Near-Optimal conversion of Hardness into Pseudo-Randomness

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
Hebrew University
Jerusalem, Israel
ronens@cs.huji.ac.il

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

May 3, 1999

Abstract

Various efforts ([BFNW93, IW97, STV99]) have been made in recent years to derandomize probabilistic algorithms using the complexity theoretic assumption that there exists a problem in $E = dtime(2^{O(n)})$, that requires circuits of size $s(n)$, (for some function s). These results are based on the NW-generator [NW88]. For the strong lower bound $s(n) = 2^{\epsilon n}$, [IW97], and later [STV99] get the optimal derandomization, $P = BPP$. However, for weaker lower bound functions $s(n)$, these constructions fall far short of the natural conjecture for optimal derandomization, namely that $bptime(t) \subseteq dtime(2^{O(s^{-1}(t))})$. The gap in these constructions is due to an inherent limitation on efficiency in NW-style pseudo-random generators.

In this paper we are able to get derandomization in almost optimal time using *any* lower bound $s(n)$. We do this by using the NW-generator in a new, more sophisticated way. We view any failure of the generator as a reduction from the given "hard" function to its restrictions on smaller input sizes. Thus, either the original construction works (almost) optimally, or one of the restricted functions is (almost) as hard as the original. Any such restriction can then be plugged into the NW-generator recursively. This process generates many "candidate" generators - all are (almost) optimal, and at least one is guaranteed to be "good". Then, to perform the approximation of the acceptance probability of the given circuit (which is the key to derandomization), we use ideas from [ACR96]: we run a tournament between the "candidate" generators which yields an accurate estimate.

Following Trevisan, we explore information theoretic analogs of our new construction. Trevisan [Tre99] (and then [RRV99]) used the NW-generator to construct efficient extractors. However, the inherent limitation of the NW-generator mentioned above makes the extra randomness required by that extractor suboptimal (for certain parameters). Applying our construction, we show how to use a weak random souce with optimal amount of extra randomness, for the (simpler than extraction) task of estimating the probability of any event (which is given by an oracle).