Preface

This book arose from an American Mathematical Society Short Course entitled:

Quantum Computation
A Grand Mathematical Challenge
for the
Twenty-First Century and the Millennium

held in Washington, DC, January 17-18, 2000 in conjunction with the Annual Meeting of the American Mathematical Society in Washington, DC, January 19-22, 2000.

This AMS Short Course was created with the objective of sharing with the scientific community the many exciting mathematical challenges arising from the new and emerging field of quantum computation and quantum information science. In so doing, it was hoped that this AMS Short Course would act as a catalyst to encourage, to entice, and, yes, ... to challenge and ultimately to dare mathematicians into working on the many diverse grand mathematical challenges arising in this field.

To meet this objective, the AMS Short Course was designed to demonstrate the great breadth and depth of this mathematically rich research field. Interrelationships with existing mathematical research areas were emphasized as much as possible. Moreover, the entire AMS Short Course was designed in such a way that course participants with little, if any, background in quantum mechanics would, on completion of the course, be prepared to begin reading the research literature on quantum computation and quantum information science.

Much to my surprise, the response to this AMS Short Course exceeded my most ambitious expectations. I thank the audience for their encouragement and enthusiastic response, and for their many helpful questions and suggestions in regard to the material presented.

This book is a written version of the eight lectures given in this AMS Short Course. Based on audience feedback and questions, the written versions of these lectures have been greatly expanded, and supplementary material has been added.

Chapter I of this book begins with two papers extending an invitation to this research field. The first by Samuel J. Lomonaco, Jr., entitled "A Rosetta Stone

©0000 (copyright holder)

to Quantum Mechanics with an Introduction to Quantum Computation," provides the reader with an overview of the relevant parts of quantum mechanics, and with an entrée into the world of quantum computation. The second by Howard E. Brandt, entitled, "Qubit Devices," provides an overview of many potential quantum mechanical computing devices.

Chapter II consists of four papers devoted to quantum algorithms and quantum complexity theory. The first paper by Peter W. Shor, entitled "Introduction to Quantum Algorithms," gives an in depth overview of quantum algorithms, explaining why recent results in this area are so surprising. It also illustrates the general technique of using the Fourier transform to find periodicity, and discusses the quantum algorithms of Simon, Shor, and Grover. The second and third papers by Samuel J. Lomonaco, Jr., entitled respectively "Shor's Quantum Factoring Algorithm" and "Grover's Quantum Search Algorithm," were created in response to audience feedback, and focus more closely on the mathematical inner workings and underpinnings of Shor's and Grover's algorithms. The chapter closes with a fourth paper by Umesh Vazirani, entitled "Quantum Complexity Theory," devoted to the many intriguing and challenging issues of quantum complexity theory. The paper begins with a discussion of the current day challenge to the Church-Turing thesis, and then proceeds into a discussion of quantum complexity classes.

Chapter III is comprised of two papers focusing on quantum error correcting codes and quantum cryptography. The first paper by Daniel Gottesman, entitled "An Introduction to Quantum Error Correction," gives an introduction to quantum information science's first line of defense against the ravages of quantum decoherence, i.e., quantum error correcting codes. The paper begins with a discussion of error models, moves on to quantum error correction and the stabilizer formalism, ending with a quantum error correction sonnet. The second paper by Samuel J. Lomonaco, Jr., entitled "A Talk on Quantum Cryptography, or How Alice Outwits Eve," gives an in depth analysis of quantum cryptographic protocols, including the BB84, B92, and possible eavesdropping counter measures. All of this is interwoven into the context of a fictional story about how Alice invents quantum cryptographic protocols to outwit the archvillainess Eve, ... or does she?

The final Chapter IV consists of three papers discussing many more diverse connections between quantum computation and mathematics and physics. The first paper by Alexei Kitaev, entitled "Topological Quantum Codes and Anyons," discusses how anyons can be applied to quantum computation. Anyons are two dimensional particles that have been found in two-dimensional electronic liquids exhibiting the fractional quantum Hall effect. This paper discusses how Aharonov-Bohm-like interactions of anyons can be used to create topological obstructions to quantum decoherence. Such topological obstructions can be used to construct quantum error correcting codes. Both abelian and nonabelian anyons are discussed. The second paper by Louis H. Kauffman, entitled "Quantum Topology and Quantum Computing," explores some of the tantalizing relationships between knots, links, three manifold invariants and quantum information science. Many possible applications of quantum topology to quantum computing and vice versa are discussed. The third and final paper by Samuel J. Lomonaco, Jr., entitled "An Entangled Tale of Quantum Entanglement," discusses how Lie group invariant theory can be used

to quantify a physical phenomenon that many believe to be at the very core of quantum computation, namely, quantum entanglement. The paper shows how to lift the big adjoint action of the group of local unitary transformations to the corresponding infinitesimal action to produce a system of partial differential equations whose solution is a complete set of entanglement invariants. Examples are given.

It is hoped that this book will encourage its readers to embrace and pursue the grand challenge of quantum computation.

Samuel J. Lomonaco, Jr.
Lomonaco@umbc.edu
http://www.csee.umbc.edu/~lomonaco
August 15, 2001