# SpringerBriefs in Computer Science

**Series editors**

Stan Zdonik, Brown University, Providence, RI, USA
Shashi Shekhar, University of Minnesota, Minneapolis, MN, USA
Xindong Wu, University of Vermont, Burlington, VT, USA
Lakhmi C. Jain, University of South Australia, Adelaide, SA, Australia
David Padua, University of Illinois Urbana-Champaign, Urbana, IL, USA
Xuemin Sherman Shen, University of Waterloo, Waterloo, ON, Canada
Borko Furht, Florida Atlantic University, Boca Raton, FL, USA
V. S. Subrahmanian, Department of Computer Science, University of Maryland, College Park, MD, USA
Martial Hebert, Carnegie Mellon University, Pittsburgh, PA, USA
Katsushi Ikeuchi, Meguro-ku, University of Tokyo, Tokyo, Japan
Bruno Siciliano, Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione, Università di Napoli Federico II, Napoli, Italy
Sushil Jajodia, George Mason University, Fairfax, VA, USA
Newton Lee, Institute for Education Research and Scholarships, Los Angeles, CA, USA

SpringerBriefs present concise summaries of cutting-edge research and practical applications across a wide spectrum of fields. Featuring compact volumes of 50 to 125 pages, the series covers a range of content from professional to academic. Typical topics might include:

- A timely report of state-of-the art analytical techniques
- A bridge between new research results, as published in journal articles, and a contextual literature review
- A snapshot of a hot or emerging topic
- An in-depth case study or clinical example
- A presentation of core concepts that students must understand in order to make independent contributions

Briefs allow authors to present their ideas and readers to absorb them with minimal time investment. Briefs will be published as part of Springer's eBook collection, with millions of users worldwide. In addition, Briefs will be available for individual print and electronic purchase. Briefs are characterized by fast, global electronic dissemination, standard publishing contracts, easy-to-use manuscript preparation and formatting guidelines, and expedited production schedules. We aim for publication 8–12 weeks after acceptance. Both solicited and unsolicited manuscripts are considered for publication in this series.

More information about this series at http://www.springer.com/series/10028

Franklin de Lima Marquezino • Renato Portugal
Carlile Lavor

# A Primer on Quantum Computing

Springer

Franklin de Lima Marquezino
Federal University of Rio de Janeiro
Rio de Janeiro
Rio de Janeiro, Brazil

Renato Portugal
National Lab of Scientific Computing
Petrópolis
Rio de Janeiro, Brazil

Carlile Lavor
Department of Applied Mathematics
(IMECC-UNICAMP)
University of Campinas
Campinas
São Paulo, Brazil

ISSN 2191-5768 ISSN 2191-5776 (electronic)
SpringerBriefs in Computer Science
ISBN 978-3-030-19065-1 ISBN 978-3-030-19066-8 (eBook)
https://doi.org/10.1007/978-3-030-19066-8

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2019
This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

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

# Preface

Quantum computation is an exciting field which is attracting increasing attention unremittingly since the early 1980s. This field rests on the shoulder of a giant because classical computation achieved amazing developments in the twentieth century. It is exciting because quantum computation is a paradigm change. The basic information unit—the qubit—behaves quite differently from the bit, which is either zero or one exclusively. The qubit admits the coexistence of zero and one. It is not possible to visualize this behavior directly; in fact, mathematics is the key that has unlocked the quantum behavior and allowed physicists to develop quantum mechanics, which predicts experimental results that have been successfully tested in labs. A paradigm change means that a new building must be made with different foundations.

In the last years, we have learned that companies such as IBM, Google, and others are building quantum computers with more and more qubits. IBM has made available 5- and 14-qubit quantum computers for any user with a composer that is very easy to use—a mouse click holds a quantum gate, then you drag and drop. After playing with the mouse, you hit the run button, and, *voilà*, the magic happens. The first part of the magic comes from classical computation and its graphical interface; the last part comes from the *superconducting transmon qubits* working under temperature as low as one-third of deep space, a pinnacle of success combining cutting-edge technology and centuries of scientific development.

To date, the so-called quantum supremacy has not been achieved. Meanwhile, classical computers continue to speed up and, nowadays, are possible to simulate the behavior of 50 qubits approximately in supercomputers. Quantum computers with more than 50 qubits are candidates to achieve the supremacy. The problem is to maintain the coexistence of zeros and ones for long enough, let us say, seconds. IBM's devices are working up to 100 ms. It is a huge technological challenge to scale up the quantum behavior to macroscopic sizes that humans can see and time spans that humans can take a breath.

Of course, we can always say that *the time is now*. Yes, we confess we believe that the time is now. Feynman said in 1982 that quantum computing is an interesting research problem, and it still is. This motivates us to finish this project which we started over a decade and a half ago. We hope you enjoy it.

Petrópolis, Brazil — Franklin de Lima Marquezino
Petrópolis, Brazil — Renato Portugal
Campinas, Brazil — Carlile Lavor
March 2019

# Acknowledgments

We are grateful to our colleagues and students from the Federal University of Rio de Janeiro (UFRJ, Brazil), the National Laboratory for Scientific Computing (LNCC, Brazil), and the University of Campinas (UNICAMP, Brazil) for several important discussions and interesting ideas.

We acknowledge CAPES, CNPq, FAPERJ, and FAPESP—Brazilian funding agencies—for the financial support to our research projects. We also thank the Brazilian Society of Computational and Applied Mathematics (SBMAC) for the opportunity to give a course on this subject that resulted in the first version of this monograph in Portuguese (http://www.sbmac.org.br/arquivos/notas/livro_08.pdf), which in turn evolved from our earliest tutorials (in arXiv quant-ph/0301079 and quant-ph/0303175).

# Contents


**1 Introduction** ..... 1
References ..... 4

**2 Bits and Qubits** ..... 7
2.1 The Classical Computer and Reversibility ..... 7
2.2 Review of Quantum Mechanics for Quantum Computation ..... 11
2.3 Quantum Circuits ..... 21
2.4 Universal Gates ..... 28
2.5 Computational Simulations ..... 31
References ..... 33

**3 Grover's Algorithm for Unstructured Search** ..... 35
3.1 Introduction ..... 35
3.2 Geometric Visualization ..... 39
3.3 A Small Example for Grover's Algorithm ..... 42
3.4 Generalization ..... 46
3.5 Grover Operator in Terms of Universal Gates ..... 49
3.6 Computational Simulations ..... 52
References ..... 54

**4 Shor's Algorithm for Integer Factorization** ..... 57
4.1 A Reduction of Integer Factorization to Order Finding ..... 58
4.2 Quantum Algorithm to Calculate the Order ..... 59
4.3 The Quantum Discrete Fourier Transform ..... 63
4.4 Generalization by Means of an Example ..... 66
4.5 Fourier Transform in Terms of the Universal Gates ..... 70
4.6 Computational Simulations ..... 76
References ..... 76

**5 Quantum Walks** ..... 79
5.1 Classical Random Walks ..... 79
5.2 Coined Quantum Walks ..... 81
5.2.1 Generalizing by Means of Examples ..... 84

5.3 Staggered Quantum Walks ..... 86
5.3.1 Tessellation Cover and the Evolution Operator ..... 86
5.3.2 An Example Using the Diamond Ring of Size 9 ..... 89
5.3.3 Diamond Ring of Size $N$ ..... 92
5.3.4 Reproducing the Flip-Flop Coined Model ..... 97
References ..... 100

**6 Conclusion and Further Remarks** ..... 103
References ..... 105

**Index** ..... 107