In Search of an Easy Witness: Exponential Time vs. Probabilistic Polynomial Time

Russell Impagliazzo*
Department of Computer Science
University of California, San Diego
La Jolla, CA 92093-0114
russell@cs.ucsd.edu

Valentine Kabanets†
Department of Computer Science
University of California, San Diego
La Jolla, CA 92093-0114
kabanets@cs.ucsd.edu

Avi Wigderson‡
Department of Computer Science
Hebrew University
Jerusalem, Israel 91904
and
Institute for Advanced Study
Princeton, NJ 08540
avi@ias.edu

August 20, 2002

Abstract

Restricting the search space $\{0, 1\}^n$ to the set of truth tables of "easy" Boolean functions on $\log n$ variables, as well as using some known hardness-randomness tradeoffs, we establish a number of results relating the complexity of exponential-time and probabilistic polynomial-time complexity classes. In particular, we show that $NEXP \subset P/poly \Leftrightarrow NEXP = MA$; this can be interpreted as saying that *no* derandomization of MA (and, hence, of promise-BPP) is possible *unless* $NEXP$ contains a hard Boolean function. We also prove several downward closure results for $ZPP, RP, BPP,$ and MA; e.g., we show $EXP = BPP \Leftrightarrow EE = BPE$, where EE is the double-exponential time class and BPE is the exponential-time analogue of BPP.