Quantum vs. Classical Communication and Computation

March 12, 1998

Harry Buhrman
Richard Cleve
Avi Wigderson

Abstract
We present a simple and general simulation technique that transforms any black-box quantum algorithm (`*a la* Grover's database search algorithm) to a quantum communication protocol for a related problem, in a way that fully exploits the quantum parallelism. This allows us to obtain new positive and negative results.

The positive results are novel quantum communication protocols that are built from nontrivial quantum algorithms via this simulation. These protocols, combined with (old and new) classical lower bounds, are shown to provide the first asymptotic separation results between the quantum and classical (probabilistic) two party communication complexity models. In particular, we obtain a quadratic separation for the bounded-error model, and an exponential separation for the zero-error model.

The negative results transform known quantum communication lower bounds to computational lower bounds in the black-box model. In particular, we show that the quadratic speed-up achieved by Grover for the *OR* function is impossible for the *PARITY* function or the *MAJORITY* function in the bounded-error model, nor is it possible for the *OR* function itself in the exact case. This dichotomy naturally suggests a study of bounded-depth predicates (i.e. those in the polynomial hierarchy) between *OR* and *MAJORITY*. We present black-box algorithms that achieve near quadratic speed up for all such predicates.