

Preface

In the decade since the publication of the first edition of “Explorations in Quantum Computing” the field has blossomed into a rich and diverse body of knowledge, and tremendous progress has been made on building functional quantum computer hardware. Yet I find that a discussion of *applications* of quantum computers still remains largely confined to Shor’s algorithm for factoring composite integers and Grover’s algorithm for quantum search. As more and more books have been written on quantum computing this standard presentation has been reinforced, thereby overlooking less well known, but arguably more interesting, applications.

In this edition I have tried to survey the field of quantum computing from a fresh perspective, showing how it can be applied to solve problems in a wide range of technical areas including physics, computer science, mathematics, chemistry, simulation, and finance. For sure, many of the newer quantum algorithms have their roots in Shor’s algorithm or Grover’s algorithm, but I think it is important to appreciate how the daughter algorithms have diverged from their parents. Moreover, there are now several quantum transforms known, such as the quantum wavelet and quantum cosine transforms, which show promising complexity properties and yet await exploitation in practical quantum algorithms. The classical versions of these transforms are of widespread utility in classical computing, especially signal and image processing, and I am optimistic that some fresh attention might stimulate others to find good uses for them.

The second edition is organized around four main parts. Part I addresses the question “What is Quantum Computing?” It provides the mathematical framework and physics concepts needed to understand quantum computing, and introduces the first quantum trick—quantum parallelism—and its use within the Deutsch-Jozsa algorithm. I assume the quantum circuit model but discuss several non-standard 2-qubit gates, such as SWAP ^{α} , iSWAP, and Berkeley B, that lend themselves more easily to implementation than does CNOT. In addition, I describe how to quantify the entangling power of quantum gates, and several techniques for constructing quantum circuits that achieve arbitrary n -qubit unitary, and non-unitary, operators including numerical, algebraic, and re-use methods, as well as specialized tricks for constructing optimal circuits for 2-qubit unitary operators.

Part II addresses the question “What Can you Do With a Quantum Computer?” I begin with Grover’s algorithm for quantum search, and applications thereof to speeding up randomized algorithms and synthesizing arbitrary superpositions. I then review Shor’s algorithm for factoring composite integers and computing discrete logarithms, and show how to apply these to breaking the RSA and elliptic curve public key cryptosystems. This is followed with a look at phase transition phenomena in computation and how to apply the insights gleaned from these studies to characterize the complexity of a nested quantum search I developed with Nicolas Cerf and Lov Grover for solving **NP-Complete** problems. This is followed by chapters on applications of quantum algorithms to quantum simulation, quantum chemistry and mathematics. These three areas have the greatest potential for finding new and important quantum algorithms for solving practical problems.

The second edition also includes a greatly expanded discussion of quantum information theory. In particular, in Part III “What Can you Do with Quantum Information”, I look at the notion of pure versus mixed states, density operators, entanglement, how to quantify it, the partial transpose (for signalling the presence of entanglement), the partial trace (for characterizing part of a larger quantum system), and Schmidt decompositions. I have gone beyond the standard presentations on quantum teleportation and superdense coding, to include less well known but potentially useful protocols such as quantum data compression, universal quantum cloning and universal negation—all with complete quantum circuit descriptions. I again emphasize applications of these protocols. In particular, I describe how quantum teleportation has inspired an entirely new, and very promising, model of quantum computation, and how approximate clones and approximate negated states can be used to determine the exact expectation values of observables of ideal clones and ideal negated states. I then describe the most mature of the quantum technologies—quantum cryptography—and discuss the challenges in integrating quantum cryptography with the commercial secure communications infrastructure. I survey the three main quantum key distribution protocols—Bennett and Brassard’s BB84, Bennett’s B92, and Ekert’s E91 protocols, and how they have been implemented in fiber and free-space systems, and look at the prospects for extending the range of quantum cryptography using quantum repeaters and Earth-to-Space channels.

Finally, the book concludes with Part IV “Towards Practical Quantum Computers” by examining some of the practical issues in designing scalable quantum computers. However, I have elected to focus not on hardware per se, for which many excellent texts already exist, but more on reliability and architectural issues. In particular, I describe several techniques for quantum error correction including error reduction by symmetrization, quantum error correcting codes, the optimal 5-qubit code, stabilizer codes, bounds on quantum codes, fault-tolerance and concatenated quantum codes. I end the book by discussing the amazing array of alternative models of quantum computing beyond the quantum circuit model, showing how they are inter-related, and how certain schemes lend themselves naturally to implementation in particular types of quantum computer hardware.

The new edition also includes numerous end-of-chapter exercises. Many of these were field tested on students I taught at Stanford University while teaching my “Introduction to Quantum Computing and Quantum Information Theory” course for

several years. In so doing, I learned first hand which concepts students found most difficult. Moreover, in teaching these classes and elsewhere I have learned that quantum physics appeals to many people who might not otherwise have much interest in science. For example, Playboy Playmate Carmen Elektra has been quoted as saying “*I’m really into quantum physics. Some of my friends are into it, some of them aren’t, so I’m trying to get them excited about discovering all these interesting things about thoughts and the power of thoughts. It gives me chills thinking about it. It’s fun.*” [169]. Although some of my colleagues have mocked her for saying this, I say bravo Carmen! Quantum physics is indeed an amazing branch of science, which challenges our most foundational assumptions about the nature of reality. It’s a wonderful thing when a scientific field can so electrify someone that they are compelled to seek a deeper understanding. Certainly, experience in teaching to a very diverse student body has encouraged me to explain things as simply as possible in a self-contained volume. And I hope the reader benefits from my more inclusive style. I can certainly say that Carmen Elektra’s interest in matters quantum has at least given me a more arresting answer to the question “Who did you have in mind when you wrote your book?” than is typical of most scholarly texts!

Finally, I would like to thank the people who have helped me make this second edition a reality. First my family for putting up with the countless evenings and weekends I was away from them. And to Wayne Wheeler and Simon Rees of Springer-Verlag for their encouragement, and eternal patience, in seeing the manuscript through to completion. They deserve a very big thank you! In addition, I am indebted to the physicists and computer scientists who have developed the field of quantum computing to what it is today. Many of these people are known to me personally, but some only via their research papers. I hope I have done justice to their research contributions in writing about them. Known personally to me or not, they have all greatly enriched my life via their discoveries and insights.

Colin P. Williams



<http://www.springer.com/978-1-84628-886-9>

Explorations in Quantum Computing

Williams, C.P.

2011, XXII, 717 p., Hardcover

ISBN: 978-1-84628-886-9