ANDREAS WINTER, University of Bristol, Department of Mathematics, Bristol BS8 1TW, UK

Random coding for quantum information

In this talk, the conceptual and mathematical ideas in a Lloyd–Shor type proof of the quantum channel capacity theorem will be presented.

To be precise, we will look at a general *quantum channel* $\mathcal{N}$, *i.e.*, a completely positive and trace preserving linear map on density operators, and study block coding of quantum information for n instances $\mathcal{N}^{\otimes n}$ of the channel, for large n. After introducing these concepts in mathematical terms, we will study a specific random coding procedure, which we call *Haar-random codes*. These are akin to P. Shor's proposal [MSRI talk, Nov. 2002; lecture notes online at `http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/`]: the code is (essentially) a subspace of the sender's typical space, chosen according to the unitarily invariant measure.

The "standard" approach to analysing the performance of quantum codes [see S. Lloyd, PRA 1997; I. Devetak, IEEE IT 2005] proceeds by showing

(i) that a basis of the code subspace can be distinguished reliably by the receiver;

(ii) that the channel environment has almost no information about this basis;

(iii) finally, how these two elements imply that superpositions of the basis vectors can be error-corrected with high fidelity.

After highlighting this strategy and some of its technical difficulties, we will demonstrate a new strategy which has the advantage of leading to the result with minimal technical effort, and which is also conceptually nice. It entirely avoids the difficult step (ii), the privacy of the code against the environment, which comes out automatically. Instead, we show

(a) that a basis and its Fourier conjugate basis of the code subspace each can be distinguished reliably by the receiver;

(b) how a recently discovered information uncertainty relation [M. Christandl and AW, `quant-ph/0501090`] then implies that the *quantum mutual information* between sender and receiver is close to maximum—and the quantum mutual information between sender and environment is close to 0;

(c) finally, a simple algebraic reasoning [B. Schumacher and M. Westmoreland, Quantum Inf. Proc. 2002] shows the existence of a decoding procedure.

Time permitting, variations and other applications of the Haar-random coding will be shown.