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
University of Haifa
Haifa 31905, Israel
ronen@cs.haifa.ac.il

Avi Wigderson§
Department of Computer Science
Institute for Advanced Study
Einstein Drive, Princeton, NJ 08540
avi@ias.edu

April 23, 2006

Abstract

The Nisan-Wigderson pseudo-random generator [NW94] was constructed to derandomize probabilistic algorithms under the assumption that there exist explicit functions which are hard for small circuits. We give the first explicit construction of a pseudo-random generator with asymptotically optimal seed length even when given a function which is hard for relatively small circuits. Generators with optimal seed length were previously known only assuming hardness for exponential size circuits [IW97, STV01].

We also give the first explicit construction of an extractor which uses asymptotically optimal seed length for random sources of arbitrary min-entropy. 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.

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. By repeatedly using this idea we get 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.

*This paper is based on two conference papers [ISW99, ISW00] by the same authors.

†Research Supported by NSF Award CCR-9734911, NSF Award CCR-0098197, Sloan Research Fellowship BR-3311, grant #93025 of the joint US-Czechoslovak Science and Technology Program, and USA-Israel BSF Grant 97-00188

‡Part of this work was done while at the Hebrew University and the Institute for advanced study.

§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