Abstract

Exponential Speedups and Limitations of Quantum Computation

PI: Sean Hallgren, Pennsylvania State University

The PI proposes to find problems where quantum computers have an exponential advantage over classical computers, and also to understand in which cases this is not possible. The main focus will be on finding efficient quantum algorithms for lattice problems. This is a fundamental class of problems in computer science that has been studied extensively classically and also in the context of quantum computation for more than 20 years, and it remains an open problem. Lattice problems are currently being proposed in cryptography for post-quantum cryptography based on the fact that there are several versions for which no quantum algorithm has been found, yet. Determining whether or not there are efficient quantum algorithms for these problem, the goal of this proposal, is crucial for secure encryption in the future.

The approach will be to explore the rich set of lattices that come from number theoretic constructions. Rather than only trying a few cases and then changing research problems, a longer term study of the problems will be carried out. Techniques in quantum algorithms can be tried and developed based on the computational problems that are discovered. The PI's recent quantum algorithm for computing the unit group of a number field led to an efficient quantum algorithm for the first special case of a lattice problem. This provides the starting point for this proposal.

The outcome of the proposed project with the biggest impact would be efficient quantum algorithms for lattice problems. Success in finding such algorithms would be a major advance in the field of quantum algorithms, with new techniques and fundamental insights required. Part of the impact would be to disrupt post-quantum cryptography, as it would eliminate one of the main candidates for replacing factoring and discrete-log based systems with systems resistant to quantum computers. It would also fundamentally advance the field of quntum algorithms. Another potential outcome would be to develop formal evidence that lattice problems do not have efficient quantum algorithms. The proposed research is high risk, and the likely outcome would be not finding an algorithm. For this reason there is usually little incentive to spend the required amount of time and effort to determine if an algorithm exists or not. The time frame and funding levels of the VBFF are an ideal fit for attacking this very important problem in quantum computing.