Quantum algorithms for algebraic problems

Ashwin Nayak (University of Waterloo and Perimeter Institute)
Leonard Schulman (California Institute of Technology)
John Watrous (University of Calgary)

Sept. 16–23, 2006

1 Overview

Quantum computers are computational devices that are based on principles of quantum mechanics. Phenomena such as superposition—the ability to exist in several states simultaneously, and interference—the ability of different computation paths to combine constructively as well as destructively, allow quantum computers a much broader range of operations than possible with current computers, which are based on the laws of classical physics. The potential of quantum devices to outperform current computers was rigorously demonstrated by Bernstein and Vazirani in 1993. Since then, efficient quantum algorithms have been discovered for a number of important problems, including integer factorization and the discrete logarithms. No efficient (polynomial-time) classical algorithms are known for these problems. In fact, cryptosystems such as RSA, whose security rests upon the computational intractability of factorization and discrete logs, are in widespread use.

Quantum computers seem to be especially effective in solving problems with a group-theoretic flavour. The aim of the proposed meeting is to develop new techniques that will allow us to tackle some outstanding questions concerning algebraic problems such as Graph Isomorphism, and Closest Lattice Vector. These problems are of complexity in between P and NP, and are considered candidates for efficient quantum algorithms. Some of these problems are also the basis of classical cryptosystems believed to be more secure than RSA. The possibility of cryptosystems secure against quantum computers hinges crucially on the quantum complexity of the underlying problems.

2 Objectives

The meeting planned to focus on quantum algorithms and complexity theory issues surrounding algebraic problems such as Graph Isomorphism, and Closest Lattice Vector.

2.1 Graph Isomorphism

Originally motivated by problems in chemistry, the Graph Isomorphism (GI) has become a central problem in classical computation. Given two undirected graphs on the same set of (say N) vertices, the problem asks if there is a permutation of the vertices that maps the edges of one graph to exactly the edges of the second. The best known classical algorithm for GI is superpolynomial in N, yet for compelling complexity-theoretic reasons, it is believed not to be NP-complete.

GI reduces to the Hidden Subgroup Problem (HSP), which generalizes integer factorization, discrete logs, and a number of other group-theoretic problems. Efficient quantum algorithms for HSP are known when the base group is abelian. The non-abelian case remains largely unsolved, and is the subject of active research in quantum computation, largely because it includes Graph Isomorphism as a particular instance.

The most fruitful approach to solving HSP has been via creating "coset states", which are uniform superpositions over cosets of the "hidden subgroup". In the case of GI, the hidden subgroup is an order two subgroup of S_N wreath product S_2, if there is an isomorphism between the two graphs, and and is trivial otherwise. A general result due to Ettinger et al. shows that $O(NlogN)$ coset states suffice to distinguish between the two cases, and in fact to find a generating set for the subgroup. However, it takes exponential time to process the coset states. Work over the past year reveals an inherent weakness of this approach [Moore et al. 05, Hallgren et al. 05]: not only are $Omega(NlogN)$ coset states necessary, but any measurement of the states that extracts useful information is necessarily entangled across all the states. In other words, independent measurements of the states (as was possible in the abelian case) are futile.

The meeting set out to alternatives to the standard coset state approach for efficiently solving Graph Isomorphism. An approach completely orthogonal to this, but possibly less daunting, would be to place Graph Non-Isomorphism in the complexity class QMA (the quantum analogue of NP).

2.2 Lattice problems

A lattice is an additive subgroup of R^N, generated by all integer linear combinations of a basis of linearly independent vectors. Many seemingly unrelated problems in mathematics and computation can be recast in terms of lattices, e.g., integer programming, polynomial factorization, and integer factorization. Computational problems related to lattices have the feature that random instances of the problem (according to specific distributions) are at least as hard as the worst case instance. This makes them ideal candidates for building cryptographic schemes (and a number of such schemes have been proposed [Ajtai and Dwork'03, Regev'04]).

The Shortest Vector problem (SVP) asks for the shortest non-zero vector in the lattice generated by a basis for R^N (in the Euclidean norm). The Closest Vector Problem (CVP) asks for the lattice point that is closest (in Euclidean norm) to a given vector in R^N. Both these problems have been studied extensively, and are known to be NP-hard. The best classical algorithm for SVP runs in time $2^O(N)$, and the best polynomial time algorithms for either problem only approximate the solution to within exponential factors. Approximation to within polynomial factors are possible via constant round interactive proofs, even co-NP proofs, and such approximation is believed not to be NP-hard.

A number of connections have been established between quantum computation and lattice problems. The first reduces approximation of SVP to an instance of the Hidden Subgroup Problem (mentioned above) over the dihedral group. The second uses quantum algorithms to reduce worst case instances of SVP to average case instances of "learning with error". Perhaps the most interesting connections are the upper bounds on the quantum and classical complexity of approximating SVP and CVP [Regev and Aharonov'03-04]. While we do not yet have efficient quantum algorithms for approximating these problem to within polynomial factors, it has was shown that approximation to within $\sqrt{N}$ is in QMA (the quantum analogue of the complexity class NP). Moreover, using the insights gained from this work, the result was improved to show that such approximation is also possible with *classical* proofs, i.e., in NP.

We would like to further investigate connections of lattices with quantum computation. In particular, we would like to study the extent to which SVP and CVP can be approximated in quantum polynomial time, or with quantum proofs. We suspect that there are further lessons for classical algorithms to be learnt from investigating these problems with techniques from quantum computation.

2.3 Other group theoretic problems

To date, the hidden subgroup problem has dominated research efforts devoted to quantum algorithms for computational problems in groups. While (as described above) there are good reasons for this focus, there are other natural types of problem in groups, for which, for some of the same reasons, it is reasonable to search for an efficient quantum algorithm. The workshop was to be a useful venue for exploring some of these problems and the means with which one might approach them.

3 Proceedings of the meeting

3.1 Schur tranform: Andrew Childs

Andrew Childs presented work on using the Schur transform to distinguish coset states in the standard approach to the hidden subgroup problem (joint work with Aram Harrow and Pawel Wocjan, quant-ph/0609110, to appear in STACS 2007). This transform exploits the permutation symmetry of many copies of the coset state, decomposing the global state into subspaces labeled by partitions. Andrew explained why simply measuring the partition (”weak Schur sampling”) provides very little information about the hidden subgroup. In fact, even a combination of weak Fourier sampling and weak Schur sampling fails to identify the hidden subgroup. He also explained how the problem is connected to a quantum version of the collision problem, and used this connection to prove tight bounds on how many coset states are required to solve the hidden subgroup problem by weak Schur sampling.

During the workshop, Andrew made some progress on extending these tight bounds to cover the case of weak Fourier-Schur sampling.

3.2 Hidden quadratic structures: Leonard Schulman

Leonard Schulman described a class of algebraic problems which might be amenable to solution by quantum computers in spite of being hard for classical computers. In this class of problems the input is a mixture of superpositions, each of which is uniform over the roots of a particular multivariate finite-field quadratic equation. Two instantiations Leonard discussed are: (a) The quadratic is a sphere of unknown radius, and the mixture is over all translates of this sphere; the problem is to determine the radius. (b) The quadratic is an axis-parallel ellipsoid of unknown eccentricity, and the mixture is over all scalings of the ellipsoid; the problem is to determine the eccentricity.

In working sessions during the workshop, several participants suggested promising variants of the problem, and there was much brainstorming about various attacks (e.g., quantum random walks). Also during the workshop, Andrew Childs was able to obtain numerical evidence in support of the conjecture that the sphere problem is (at least information-theoretically) amenable to solution by quantum computers.

After the workshop, Umesh Vazirani, Childs and Schulman continued work on this class of problems and were able to prove that quantum computers can solve various cases of it. Childs will be giving a presentation on this work at QIP (Quantum Information Processing) 2007, and a paper is in the writing stages.

3.3 Open problem session: John Watrous

John Watrous discussed two open problems in quantum computation. The problems were not new – the intention was to take a fresh look at interesting problems in the light of more recently developed techniques.

The first problem asks whether or not it is possible to compute the greatest common divisor of two positive integers using a logarithmic or poly-logarithmic depth quantum circuit. The analogous question for classical circuits is a long-standing open question in theoretical computer science. The fact that the quantum Fourier transform can be performed using logarithmic depth quantum circuits (Cleve and Watrous, FOCS 2000) might be a useful tool for addressing this problem.

The second problem concerned the quantum complexity of the Group Order problem. In this problem, one is given generators of a finite group along with a means to compute products and inverses. The black-box group model reflects this situation. The goal of the problem is to compute the order (or size) of the generated group. This is a candidate for a difficult computational problem even for quantum computers – although the Abelian case is easily handled using Shor’s algorithm, thus far quantum algorithms are of little help in the non-Abelian case. The question is this: is the problem in QMA? In other words, is it possible to prepare a quantum state that, although not necessarily efficiently preparable, could efficiently convince someone with a quantum computer that the order of a given group was some given value N?

3.4 Quantum one-way functions: Umesh Vazirani

Umesh Vazirani discussed recent work done by himself along with Cris Moore and Alex Russell on quantum one-way functions. The goal is to find a function that can be efficiently computed in the forward direction by a classical computer, but which is difficult to invert even using a quantum computer. Such functions have potential to be very important in cryptographic applications when security is required against adversaries having quantum computers. The specific class of functions that was proposed is related to the notorious hidden subgroup problem that has frustrated quantum algorithm designers for several years. In this case, however, the difficulty of the Hidden Subgroup problem is beneficial, because the difficulty of inverting a given function is closely related to solving instances of the problem.

A paper describing these results has recently appeared on the quant-ph preprint archive.

3.5 Two quantum algorithms: Ashwin Nayak

Ashwin Nayak presented two works, one on the use of quantum walks in search algorithms (by Frederic Magniez, A.N., Jeremie Roland, and Miklos Santha), and the other on the learnability of quantum states (by Scott Aaronson).

There are several ways of devising quantum processes analogous to random walks, and these have been used fairly successfully in designing search type algorithms. The algorithms extend the search technique due to Grover to “structured databases” and provide polynomial speed-up over the best classical algorithms. Ashwin described a quantum walk based algorithm that may be defined for an arbitrary ergodic Markov Chain. It combines the benefits of two previous approaches (due to Ambainis and Szegedy, 2004) while guaranteeing the better form of run time. Ashwin also pointed out an open question regarding the speed-up in hitting time achievable by considering the quantum analogue of a non-reversible Markov chain. The question asks if a certain “discriminant matrix” has singular value gap that is significantly larger than the eigenvalue gap of the Markov chain.

The work due to Aaronson may be seen as the poor man’s version of quantum state tomography. State tomography involves estimating the exponentially many variables that determine the state of a quantum system. Often we are more interested in the outcome of making a certain measurement on a quantum state, rather than in explicitly knowing the entire state. A typical example is in the setting of a two-party communication protocol, where the parties wish to compute a bivariate function f(x,y) by sending only one message. Here, a quantum state encoding one input is sent as the message. In a classical simulation of the protocol, we may avoid sending the exponential size description of the message, since the other party need only recover the result of the measurement made on input y. Aaronson showed how a polynomial number of observations may be used to form a reasonable hypothesis on the state. The hypothesis would allow outcomes of typical measurements to be predicted correctly with high probability.

3.6 Closest vector problem: Niel de Beaudrap

Niel de Beaudrap discussed the possible use of Gaussian states over lattices in algorithms for the closest vector problem (CVP). The problem asks for the lattice point that is closest (in Euclidean norm) to a given vector in R^N. Gaussian states have occurred in most recent results on quantum and classical algorithms (or interactive proofs) for lattice problems and in cryptosystems based on lattices. Niel described a quantum algorithm that is in a limited sense, a worst case to average case reduction. This was used by Aharonov and Regev in a polynomial-time classical algorithm for the $\sqrt{N}$-gap CVP with pre-processing. During the meeting, Niel and Ashwin Nayak identified the key difficulties in converting the reduction to a full-fledged polynomial-time algorithm for $\sqrt{N}$-Gap-CVP. Work on the problem is still under way.