

Programma del corso di Informazione Quantistica (a.a. 2005-2006)

Prima parte: Introduzione al calcolo classico

The Turing machine. Addition on a Turing machine. The Church–Turing thesis. The universal Turing machine. The probabilistic Turing machine. The halting problem. The circuit model of computation. Binary arithmetics. Elementary logic gates. Universal classical computation. Computational complexity. Complexity classes. The Chernoff bound. Energy and information. Maxwell’s demon. Landauer’s principle. Extracting work from information. Reversible computation. Toffoli and Fredkin gates.

Seconda parte: Richiami di meccanica quantistica

The Stern–Gerlach experiment. Young’s double-slit experiment. Linear vector spaces. The postulates of quantum mechanics. The EPR paradox and Bell’s inequalities.

Terza parte: Calcolo quantistico

Quantum Computation. The qubit. The Bloch sphere. Measuring the state of a qubit. The circuit model of quantum computation. Single-qubit gates. Rotations of the Bloch sphere. Controlled gates and entanglement generation. The Bell basis. Universal quantum gates. Unitary errors. Function evaluation. The quantum adder. Deutsch’s algorithm. The Deutsch–Jozsa problem. An extension of Deutsch’s algorithm. Quantum search. Searching one item out of four. Searching one item out of N . Geometric visualization. The quantum Fourier transform. Quantum phase estimation. Period finding and Shor’s algorithm. First experimental implementations. Elementary gates with spin qubits. Overview of the first implementations.

Quarta parte: Comunicazione e crittografia quantistiche

Classical cryptography. The Vernam cypher. The public-key cryptosystem. The RSA protocol. The no-cloning theorem. Faster-than-light transmission of information? Quantum cryptography. The BB84 protocol. Quantum teleportation.

Testi consigliati

G. Benenti, G. Casati and G. Strini, “Principles of Quantum Computation and Information. Volume I: Basic Concepts” (World Scientific, Singapore, 2004): Capitolo 1 (escluso 1.4, 1.6.2), Capitolo 2, Capitolo 3 (escluso 3.5.1, 3.13, 3.15), Capitolo 4 (escluso 4.3.2, 4.4).

(*)Programma del corso disponibile alla pagina web
<http://www.ba.infn.it/~pascazio/teoriacampi.html>