Preface

Quantum computing is a beautiful combination of quantum physics, computer science, and information theory. The purpose of this book is to make this exciting research area accessible to a broad audience. In particular, we endeavor to help the reader bridge the conceptual and notational barriers that separate quantum computing from conventional computing.

The book is concerned with theory: what changes when the classical model underpinning conventional computing is replaced with a quantum one. It contains only a brief discussion of the ongoing efforts to build quantum computers, an active area which is still so young that it is impossible even for experts to predict which approaches will be most successful. While this book is about theory, it is important to ground the discussion of quantum computation in the physics that motivates it. For this reason, the text includes discussions of quantum physics and experiments that illustrate why the theory is defined the way it is.

We precisely define concepts used in quantum computation and emphasize subtle distinctions. This rigor is motivated in part by our experience working with members of the joint FXPAL[1]/PARC[2] reading group and with reviewing papers by authors new to the field. Mistakes commonly arise due to a lack of precision. For example, we take care to distinguish a quantum state from a vector that represents it. We make clear which notions are basis dependent (e.g., superposition) and which are not (e.g., entanglement), and emphasize the dependence of certain notions (e.g., entanglement) on a particular tensor decomposition. The distinction between tensor decompositions and direct sum decompositions, both used extensively in quantum mechanics, is discussed explicitly in both quantum mechanical and classical probabilistic settings. Definitions are carefully motivated. For example, instead of starting with axioms for density operators or mixed states, the definitions of these concepts are motivated by a discussion of what can be deduced about a subsystem from measurements of the subsystem alone.

One advantage of dealing only with theory, and not with the efforts to build quantum computers, is that the amount of quantum physics and supporting mathematics needed is reduced. We are able to develop all of the necessary quantum mechanics within the book; no previous exposure to quantum physics is required. We give careful and precise descriptions of fundamental concepts—such as quantum state spaces, quantum measurement, and entanglement—before covering the standard quantum algorithms and other quantum information processing tasks such as quantum key distribution and quantum teleportation.

The intent of this book is to make quantum computing accessible to a wide audience of computer scientists, engineers, mathematicians, and anyone with a general interest in the subject who knows sufficient mathematics. Basic concepts from college-level linear algebra such as vector spaces, linear transformations, eigenvalues, and eigenvectors are used throughout the book. A few sections require more mathematics; familiarity with group theory is required for sections 8.6.1 and 8.6.2, appendix B, and much of chapter 11. Group theory is reviewed in boxes, but readers who have never seen group theory should consult a book on the subject or skip those sections.

While we hope our book lives up to the *gentle* of its title, reading it will require effort. Many of the concepts are subtle and unintuitive, and much of the notation unfamiliar. Readers will need to spend time working with the concepts and notations to develop a level of fluency at each stage. For example, even readers with significant mathematical background may not have worked much with tensor products and may not be familiar with the relation of tensor product spaces to their component spaces. The early chapters of the book develop these notions carefully, since they are absolutely fundamental to quantum information processing. It is well worth the effort to master them, as well as the concise Dirac notation in which they are generally expressed, but mastery will require effort. The precise nature of these mathematical formalisms provides a means of working with quantum concepts before fully understanding them. Intuition for quantum mechanics and quantum information processing will develop from playing with the formal mathematics.

The book emphasizes features of quantum mechanics that give quantum computation its power and are responsible for its limitations. Neither the extent of the power of quantum computation nor its limitations have been fully understood. Research challenges remain not only in building quantum computers and developing novel algorithms and protocols, but also in answering fundamental questions as to the source of quantum computing's power and the reasons for its limitations. This book examines what is known about what quantum computers can and cannot do, and also explores what is known about why.

The focus on the reasons underlying quantum computing's effectiveness results in the inclusion of topics frequently left out of other expositions of the subject. For example, one theme of the book is the relationship of quantum information processing to probability. That many quantum algorithms are nonprobabilistic is emphasized. A section is devoted to modifications of Grover's original algorithm that preserve the speed-up but return a solution with certainty. On the other hand, the strong formal resemblance between quantum theory and probability theory is described in detail and distinctions are highlighted, illuminating, for example, how entanglement differs from correlation, and the difference between a superposition and a mixture.

As another example, while *quantum entanglement* is the most common explanation given for why quantum information processing works, multipartite entanglement remains poorly understood. Bipartite entanglement is much better understood but has limited use for understanding quantum computation. The book includes sections on multipartite entanglement, a topic often left out of introductory books, and discusses bipartite entanglement. Discussions of multipartite entanglement require examples, which made it natural to include a section on cluster states, the fundamental entanglement resource used for cluster state, or one-way, quantum computation. Cluster state quantum computation and adiabatic quantum computation, two alternatives to the standard circuit model, are briefly introduced and their strengths and applications discussed.

As a final example, while the conversion between general classical circuits and reversible classical circuits is a purely classical topic, it is the heart of the proof that anything a classical computer can do, a quantum computers can do with comparable efficiency. For this reason, the book includes a detailed account of this piece of classical, but nonstandard, computer science.

This is not a book about quantum mechanics. We treat quantum mechanics as an abstract mathematical theory and consider the physical aspects only to elucidate theoretical concepts. We do not discuss issues of interpretation of quantum mechanics; the occasional use of terms such as *quantum parallelism*, for example, is not to be construed as an endorsement of one or another particular interpretation.

Acknowledgments

We are enormously indebted to Michael B. Heaney and Paul McEvoy, both of whom read multiple versions of many of the chapters and provided valuable comments each time. It is largely due to their steadfast belief in this project that the book reached completion. The FXPAL/PARC reading group enabled us to discover which expository approaches worked and which did not. The group's comments, struggles, and insights spurred substantial improvements in the book. We are grateful to all of the members of that group, particularly Dirk Balfanz, Stephen Jackson, and Michael Plass. Many thanks to Tad Hogg and Marc Rieffel for their feedback on some of the most technical and notationally heavy sections. Thanks also go to Gene Golovchinsky for suggestions that clarified and streamlined the writing of an early draft, to Livia Polanyi for suggestions that positively impacted the flow and emphasis, to Garth Dales for comments on an early draft that improved our wording and use of notation, and to Denise Greaves for extensive editorial assistance. Many people provided valuable comments on drafts of the tutorial[3] that was the starting point for this book. Their comments improved this book as well as the tutorial. We gratefully acknowledge the support of FXPAL for part of this work. We are grateful to our friends, to our family, and especially to our spouses for their support throughout the years it took us to write this book.

Notes

[1] FX Palo Alto Laboratory.
[2] Palo Alto Research Center.
[3] E. G. Rieffel and W. Polak. An introduction to quantum computing for non-physicists. *ACM Computing Surveys*, 32(3):300–335, 2000.