Pseudorandom Generators in Propositional Proof Complexity

Michael Alekhnovich*, Eli Ben-Sasson†
Alexander A. Razborov‡, Avi Wigderson§

February 9, 2001

Abstract

We call a pseudorandom generator $G_n : \{0,1\}^n \to \{0,1\}^m$ *hard* for a propositional proof system P if P can not efficiently prove the (properly encoded) statement $G_n(x_1, \ldots, x_n) \neq b$ for *any* string $b \in \{0,1\}^m$. We consider a variety of "combinatorial" pseudorandom generators inspired by the Nisan-Wigderson generator on the one hand, and by the construction of Tseitin tautologies on the other. We prove that under certain circumstances these generators are hard for such proof systems as Resolution, Polynomial Calculus and Polynomial Calculus with Resolution (PCR).

*Moscow State University, Moscow, Russia mike@mccme.ru. Supported by INTAS grant # 96-753 and by the Russian Basic Research Foundation

†Institute of Computer Science, Hebrew University, Jerusalem, Israel. elli@cs.huji.ac.il.

‡Steklov Mathematical Institute, Moscow, Russia razborov@genesis.mi.ras.ru. Supported by INTAS grant # 96-753 and by the Russian Basic Research Foundation; part of this work was done while visiting Princeton University and DIMACS

§Institute for Advanced Study, Princeton, and Institute of Computer Science, Hebrew University, Jerusalem, avi@math.ias.edu. This research was supported by grant number 69/96 of the Israel Science Foundation, founded by the Israel Academy for Sciences and Humanities. Support for this research has been provided by The Alfred P. Sloan Foundation