Speaker: Greg Kuperberg
Title: A subexponential-time quantum algorithm for the dihedral hidden subgroup problem

Abstract: The most exciting aspect of quantum complexity theory is the possibility of an exponential speedup over classical randomized computation. Grover's search algorithm offers a quadratic speedup for an arbitrary combinatorial search, but exponential speedup is much rarer. All known examples to date are closely related to Shor's period-finding algorithm, which among other things can be used to factor numbers in quantum polynomial time.

One interesting next case is the dihedral hidden subgroup problem. This is equivalent to the hidden shift problem, in which the task is to find, given black-box functions $f$ and $g$ on $\mathbb{Z}/N$, the shift $s$ in a promised relation $f(x) = g(x+s)$. The classical query complexity for this problem is $O(\sqrt{N})$. I will discuss a quantum algorithm with time and query complexity $2^{\alpha}(\sqrt{\log(N)})$. This is not polynomial in $\log(N)$, but it is subexponential.

---------------------------------------------------------------