abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

A theorem of Green, Tao and Ziegler can be stated (roughly) as follows: if R is a pseudorandom set, and X is a dense subset of R, then there is a "model" Y for X such that Y is a dense set and X and Y are indistinguishable. (The precise statement refers to "measures" or distributions rather than sets.) The proof is very general, and it applies to notions of pseudorandomness and indistinguishability defined in terms of any family of adversaries. The proof proceeds via iterative partitioning and an energy increment argument, in the spirit of the proof of the weak Szemeredi regularity lemma. The "reduction" involved in the proof has exponential complexity in the distinguishing probability

We present a new proof inspired by Nisan's proof of the Impagliazzo hard core set theorem. The reduction in our proof has polynomial complexity in the distinguishing probability and provides a new characterization of the notion of "pseudoentropy" of a distribution.

Following the connection between this theorem and the Impagliazzo hard core set theorem in the opposite direction, we present a new proof of the Impagliazzo hard core set theorem via iterative partitioning and energy increment. While our reduction has exponential complexity in some parameters, it has certain consequences that do not seem to follow from known proofs.

Finally, if time allows we will present a proof (which is folklore in the arithmetic combinatorics literature) that the Szemeredi regularity lemma applies to dense subgraphs of sparse expanders, a related instantiation of the principle that dense subsets of pseudorandom objects "behave like" truly dense objects.

This is joint work with Omer Reingold, Madhur Tulsiani and Salil Vadhan