Department of Mathematics Vanderbilt University

Fall Semester 2002, MATH 394A

QUANTUM INFORMATION THEORY

TuTh 9:35-10:50 AM, SC 1403

Dietmar Bisch

Prerequisites: Basic linear algebra and analysis. Some knowledge of quantum mechanics would be helpful, but I will spend a few lectures reviewing the basics.

Syllabus: I will discuss in this course some of the basic concepts in *quantum computing* and *quantum information theory*, that is the theory of information processing using a quantum physical system.

After a short introduction to quantum mechanics (observables, states, measurements, density matrices and all that), I plan to discuss the notion of *entanglement* of quantum systems. Entanglement is a feature of quantum mechanics, which does not exist in classical physics (Einstein called it the "*spooky action at a distance*"). It expresses a correlation of subsystems of a quantum physical system which appears naturally as soon as the commutative algebras of functions in classical physics are replaced by *non-commutative* algebras of operators (matrices) in quantum physics. If correlated quantum systems contain "enough" entanglement, then they can be used to transmit quantum information on a classical channel (so-called *quantum teleportation*). Mathematically, noncommutative structures described by *operator theory*, the theory of *operator algebras* and the theory of *completely positive maps* are at the heart of these phenomena.

In the second part of the course I will present the basics of quantum computation and quantum algorithms. In particular I will describe Peter Shor's famous *factoring algorithm*, which can be used to factor integers on a (hypothetical) quantum computer in polynomial time. Shor's result was quite a surprise since the best known algorithms on a classical computer to date are exponential in the number of digits of the integer to be factored. Current encryption schemes that insure network and data security are based on the assumption that factoring an integer (or equivalent problems) is a hard problem in the sense of complexity theory. Quantum computing has triggered the need for new encryption schemes, which has led to the field of *quantum cryptography*, currently a very active research area.

This course will concentrate on the more theoretical aspects of quantum computing and quantum information theory. For instance, I will not have time to discuss the numerous ideas currently on the market for actually building a quantum computer.

Grading: There will be no exams. The course grade will be based on attendance. I will assign (optional) problems during the lectures.

Recommended literature: 1) Michael Nielsen, Isaac Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.
2) A. Kitaev, A.H. Shen, M.N. Vyali, *Classical and quantum computation*, American Mathematical Society 2002.
3) R.F. Werner, *Quantum Information Theory - An Invitation* (available at the preprint server xxx.lanl.gov, quant-ph/0101061).

Further references to research articles will be given throughout the course.