abstract

Computer Science/Discrete Mathematics Seminar I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

In many distributed systems, the cost of computation is dominated by the cost of communication between the machines participating in the computation. Communication complexity is therefore a very useful tool in understanding distributed computation, and communication complexity lower bounds have been used extensively to obtain lower bounds on various distributed problems. However, almost all applications of communication complexity lower bounds in distributed computing use two-party lower bounds, despite the fact that distributed computation usually involves many players. Unfortunately, there are interesting distributed problems that it appears cannot be addressed using two-player lower bounds, because reductions from two-player problems seem to lose the "hardness" of the problem. I will give a few examples in the talk.

With this motivation in mind, in this work we study communication complexity in the multi-party message-passing model, which has been extensively used in distributed computing and in secure multi-party computation. In the message-passing model there are k players, each with a private n-bit input, and the players communicate with each other over private channels. We show a lower bound of Omega(n*k) on the communication complexity of set disjointness in the message-passing model. To obtain this bound we develop information complexity tools for the model, prove a direct-sum theorem, and show that the information complexity of computing a 1-bit AND with k players is Omega(k).

This is joint work with Mark Braverman, Faith Ellen, Toniann Pitassi and Vinod Vaikuntanathan.