

On Interactive Proofs with a Laconic Prover

PRELIMINARY VERSION

Oded Goldreich*

Department of Computer Science
Weizmann Institute of Science
Rehovot, ISRAEL.
oded@wisdom.weizmann.ac.il

Salil Vadhan†

Division of Engineering & Applied Sciences
Harvard University
Cambridge, MA
salil@eecs.harvard.edu

Avi Wigderson‡

Institute for Advanced Study
Princeton, NJ.
avi@ias.edu

July 1, 2001

Abstract

We continue the investigation of interactive proofs with bounded communication, as initiated by 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 \bar{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 cannot 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 \bar{L} .

Keywords: interactive proofs, Arthur-Merlin games, sampling protocols, statistical zero knowledge, game theory

*Supported by the MINERVA Foundation.

†Work done while at the Institute for Advanced Study, Princeton, NJ, supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship. URL: <http://eecs.harvard.edu/~salil>.

‡Partially supported by NSF grants CCR-9987845 and CCR-9987077.