On Interactive Proofs With a Laconic Power

Oded Goldreich
Salil Vadhan
Avi Wigderson

Abstract

We continue the investigation of interactive proofs bounded communication, as initiated by Oded Goldreich and Håstad (IPL 1998). Let L be a language that has an interactive proof in which the prover sends few (say b) bits to the verifier. We prove that the complement $\overline L$ has a *constant-round* interactive proof of complexity that depends only exponentially on b. This provides the first evidence that for NP-complete languages, we cannon expect interactive provers to be much more “laconic” than the standard NP proof. When the proof system is further restricted (e.g. when $b=1$, or when we have perfect completeness), we get significantly better upper bounds on the complexity of L.