MAR11-2010-002777

Abstract for an Invited Paper
for the MAR11 Meeting of
the American Physical Society

A Brief Prehistory of Qubits

BENJAMIN SCHUMACHER, Kenyon College

In the early 1990's, alongside the early work on quantum cryptography, there existed a considerable body of research on the classical information capacity of quantum channels. The strongest and most general result known was the theorem of Holevo giving an entropic bound for the accessbile information in a mixture of quantum signals. This motivated the problem of whether the Holevo bound could be closely approached by suitable choice of code and decoding observable. If so, then the quantum (von Neumann) entropy had a straightforward informational interpretation. When this question was found to be very difficult to answer, quantum data compression and the idea of a "qubit" was introduced as an alternate framework for thinking about information in quantum systems and interpreting the quantum entropy. However, the mathematical ideas from the new framework proved essential to solving the original problem of showing that the Holevo bound was asymptotically achievable. This was an early example of the interplay between classical and quantum concepts of information – an interplay that has been, to say the least, extremely fruitful.