abstract

Computer Science/Discrete Mathematics Seminar II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We present an iterative approach to constructing pseudorandom generators, based on the repeated application of mild pseudorandom restrictions. We use this template to construct pseudorandom generators for combinatorial rectangles and read-once CNFs and a hitting set generator for width-3 branching programs that achieve near-optimal seed-length even in the low error regime.

The (pseudo)random restrictions we use are milder than those typically used for proving circuit lower bounds, in that we only set a constant fraction of the bits at a time. While such restrictions do not simplify the functions drastically, we show that they can be derandomized using small-bias spaces.

Based on joint work with Raghu Meka, Omer Reingold, Luca Trevisan and Salil Vadhan.