

Quantum Information Theory

Quantum mechanics makes probabilistic predictions about experiments, and indeed it is a theory of generalised probability: Rather than treating probability distributions as primary objects, these are generalised to density operators and their transformations. In short, it is the pre-eminent example of a “non-commutative probability theory”.

Since the 1980s this point of view has led to the development of a theory of quantum information that generalises previous notions of probability and information. Armed with such a theory we can see how uncertainty relations and entanglement allow us to build unbreakable cryptosystems based on quantum communication, and how our intuitive notions of information has extensions into the quantum world, and often unprecedented analogues that have no classical counterpart.

This unit teaches the basics of quantum information, and describes some of its key applications to quantum communication. The unit is self-contained and assumes only knowledge of basic linear algebra and probability. Previous experience with quantum mechanics is helpful, but not required.

Instead, the unit will introduce a range of mathematical techniques and ideas that find applications in quantum information: normed spaces, operator algebras, convex geometry, convex (in particular: semidefinite) optimisation, and of course information theory.

Topics

- *Introduction*: -pure states, measurements, distinguishing quantum states. Tensor products and composite systems. Super-dense coding, teleportation and the no-cloning theorem.
- *Errors*: quantum error-correcting codes, remarks on fault-tolerant quantum computing.
- *Quantum nonlocality and quantum cryptography*: entanglement, Bell’s inequalities, secret key distribution.
- *Information theory*: noisy quantum states, purifications, von Neumann entropy, data compression and noisy quantum channels.