abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

Razborov and Rudich have shown that so-called natural proofs are not useful for separating P from NP unless hard pseudorandom number generators do not exist. This famous result is widely regarded as a serious barrier to proving strong lower bounds in circuit complexity theory.

By definition, a natural combinatorial property satisfies two conditions, constructivity and largeness. Our main result is that if the largeness condition is weakened slightly, then not only does the Razborov-Rudich proof break down, but such "almost-natural" (and useful) properties provably exist. Specifically, under the same pseudorandomness assumption that Razborov and Rudich make, a simple, explicit property that we call "discrimination" suffices to separate P/poly from NP; discrimination is nearly linear-time computable and almost large, having density 2^(-q(n)) where q grows slightly faster than a quasi-polynomial function.

The discrimination property is not only constructive, but may also be regarded as a minor alteration of a property of a random function. Thus our result suggests that it may be worth revisiting the old hope that NP can be separated from P/poly using a constructive property of a random function in some sense.