Proving the results of quantum computations

Joseph Fitzsimons

Centre for Quantum Technologies, National University of Singapore,
3 Science Drive 2, Singapore 117543.
joe.fitzsimons@nus.edu.sg

Abstract. For certain applications quantum algorithms offer vastly more efficient computation than is possible with known classical algorithms. For some of these problems, such as factoring or calculating discrete logarithms, the problem is in FNP, and hence the result of the quantum computation can be efficiently verified classically. For other applications, however, such as simulating quantum systems which is not believed to be in FNP, there is no known efficient classical test on the output to verify its correctness.

Interactive proofs provide a potential solution to this problem. In this talk I will focus on the problem of whether or not the results of a quantum computer can be classically verified via interactive proof. I will introduce the notion of 'blind quantum computation', and discuss how it can be exploited in the context of verification and interactive proof systems. Blind quantum computation refers to the problem of allowing Alice to have Bob carry out a quantum computation for her such that Bob learns nothing about the computation that he performs. I will introduce a protocol for performing secure blind computation and show that it allows any quantum computation to be verified by a classical verifier given to non-communicating but entangled quantum provers, or by a semi-classical verifier using only a single quantum prover. The existence of such a protocol has consequences for the study of complexity theory, as it allows quantum verifiers in multiple-prover interactive proofs to be replaced with classical verifiers. Based on joint work with Anne Broadbent and Elham Kashefi.