abstract

Computer Science/Discrete Mathematics Seminar II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

One powerful theme in complexity theory and pseudorandomness in the past few decades has been the use of lower bounds to give pseudorandom generators (PRGs). However, the general results using this hardness vs. randomness paradigm suffer a quantitative loss in parameters, and hence do not give nontrivial implications for models where we only know lower bounds of a fixed polynomial. We show that when such lower bounds are proved using random restrictions, we can indeed construct PRGs which are essentially best possible without in turn improving the lower bounds.

More specifically, say that a circuit family has shrinkage exponent Gamma if a random restriction leaving a p fraction of variables unset shrinks the size of any circuit in the family by a factor of p^{Gamma}. Our PRG uses a seed of length roughly s^{1/(Gamma + 1)} to fool circuits in the family of size s. By instantiating this generic construction, we get PRGs for the following classes:

1) de Morgan formulas of size s, seed length s^{1/3}.

2) Formulas over an arbitrary basis, seed length s^{1/2}.

3) Branching programs of size s, seed length s^{1/2}.

The previous best PRGs known for these classes used seeds of length bigger than n/2 to output n bits, and worked only when the size s=O(n).

Joint work with Russell Impagliazzo and David Zuckerman.