Randomness vs. Time: De-randomization under a uniform assumption

Russell Impagliazzo
Avi Wigderson

Abstract

We prove that $BPP \neq EXP$, then every problem in BPP can be solved deterministically in sub-exponential time on almost every input (on every samplable ensemble for infinitely many input sizes). This is the first derandomization result for BPP based on uniform, non-cryptographic hardness assumptions. It implies the following gap in the average-instance complexities of problems in BPP: either these complexities are always sub-exponential or they contain arbitrarily large exponential functions.

We use a construction of a small “pseudorandom” set of strings from a “hard function” in EXP which is identical to that used in the analogous non-uniform results of [21,3]. However, previous proofs of correctness assume the “hard function” is not in $P/poly$. They give a non-constructive argument that a circuit distinguishing the pseudo-random strings from truly random strings implies that a similarly sized circuit exists computing the “hard function”. Our main technical contribution is to show that, if the “hard function” has certain properties, then this argument can be made constructive. We then show that, assuming $EXP \subseteq P/poly$, there are EXP-complete functions with these properties.