

BPP has Subexponential Time Simulations unless $EXPTIME$ has Publishable Proofs

Laszlo Babai
Lance Fortnow
Noam Nisan
A. Wigderson

Abstract

We show that BPP can be simulated in subexponential time for infinitely many input lengths unless exponential time

- Collapses to the second level of the polynomial-time hierarchy,
- Has polynomial-size circuits and
- Has publishable proofs $(EXPTIME=MA)$.

We also show that BPP is contained in subexponential time unless exponential time has publishable proofs for infinitely many input lengths. In addition, we show BPP can be simulated in subexponential time for infinitely many input lengths unless there exist unary languages in $MA - P$.

The proofs are based on the recent characterization of the power of multiprover interactive protocols and on random self-reducibility via low degree polynomials. They exhibit an interplay between Boolean circuit simulation, interactive proofs and classical complexity classes. An important feature of this proof is that it does not relativize.

One of the ingredients of our proof is a lemma that states that if $EXPTIME$ has polynomial size circuits then $EXPTIME=MA$. This extends previous work by Albert Meyer.