Local Proofs Approaching the Witness Length

Abstract:

Interactive oracle proofs (IOPs) are a hybrid between interactive proofs and PCPs. In an IOP the prover is allowed to interact with a verifier (like in an interactive proof) by sending relatively long messages to the verifier, who in turn is only allowed to query a few of the bits that were sent (like in a PCP).

For any NP relation for which membership can be decided in polynomial-time and bounded polynomial space (e.g., SAT, Hamiltonicity, Clique, Vertex-Cover, etc.) and for any constant $\gamma > 0$, we construct an IOP with communication complexity $(1+\gamma) \cdot n$, where $n$ is the original witness length. The number of rounds as well as the number of queries made by the IOP verifier are constant.

Joint work with Noga Ron-Zewi