Constant-Round Interactive Proofs for Delegating Computation

Abstract:

Interactive proofs have had a dramatic impact on Complexity Theory and Cryptography. The celebrated IP=PSpace Theorem [LFKN92,Shamir92] allows an all-powerful but untrusted prover to convince a polynomial-time verifier of the validity of extremely complicated statements (as long as they can be evaluated using polynomial space). The interactive proof system designed for this purpose requires a polynomial number of communication rounds. This talk will focus on studying the power of more efficient interactive proof systems.

Our main result is that for every statement that can be evaluated in polynomial time and bounded-polynomial space, there exists an interactive proof that satisfies the following strict efficiency requirements:

(1) The honest prover runs in polynomial time.

(2) The verifier is almost linear time (and under some conditions even sub linear).

(3) The interaction consists of only a constant number of communication rounds.

To obtain this result, we introduce and study several new notions for interactive proofs, which may be of independent interest. One of these notions is that of unambiguous interactive proofs, where the prover has a unique successful strategy. Another notion is that of probabilistically checkable interactive proofs (PCIPs) where the verifier only reads a few bits of the transcript in checking the proof (this could be viewed as an interactive extension of PCPs).

Joint work with Omer Reingold and Ron Rothblum.