abstract

COMPUTER SCIENCE/DISCRETE MATH SEMINAR, II
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

The links between propositional proof systems and bounded arithmetic (a generic name for a collection of first-order theories of arithmetic) have many facets but informally one can view them as two sides of the same thing: The former is a non-uniform version of the latter. In particular, it is known that proving lengths-of-proofs lower bounds for propositional proof systems is very much related (even equivalent, when formulated properly) to constructing models of bounded arithmetic. This offers a very clean and coherent framework for thinking about lengths-of-proofs lower bounds.

I shall describe a new method for constructing relevant bounded arithmetic models, and hence for lengths-of-proofs lower bounds. I will attempt to specialize this to proof complexity without going (explicitly) through bounded arithmetic. The models are Boolean-valued and are built from random variables. Some of the models appear interesting in their own right but we interpret the construction primarily as a method that reduces a lengths-of-proofs lower bound to a purely combinatorial/complexity-theoretic statement about a family of random variables samplable in a particular way. In the talk I will put emphasis on this aspect of the method.