DALHOUSIE MATHEMATICS COLLOQUIUM

Thursday April 5, 2:30 pm, Chase 319
Speaker: Peter Selinger
(Dalhousie University)

Number-Theoretic Methods in Quantum Computing

An important problem in quantum computing is the so-called approximate synthesis problem. In this problem, we are given a fixed finite set of unitary operators (called gates) spanning a dense subgroup of $PSU(2)$. Given a target operator U, the goal is to find a word in the generators (called a circuit), preferably as short as possible, that approximates U up to a given accuracy ϵ. For nearly two decades, the standard solution to this problem was the Solovay-Kitaev algorithm, which is based on geometric ideas. This algorithm produces circuits of size $O(log^c(1/\epsilon))$, where c is a constant approximately equal to 3.97. It was a long-standing open problem whether the exponent c could be reduced to 1.

In the last few years, a new class of efficient algorithms has emerged that achieve circuit size $O(log(1/\epsilon))$, thereby answering the above question positively. These new algorithms are based not on geometry, but on number theory. In certain important cases, such as the commonly used Clifford+T gates, one can even find algorithms that are optimal, i.e., they always find the shortest possible sequence of gates. I will give an overview of these developments, which have already reduced the resources required for (future) practical quantum computation by at least 2-3 orders of magnitude.