

INTRODUCTION TO QUANTUM INFORMATION SCIENCE, ECE 548

Quantum phenomena provide computing and information handling paradigms that are distinctly different and arguably much more powerful than their classical counterparts. In the past quarter of the century, much progress has been made on the theoretical side, and experiments have been carried out in which quantum computational operations were executed on a very small number of quantum bits. The NSF has declared this general area to be one of the 10 big ideas for future investments.

This new course will provide an introduction to the theory of quantum computing and information. The topics that will be covered are include 1) the fundamental elements of quantum information processing (qubits, unitary transformations, density matrices, measurements); 2) entanglement, protocols for teleportation, the Bell inequality, 3) basic quantum algorithms such as Shors factoring and Grovers search, and 4) basic quantum data compression and error correction. The course material will be accessible to undergraduate and graduate students with a variety of backgrounds, e.g., electrical engineers, physicists, mathematicians, and computer scientists.

Learning Objective:

The students will learn the fundamentals of quantum information science, as well as a selected number of more advanced topics of their individual interests.

Instructor: Emina Soljanin emina.soljanin@rutgers.edu, CoRE 511, 848-445-5256.

Office hours: TBD & by appointment,

Class time and place: TBD

Prerequisites: Calculus, linear algebra, and probability at an undergraduate level as well as familiarity with complex numbers are required. Prior exposure to quantum mechanics and information/coding theory is helpful but not essential.

Grading: homework homework 20%, 2 midterm exams 20% each, final exam 40%.
(Exams will be in class, approximately late September and late October)

Text: N. D. Mermin, *Quantum Computer Science: An Introduction*, Cambridge Univ. Press (2007)
(see attached table of contents)

Course notes: given per week in separate documents on the class Sakai page.

Final remark: The topics outlined above are very common for a quantum information science course at this level. Such courses have been thought at many universities for many years, e.g. for almost two decades at Cornell based on the proposed textbook.

Quantum Computer Science

An Introduction

©2006, N. David Mermin

Table of Contents

Preface

A note on references

1. Cbits and Qbits

- 1.1. What is a quantum computer?
- 1.2. Cbits and their states
- 1.3. Reversible operations on Cbits
- 1.4. Manipulating operations on Cbits
- 1.5. Qbits and their states
- 1.6. Reversible operations on Qbits
- 1.7. Circuit diagrams
- 1.8. Measurement gates and the Born rule
- 1.9. The generalized Born rule
- 1.10. Measurement gates and state preparation
- 1.11. Constructing arbitrary 1- and 2-Qbit states
- 1.12. Summary: Qbits vs. Cbits

Chapter 2. General Features and Some Simple Examples

- 2.1. The general computational process
- 2.2. Deutsch's problem
- 2.3. Why additional subroutine Qbits needn't mess things up
- 2.4. The Bernstein-Vazirani problem
- 2.5. Simon's problem
- 2.6. Constructing Toffoli gates

Chapter 3. Breaking RSA Encryption with a Quantum Computer

- 3.1. Period finding, factoring, and cryptography
- 3.2. Number theoretic preliminaries
- 3.3. RSA encryption

- 3.4. Quantum period-finding: preliminary remarks
- 3.5. The quantum Fourier transform
- 3.6. Eliminating the 2-Qbit gates
- 3.7. Finding the period with help of the quantum Fourier transform
- 3.8. Calculating the periodic function: quantum vs. classical programming
- 3.9. Unimportance of small phase errors: digital vs. analogue
- 3.10. Period finding and factoring

Chapter 4. Searching with a Quantum Computer

- 4.1. Nature of the search
- 4.2. The Grover iteration
- 4.3. How to construct **W**
- 4.4. Generalization to several special numbers
- 4.5. Searching for 1 out of 4 items

Chapter 5. Quantum Error correction

- 5.1. The miracle of quantum error correction
- 5.2. A simplified example
- 5.3. The physics of error generation
- 5.4. Diagnosing error syndromes
- 5.5. The 5-Qbit error correcting code
- 5.6. The 7-Qbit error correcting code
- 5.7. Operations on 7-Qbit codewords
- 5.8. A 7-Qbit encoding circuit
- 5.9. A 5-Qbit encoding circuit

Chapter 6. Protocols that use just a few Qbits

- 6.1. Bell states
- 6.2. Quantum cryptography
- 6.3. Bit commitment
- 6.4. Quantum dense coding
- 6.5. Teleportation
- 6.6. The GHZ state

Appendix A. Vector spaces: basic properties and Dirac notation

Appendix B. Structure of the general 1-Qbit unitary transformation

Appendix C. Structure of the general 1-Qbit state

Appendix D. Spooky action at a distance
Appendix E. Consistency of the generalized Born rule
Appendix F. Other aspects of Deutsch's problem
Appendix G. Probability of success in Simon's problem
Appendix H. One way to make a cNOT gate
Appendix I. A little elementary group theory
Appendix J. Some simple number theory
Appendix K. Period finding and continued fractions
Appendix L. Better estimates of success in period-finding
Appendix M. Factoring and period finding
Appendix N. Shor's 9-Qbit error correcting code
Appendix O. Circuit diagrammatic treatment of the 7-Qbit code
Appendix P. On bit commitment