Proofs for Algorithms, Algorithms from Proofs

Abstract:

The interplay between **algorithms** and **proofs** has been one of the most fascinating and fruitful themes in theoretical Computer Science. In this talk I will describe a different connection between these two concepts - a general methodology for algorithm design using an automatic transformation of a proof into an algorithm. This methodology yields a systematic way to design and analyze algorithms across many domains. In particular we and others have used it for problems in combinatorial optimization, machine learning, and quantum information theory, and it shows promise for making progress on important open questions such as settling Khot’s Unique Games Conjecture. I will demonstrate this methodology by presenting an algorithm for the Sparse Coding / Dictionary Learning problem that handles much more general inputs than was known before, and an algorithm for the Unique Games problem that can solve all the previously known candidate hard instances. Key to our approach is the notion of "pseudo-distributions", which are objects that are emphatically different than actual distributions but behave like them in the eyes of low degree polynomials. We use these pseudo-distributions to "lift" a proof into an algorithm via the Shor-Parrilo-Lasserre "Sum-of-Squares" semidefinite programming hierarchy. The talk will be based on several joint works with (varying subsets of) Fernando Brandao, Aram Harrow, Jonathan Kelner, David Steurer and Yuan Zhou.