ROBERT RAUSSENDORF, University of British Columbia, Department of Physics and Astronomy, 6224 Agricultural Road, Vancouver, BC, V6T 1Z4

Graph Theory and the hardness of classical simulation of quantum computation

Using the laws of quantum mechanics for computation leads to exponential savings in computational cost and run-time. The best known example is Shor's algorithm for factoring numbers, which breaks the RSA crypto system. But which quantum mechanical property causes this speed-up? We approach this question by investigating circumstances under which the speedup vanishes, namely when a quantum computation becomes efficiently simulatable on a classical computer.

To date, three techniques for the efficient simulation of special classes of quantum computations are known:

(1) the Stabilizer formalism,

(2) the fermionic/matchgate method, and the tensor contraction method.

It turns out that, through the framework of measurement-based quantum computation (MQC), all of them have a connection with graph theory. I briefly review these methods and then show that measurement-based quantum computation on a graph state $|G>$ can be simulated by the matchgate method if and only if G is a circle graph.

Joint work with Jim Geelen (UW), Chris Godsil (UM) and Maarten van den Nest (MPI for Quantum Optics, Garching, Germany).