Quantum Interactive Proofs

John Watrous (jwatrous@cpsc.ucalgary.ca)
University of Calgary
Department of Computer Science
Calgary, Alberta
T2N 1N4, Canada

Abstract.

Interactive proof systems were first introduced in 1985, both as a natural extension of the class **NP** and as a model for various cryptographic situations. Quantum interactive proof systems are interactive proof systems in which the prover and verifier may perform quantum computations and exchange quantum messages. In this talk, I will survey some of the known facts about quantum interactive proof systems, and discuss some of the tools that are helpful for analysing their properties.