On Pseudorandomness with respect to Deterministic Observers

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

Avi Wigderson
The Hebrew University, Jerusalem
and
The Institute for Advanced Study, Princeton
avi@math.ias.edu

May 4, 2000

Abstract

In the theory of pseudorandomness, potential (uniform) observers are modeled as *probabilistic* polynomial-time machines. In fact many of the central results in that theory are proven via probabilistic polynomial-time reductions. In this paper we show that analogous deterministic reductions are unlikely to hold. We conclude that randomness of the observer is essential to the theory of pseudorandomness.

What we actually prove is that the hypotheses of two central theorems (in the theory of pseudorandomness) hold unconditionally when stated with respect to *deterministic* polynomial-time algorithms. Thus, if these theorems were true for deterministic observers, then their conclusions would hold unconditionally, which we consider unlikely. For example, it would imply (unconditionally) that any unary language in $\mathcal{BPP}$ is in $\mathcal{P}$.

The results are proven using diagonalization and pairwise independent sample spaces.

Keywords: Pseudorandomness, Computational Difficulty, Derandomization, Unary Languages, Diagonalization, Pairwise Independent Sample Spaces.

*Supported by MINERVA Foundation, Germany.