

abstract

SPECIAL COMPUTER SCIENCE/DISCRETE MATH SEMINAR, III

Topic:

Speaker:

Affiliation:

Date:

Time/Room:

A randomness extractor is an algorithm which extracts randomness from a low-quality random source, using some additional truly random bits. Extractors have proved useful in a variety of seemingly unrelated areas. We construct new extractors which require only $\log n + O(1)$ additional random bits for sources with constant entropy rate. A similar construction allows us to derandomize the results of Hastad and Feige-Kilian and show that approximating Clique and Chromatic Number to within $n^{1-\epsilon}$ are NP-complete, for any $\epsilon > 0$.

Our constructions rely on recent results in additive number theory and extractors by Bourgain-Katz-Tao, Barak-Impagliazzo-Wigderson, Barak-Kindler-Shaltiel-Sudakov-Wigderson, and Raz. We also simplify and slightly strengthen key lemmas in the second and third of these papers.