

Pseudorandomness for Network Algorithms

Russell Impagliazzo

Noam Nisan

Avi Wigderson

Abstract

We define pseudorandom generators for Yao's two-party communication complexity model and exhibit a simple construction, based on expanders, for it. We then use a recursive composition of such generators to obtain pseudorandom generators that fool distributed network algorithms. While the construction and the proofs are simple, we demonstrate the generality of such generators by giving several applications.