Quantum One-Way Communication can be Exponentially Stronger Than Classical Communication

Oded Regev (joint work with B. Klartag)

In STOC 1999, Raz presented a (partial) function for which there is a quantum protocol communicating only $O(\log n)$ qubits, but for which any classical (randomized, bounded-error) protocol requires poly(n) bits of communication. That quantum protocol requires two rounds of communication. Ever since Raz's paper it was open whether the same exponential separation can be achieved with a quantum protocol that uses only one round of communication. In other words, can quantum one-way communication be exponentially stronger than classical two-way communication? Here we settle this question in the affirmative.