

Course content for MT3450/MT4450, Quantum Information and Coding

Prerequisites:

MT2800

Aims:

'Anybody who is not shocked by quantum theory has not understood it' (Niels Bohr). This course aims to provide a sufficient understanding of quantum theory in the spirit of the above quote. Many applications of the novel field of quantum information theory can be studied using undergraduate mathematics. The course relies almost exclusively on tools from linear algebra – prior knowledge of applied mathematics or quantum theory is neither required nor particularly useful.

Learning outcomes:

On completion of the course the student should be able to:

- demonstrate an understanding of the principles of quantum superposition and quantum measurement;
- use the basic linear algebra tools of quantum information theory confidently; manipulate tensor-product states and use and explain the concept of entanglement;
- explain applications of entanglement such as quantum teleportation or quantum secret key distribution;
- describe the Einstein-Podolsky-Rosen paradox and derive a Bell inequality; solve a range of simple problems involving one or two quantum bits;
- explain Deutsch's algorithm and its implications for the power of a quantum computer;
- MT4450: demonstrate a breadth of understanding appropriate for an M-level course.

Course content:

Linear algebra: Complex vector space, inner product, Dirac notation, projection operators, unitary operators, Hermitian operators, Pauli matrices.

One qubit: Pure states of a qubit, the Poincaré sphere, von Neumann measurements, quantum logic gates for a single qubit.

Tensor products: 2 qubits, 3 qubits, quantum logic gates for 2 qubits, Deutsch's algorithm, the Schmidt decomposition.

Mixed states: Partial trace, probability, entropy, von Neumann entropy.

Entanglement: The Einstein-Podolsky-Rosen paradox, Bell inequalities, quantum teleportation, measures of entanglement, decoherence.

Further applications, such as e.g. the quantum Fourier transform, Shor's factoring algorithm, the BB84 key distribution protocol, Grover's search algorithm, quantum channel capacity, the Holevo bound.