not faster than $g(n)$
$\Omega(g(n))$	The class of functions growing at least as fast as $g(n)$
$\Theta(g(n))$	The class of functions growing of the same order as $g(n)$

Notation of main quantum gates see on pages 13 and 30