abstract

Computer Science/Discrete Mathematics Seminar I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We study a new type of proof system, where an unbounded prover and a polynomial time verifier interact, on inputs a string x and a function f, so that the Verifier may learn $f(x)$. The novelty of our setting is that there no longer are ``good" or ``malicious" provers, but only rational ones. In essence, the Verifier has a budget c and gives the Prover a reward $r \in [0,c]$ determined by the transcript of their interaction; the prover wishes to maximize his expected reward; and his reward is maximized only if he the verifier correctly learns $f(x)$.

Rational proof systems are as powerful as their classical counterparts for polynomially many rounds of interaction, but are much more powerful when we only allow a constant number of rounds. Indeed, we prove that if $f \in \#P$, then f is computable by a one-round rational Merlin-Arthur game, where, on input x, Merlin's single message actually consists of sending just the value $f(x)$. Further, we prove that CH, the counting hierarchy, coincides with the class of languages computable by a constant-round rational Merlin-Arthur game.

Our results rely on a basic and crucial connection between rational proof systems and proper scoring rules, a tool developed to elicit truthful information from experts.