abstract

COMPUTER SCIENCE/DISCRETE MATH II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Sipser and Gács, and independently Lautemann, proved in '83 that probabilistic polynomial time is contained in the second level of the polynomial-time hierarchy, i.e. BPP is in \Sigma_2 P. This is essentially the only non-trivial upper bound that we have on the power of probabilistic computation.

The Sipser-Gács-Lautemann simulation incurs a quadratic blow-up in the running time (i.e., BPTime(t)in \Sigma_2 Time(t2)). In this talk we show that this quadratic blow-up is in fact necessary for black-box simulations, such as those of Sipser, Gács, and Lautemann.

To obtain this result, we prove a new circuit lower bound for computing approximate majority, i.e. computing the majority of a given bit-string whose fraction of 1's is bounded away from 1/2: We show that small depth-3 circuits for approximate majority must have bottom fan-in Omega(log n).

On the positive side, we show a quasilinear time simulation of probabilistic time at the third level of the polynomial-time hierarchy (i.e. BPTime(t) in \Sigma_3 Time(t polylog t)).
If time permits, we will discuss some applications of our results to proving lower bounds on space-bounded randomized machines.