The mechanism design approach to interactive proofs

Abstract:

The model of interactive proofs, introduced nearly two and a half decade, is now increasingly widely being used to design computation-outsourcing protocols. In an interactive proof, an honest party interacts with powerful but strategic provers, to elicit from them the correct answer to a computational question. Classical interactive proofs assume that the provers are adversarial (i.e., they want to mislead the verifier) and cooperative (work together as a team).

In this talk, I will present my work on a new payment-based interactive-proof system, called rational proofs. In rational proofs, the provers are not adversarial but rational, that is, they want to maximize the payment received from the verifier. Using principles from mechanism design, I will show how these payments can be used to leverage correctness from multiple provers who are either cooperative or non-cooperative in nature. I will also present how the guarantees of rational proofs are related to the soundness and completeness guarantees of classical interactive proofs.

Bio: Shikha Singh is currently an Assistant Professor of Computer Science at Wellesley College and will be joining Williams College as an Assistant Professor in Fall 2019. She obtained her PhD in Computer Science from Stony Brook University and her Integrated MSc. in Mathematics and Computing from IIT Kharagpur. Her broad research interests include algorithmic game theory, algorithms and data structures for big data, and complexity theory.