P=BPP Unless E has Subexponential Circuits: Derandomizing the XOR Lemma

Russell Impagliazzo
Avi Wigderson

Abstract
Yao showed that the XOR of independent random instances of a somewhat hard Boolean problem becomes almost completely unpredictable.

In this paper we show that, in non-uniform settings, total independence is not necessary for this result to hold. We give a pseudo-random generator which produces n instances of a problem for which the analog of the XOR lemma holds. Combining this generator with the results of [25, 6] gives substantially improved results for hardness vs. randomness trade-offs. In particular, we show that if any problem in $E = DTIME(2O(n))$ has circuit complexity $2(n)$, then $P = BPP$. Our generator is a combination of two known ones - the random walks on expander graphs of [1, 10, 19] and the nearly disjoint subsets generator of [23, 25]. The quality of the generator is proved via a new proof of the XOR lemma which may be useful for other direct product results.