

Physics 219/Computer Science 219

Quantum Computation

Alexei Kitaev

Fall 2004 – Winter 2005

Course Description

Basic concepts of quantum mechanics. Quantum gates and circuits. Quantum entanglement. Introduction into computation complexity. Quantum algorithms. Quantum error-correcting codes and fault-tolerant quantum computation. Some proposed physical realizations of a quantum computer. Anyons and topological quantum computation.

Prerequisites

I hope to make the course self-contained and accessible to people with a variety of backgrounds. The essential prerequisites are linear algebra and some basic concepts in probability and group theory. It would be useful (but not necessary) to have had a previous course on quantum mechanics. In the discussion of Shor's algorithm, we will use some rudimentary number theory.

Class meetings

Monday and Wednesday 9:00–10:30 107 Downs

Instructors

Alexei Kitaev

280 Jorgensen

Telephone: (626)395-8760

e-mail: kitaev@iqi.caltech.edu

Teaching assistant: **Graeme Smith**

445 Lauritsen

Telephone: (626)395-2633

e-mail: graeme@its.caltech.edu

office hours: to be determined

References

- Textbooks:
- John Preskill, *Lecture notes*, <http://www.theory.caltech.edu/people/preskill/ph229/>
 - A. Kitaev, M. Vyalyi, and A. Shen, *Classical and Quantum computation*
- Other recommended books: Michael Nielsen and Isaac Chuang, *Quantum Computation and Quantum Information*
- Research papers: Many original papers on the subject can be found in the e-print archive <http://www.arxiv.org>, section Quantum Physics. Some particular references will be given during the course.

Note: Preskill's notes are very nice and easy to read. They provide an excellent introduction and cover some of the advanced topics (in particular, anyons). The book by Kitaev, Vyalyi, and Shen is more mathematical and focused on computational complexity. Nielsen and Chuang's book is the most comprehensive and can be used as a reference.

Course Requirements

There will be regularly assigned problem sets (four in each term). The grading is pass/fail.

Policies

Late homework: Late assignments normally lose 25% credit, but you will be allowed one one-week extension per term without penalty. Assignments late by more than one week are not accepted. Exceptions may be granted for legitimate reasons, but you should ask for them prior to the deadline.

Collaboration: You may discuss the problems with each other while you are trying to solve them, but you must write up your solutions alone.

Other: Some of the problems will be taken from the last year course (exactly or with minor modifications); their solutions might be circulated. You may not look at those solutions until you have turned in your homework.

Course Outline

First term (Fall 2004)

Brief overview of the course material.

Foundations of quantum mechanics: Quantum states. Measurement and probability. Unitary operators and continuous-time dynamics. Quantum gates and circuits.

Quantum mechanics of an open system: Density matrix. The Schmidt decomposition and purification. Models of measurement and decoherence. The nature of irreversibility.

Tensor algebra: Basis changes and invariant language. The dual space. Tensor product. Index contraction and tensor networks.

Entanglement: The Einstein-Podolsky-Rosen paradox and quantum notion of causality. Bell inequalities. Quantum games without communication. Superdense coding and quantum teleportation. The impossibility of quantum bit commitment.

Distance measures for density operators: Trace norm and fidelity.

Transformations of density operators: POVM measurements. Superoperators.

Introduction into complexity theory: Turing machines and Boolean circuits. Uniform and nonuniform computational models; classes P and P/poly. Other complexity classes: BPP, NP, PSPACE. Karp and Turing reductions.

Quantum circuits: Reversible classical computation. Various tricks with quantum gates. Representing unitary operators by two-qubit gates. Precision. Universal gate sets. Quantum Fourier transform.

Quantum algorithms: The class BQP. Grover's algorithm and its optimality. Simon's algorithm.

Elements of number theory: Greatest common divisor and Euclid's algorithm. Modular arithmetic. Unique factorization for integers. Chinese remainder theorem. Fermat's little theorem.

More quantum algorithms: Phase estimation. Factoring. The hidden subgroup problem.

Second term (Winter 2005)

Classical and quantum error-correcting codes

Fault-tolerant quantum computation

Some proposed physical realizations of a quantum computer

Anyons and topological quantum computation