Quantum Lower Bounds (Adversary Method)

Andris Ambainis (ambainis@ias.edu)
Institute for Advanced Study
School of Mathematics
Princeton, NJ 08540
USA

Abstract.

The adversary method is one of main methods for proving lower bounds in quantum computing. There are two versions of this method: the classical adversary and the quantum adversary. In classical adversary, we prove a lower bound by simulating an algorithm on an input or probability distribution on inputs. In quantum adversary, we simulate an algorithm on a quantum state consisting of various classical inputs. The algorithm's internal state then becomes entangled with the input state and we can prove lower bounds by bounding this entanglement.

In my talk, I will describe both versions of the adversary method, show how they give the $\Omega(\sqrt{n})$ lower bound on Grover's search problem and a general lower bound theorem which applies to a variety of problems.