Reducing the seed length in the Nisan-Wigderson generator*

Russell Impagliazzo†
Computer Science and Engineering
UC, San Diego
9500 Gilman Drive
La Jolla, CA 92093-0114
russell@cs.ucsd.edu

Ronen Shaltiel
Department of Computer Science
Weizmann Institute of Science
Rehovot 76100, Israel
ronens@wisdom.weizmann.ac.il

Avi Wigderson‡
Department of Computer Science
Hebrew University
Jerusalem, Israel
avi@cs.huji.ac.il

Abstract

The Nisan-Wigderson pseudo-random generator [NW94] was constructed to derandomize probabilistic algorithms under the assumption that hard functions exist. We give the first construction of a pseudo-random generator with optimal seed length that uses arbitrary hardness assumption (namely almost any superpolynomial circuit lower bound). Such generators were previously known only assuming exponential hardness [IW97, STV01].

The key is a new analysis of the NW-generator [NW94]. We show that it fails to be pseudo random only if a much harder function can be efficiently constructed from the given hard function. This leads to a new recursive generator, which may be viewed as a reduction from the general case of arbitrary hardness to the solved case of exponential hardness.

We also give the first construction of an extractor which uses optimal seed length, for random sources of arbitrary min-entropy. Thus, our construction is the first to use the optimal seed length for sub-polynomial entropy levels. It builds on the fundamental connection between extractors and pseudo-random generators discovered by Trevisan [Tre01], combined with the construction above. Using Kolmogorov Complexity rather than circuit size in the analysis of the extractor enables us to increase the number of bits extracted and extract a polynomial fraction of the initial randomness.

---
*This paper is the combination of two previous works [ISW99, ISW00] by the same authors.
†Research Supported by NSF Award CCR-9734911, Sloan Research Fellowship BR-3311, grant #93025 of the joint US-Czechoslovak Science and Technology Program, and USA-Israel BSF Grant 97-00188
‡This research was supported by grant number 69/96 of the Israel Science Foundation, founded by the Israel Academy for Sciences and Humanities and USA-Israel BSF Grant 97-00188