abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

I will discuss the following two results. I will assume no prior knowledge of quantum information or the PCP theorem.

1) The membership of x in SAT (for x of length n) can be proved by a logarithmic-size quantum state Ψ, together with a polynomial-size classical proof consisting of blocks of length $polylog(n)$ bits each, such that after measuring the state Ψ a verifier only needs to read ONE of the blocks of the classical proof.

This shows that if a short quantum witness is available then a (classical) PCP with only one query is possible.

2) The class $QIP/qpoly$ contains ALL languages. That is: for any language L (even non-recursive), the membership of x in L (for x of length n) can be proved by a polynomial-size quantum interactive proof, where the verifier is a polynomial-size quantum circuit with working space initiated with
some quantum state $\Psi(L,n)$ (depending only on L and n).

The interactive proof that we give is of only one round, and the messages communicated are classical. The advice $\Psi(L,n)$ given to the verifier can also be replaced by a classical probabilistic advice, as long as this advice is kept as a secret from the prover.

The second result can hence be interpreted as: The class $IP/rpoly$ contains all languages.

For the proof of the second result, we introduce the "quantum low-degree-extension" of a

string of bits. The first result requires an additional machinery of "quantum low-degree-test".