abstract

COMPUTER SCIENCE DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Any proof of P!=NP will have to overcome two barriers: relativization and natural proofs. Yet over the last decade, we have seen circuit lower bounds (for example, that PP does not have linear-size circuits) that overcome both barriers simultaneously. So the question arises of whether there is a third barrier to progress on the central questions in complexity theory.

In this talk we present such a barrier, which we call "algebraic relativization" or "algebrization." The idea is that, when we relativize some complexity class inclusion, we should give the simulating machine access not only to an oracle A, but also to the low-degree extension of A over a finite field or ring.

We systematically go through basic results and open problems in complexity theory to delineate the power of the new algebrization barrier. We first show that all known non-relativizing results -- both inclusions such as IP=PSPACE and MIP=NEXP, and separations such as MA-EXP not in P/poly -- do indeed algebrize. We next show that most open problems -- including P versus NP, P versus BPP, and NEXP versus P/poly -- will require non-algebrizing techniques, of which we currently have not a single example. In some cases algebrization seems to explain exactly why progress stopped where it did: for example, why we have superlinear circuit lower bounds for PromiseMA but not for NP.

We also exhibit a surprising connection between algebrization and communication complexity. Using this connection, we give an MA-protocol for the Inner Product function with O(sqrt(n) log(n)) communication (essentially matching a lower bound of Klauck), and describe a pure communication complexity conjecture whose truth would imply P!=NP.