Computer Science Project: Report 2010-2011

I. GROUP MEMBERS AND VISITORS

The composition of the group:

1. Principal Investigators : Rahul Jain, Hartmut Klauck (since April 2010), Miklos Santha.

2. Post-docs : Thomas Decker (will stay one more year), Matthew McKague (since July 2010, will stay two more years). Sarvagya Upadhyay will join us in September, 2011. Recently we have made offer to Carlos A. Perez-Delgado.

3. Ph.D students : Attila Pereszlenyi, Ved Prakash (since August 2010), Penghui Yao.

4. Visiting Researchers : Joe Fitzsimons (since 2010), Peter Hoyer (stayed six months), Gabor Ivanyos (regularly two months per year), Iordanis Kerenidis (regularly two months per year), Troy Lee (started July 2010 and will stay one more year), Ashwin Nayak (stayed two months), Mario Szegedy (stayed three months), Shengyu Zhang (regularly two months per year).

II. RESEARCH

A. Summary of achievements

1. Algorithms and Complexity

1. In the usual model of quantum query complexity, one tries to evaluate a function $f(x)$ by making as few queries to the input x as possible. Looking at the evolution of a successful algorithm, it begins in some fixed state $|0\rangle$ and evolves to a state close to $|f(x)\rangle|0\rangle$. In the more general state-conversion problem, an algorithm begins in a state $|\sigma_x\rangle$, which can depend on the input x, and tries to convert this into a target state $|\rho_x\rangle$, again by making as few queries to the input as possible. We characterized the quantum query complexity of the state-conversion problem in terms of a metric that measures the distance between the set of initial and target states. This metric is closely related to the adversary bound in the functional case, and is defined in terms of a norm which generalizes the Schur-product operator norm. One consequence of this characterization is that the discrete and continuous query models are equivalent up to constant factors, even for the general state-conversion problem.

2. Recursive Majority-of-three (3-Maj) is a deceptively simple problem in the study of randomized decision tree complexity. The precise complexity of this problem is unknown, while that of the similarly defined Recursive NAND tree is completely understood. We revisited 3-Maj with the goal of understanding the nature of randomized algorithms. We proved a lower bound of $(1-2\epsilon)(5/2)^h$ for ϵ-bounded error randomized algorithms for evaluating a height h formula. This improves over the best known bound of $(1-2\epsilon)(7/3)^h$ due to Jayram, Kumar, and Sivakumar (2003). We also presented a zero-error randomized algorithm with complexity roughly 2.649^h, where the previous best bound was roughly 2.656^h. These improvements are obtained by extending the techniques due to Jayram et al. in novel ways. It is worth noting that the complexity of 3-Maj in the quantum analogue of the model is also well-characterized. Our work illustrates that unlike the quantum algorithm for the problem and the classical one for Recursive NAND, the optimal randomized algorithm for 3-Maj is unlikely to have a simple recursive structure.

3. We developed efficient quantum algorithms for several black-box problems related to hidden polynomial functions. To achieve this we defined and analyzed on a more abstract level the Hidden Symmetry Subgroup Problem (HSSP), which is a generalization of the well-studied Hidden Subgroup Problem (HSP). We developed a general method for reducing the HSSP to the HSP, which works efficiently in several cases. Based on this method, we obtained the first efficient quantum algorithm for the hidden polynomial problem for multivariate quadratic polynomials over fields of constant characteristic. We also applied the new methods

to polynomial function graph problems and obtained an efficient quantum procedure for constant degree multivariate polynomials over any field, which improved previously known algorithms in several ways.

We also developed a quantum algorithm for solving the HSP in the general linear group over a finite field where the hidden subgroup is promised to be a conjugate of the group of the invertible lower triangular matrices. The complexity of the procedure is polynomial when the size of the base field is not much smaller than the degree. This appears to be the first efficient hidden subgroup algorithm in almost simple groups of non-constant rank.

4. We gave a construction for a self–test for any connected graph state. In other words, for each connected graph state we gave a set of non–local correlations that can only be achieved (quantumly) by that particular graph state and certain local measurements. The number of correlations considered is small, being linear in the number of vertices in the graph. We also prove robustness for the test.

2. Interactive Proofs, Zero Knowledge, Quantum Games

1. In recent paper titled "QIP = PSPACE", we have settled a long standing open question in this area and have shown that Quantum Interactive Proofs possess exactly the same power as Classical Interactive Proofs. The holy grail in this area has been found ! This work further asserts the robustness of the complexity class PSPACE (= IP). This work is a natural successor of the previous work titled "Two-message quantum interactive proofs are in PSPACE" in which we showed that two-message Quantum Interactive Proofs possess no extra power over Classical Interactive Proofs. This was already a significant step forward towards settling the main question since three-message Quantum Interactive Proofs capture the entire power of QIP. In a related work which can be considered first in this series of work titled, "Parallel approximation of non-interactive zero-sum quantum games", we had shown that QRG(1), which is the class of problems having a single message Two-Competing Provers Quantum Protocol is contained in PSPACE. The main technique used in all of the above work is to present fast parallel algorithms for different classes of semi-definite programs and this helps to obtain containment of respective classes inside PSPACE. In a recent paper titled "A fast parallel algorithm for positive semi-definite programming", we have provided a fast parallel algorithm for solving positive semi-definite programs (without any width constraints). These are an important sub-class of semi-definite programs with applications in Optimization, Approximation and Quantum Computing.

2. Coin flipping is a fundamental cryptographic primitive that enables two distrustful and far apart parties to create a uniformly random bit [Blu81]. The previously best-known quantum protocol by Ambainis achieved a cheating probability of at most 3/4 [Amb01]. On the other hand, Kitaev showed that no quantum protocol can have cheating probability less than $1/\sqrt{2}$ [Kit03]. In the paper titled "Optimal quantum strong coin flipping" as above, we close this gap by presenting a quantum strong coin flipping protocol with cheating probability arbitrarily close to $1/\sqrt{2}$.

3. In a celebrated paper, Valiant and Vazirani raised the question of whether the difficulty of NP-complete problems was due to the wide variation of the number of witnesses of their instances. They gave a strong negative answer by showing that distinguishing between instances having zero or one witnesses is as hard as recognizing NP, under randomized reductions. We consider the same question in the quantum setting in the paper titled "On the power of unique quantum witness", and show that in the complexity class QMA (the quantum analogue of NP) polynomially many witnesses can be reduced to a unique witness.

   Future Work: The question of comparison of the powers of Quantum Multi-Prover Proof System and Classical Multi-Prover Proof systems is still open. Many interesting questions related to Quantum Zero-Knowledge are planned to be explored. The role of entanglement in Quantum Communication and Quantum Games is very poorly understood.

3. Communication Complexity, Query Complexity and other aspects of Communication

1. Direct Sum and Direct Product results in different models and settings of communication complexity have been shown. They roughly state that the resources required for computing k-copies together are k-times the resources required for one instance of the problem. In recent work "New strong direct product results in communication complexity" we have settled the direct product conjecture in the affirmative for all relations in the one-way public-coin model of classical communication complexity. We have also provided a new direct product result for two-way public-coin classical communication complexity which also uniformly implies many previously known direct product results including that for the well studied function Set Disjointnes. Direct product for Set Disjointness was first shown by our group in the paper titled "A Strong Direct Product Theorem for Disjointness". Many other direct product and direct sum results appear in the papers titled : "New Results in the Simultaneous Message Passing Model", "Direct product theorems for classical communication complexity via subdistribution bounds", "A Strong Direct Product Theorem for Disjointness". Similar results have also been obtained in the area of query complexity in the paper titled : "Optimal Direct Sum Results for Deterministic and Randomized Decision Tree Complexity".

2. New general lower bound methods in Communication complexity and Query Complexity are proposed in "The Partition Bound for Classical Communication Complexity and Query Complexity" which are the strongest lower bounds known. New general upper bounds for classical communication complexity and new general lower bounds are proposed in "New bounds on classical and quantum one-way communication complexity".

3. Novel methods for generating correlations among remote parties was exhibited in "The communication complexity of correlation". New lower bounds on the communication complexity of AND-OR Trees is shown in "Depth-Independent Lower bounds on Communication Complexity of Read-Once Boolean Functions". Lower bounds on space required by streaming algorithms for the problem of recognizing well-parenthesized expression is shown in "The space complexity of recognizing well-parenthesized expression"

4. New proof of the well known 'influence lower bound method' in query complexity has been provided in the paper "The influence lower bound via query elimination". This is a conceptually simpler and shorter proof that proceeds via query elimination, an idea with potentially other applications in query complexity.

5. A conceptually simpler and much shorter proof (than the originial by J. Radhakrishan and Sen, JACM, 2009) of the Quantum Substate Theorem has been provided in the paper "A short proof of the quantum Substate Theorem". The substate theorem has found many applications in communication complexity and cryptography, including optimal Direct sum theorem for entanglement assisted quantum one-way communication complexity.

Future Work: We intend to further explore still widely open questions of Direct Sum and Direct Product, specially in the quantum setting. There are many interesting questions related to the New Lower Bound methods proposed by us, which are worth exploring. The area of Multiparty Communication Complexity is still quite nascent with some very hard and interesting questions.

B. Selected invited talks

1. Rahul Jain, invited speaker at conference 'Quantum Information and Processing' 2010, ETH, Zurich, Switzerland. Presented talk on the result 'QIP=PSPACE'.

2. Miklos Santha, invited speaker at '5th International Computer Science Symposium in Russia', Kazan, Russia, 2010.

3. Miklos Santha, invited speaker at 'NATO Advanced School in Quantum Information Processing and Quantum Cryptography', Montreal, Canada, 2010.

4. Rahul Jain, invited speaker at the '2nd Annual Mysore Park Workshop in Theoretical Computer Science: Algorithms and Complexity', Infosys Campus, Mysore, India, May, 2011.

5. Miklos Santha, invited speaker at ’Workshop on Quantum Computer Science’, Riga, Latvia, 2011.
6. Iordanis Kerenidis, invited speaker at conference ’Quantum Information and Processing’ 2010, ETH, Zurich, Switzerland. Presented talk on ’Optimal Quantum Strong Coin Flipping’.
7. Ashwin Nayak, invited speaker at ’Quantum information in Paris Day’, Institut Henri Poincare, Paris, France, 2010. Presented talk on ’Fault-tolerant quantum communication with constant overhead’.
8. Ashwin Nayak, invited speaker at ’The Boulder School in Condensed Matter and Materials Physics: Computational and Conceptual Approaches to Quantum Many-Body Systems’, University of Colorado, 2010.
9. Iordanis Kerenidis, invited talk at the ’Journee Groupe de Travail-Informatique Quantique’, 2011 (Paris).
10. Troy Lee, ’Dagstuhl seminar on Computational Complexity of Discrete Problems’, Invited survey talk on Communication complexity.
11. Joe Fitzsimons, invited talk a the ’Bellairs Workshop on Information Theory, Quantum Mechanics and Security’, at the Bellairs Research Institute, Barbados, 2011.

III. OTHERS

1. Awards

1. Penghui Yao won the Dean’s Graduate Research Achievement Award, School of Computing, National University of Singapore, 2011.

2. Outreach

1. Troy Lee and Bill Rosgen have conducted the ’Xperiment booth with soap bubble computers and billiard ball computers’, at SunTech City Mall, Singapore. They have introduced the public to P and NP and thinking about the role of physics in computation.
2. Rahul Jain has participated in the ’Maths and Science UPDATES - Teacher’s Workshop : Modern Applications of Quantum Physics’, 2010, and presented talk on Quantum Computation.

3. Organization

1. We took part in the organization of Quantum Information Processing, Singapore, 2011.

IV. PUBLICATIONS

1. J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar. (2011). Fully Distrustful Quantum Cryptography. Phys. Rev. Lett.
2. Andre Chailloux, and I. Kerenidis. (2011). Optimal bounds for quantum bit commitment. Proceedings of IEEE FOCS
3. Yuichiro Matsuzaki, Simon C. Benjamin, and J. Fitzsimons. (2011). Entangling unstable optically active matter qubits. Phys. Rev. A 83, 060303.
4. Tom Close, Femi Fadugba, Simon C. Benjamin, J. Fitzsimons, and Brendon W. Lovett. (2011). Rapid and robust spin state amplification. Phys. Rev. Lett. 106, 167204.

5. Yuichiro Matsuzaki, Simon C. Benjamin, and J. Fitzsimons. (2011). Magnet field sensing beyond the standard quantum limit under the effect of decoherence. Phys. Rev. A 84, 012103.

6. M.E. McKague. (2011). Super-quantum non-local correlations in quaternionic quantum theory. Int. J. Quant. Info.

7. M.E. McKague. (2011). Self-testing graph states. Proceedings of TQC

8. S. Zhang. (2011). On the Power of Lower Bound Methods for One-Way Quantum Communication Complexity. Proceedings of ICALP 1, 49-60.

9. Frederic Magniez, A. Nayak, Peter Richter, and M. Santha. (2011). On the hitting times of quantum versus random walks. Algorithmica

10. Frederic Magniez, Ashwin Nayak, Peter C. Richter, and Miklos Santha. (2011). On the hitting times of quantum versus random walks. Algorithmica

11. G. Ivanyos, Luc Sanselme, and M. Santha. (2011). An efficient quantum algorithm for the hidden subgroup problem in nil-2 groups. Algorithmica

12. Frederic Magniez, A. Nayak, Jeremie Roland, and M. Santha. (2011). Search via Quantum Walk. SIAM Journal of Computing 1, 142-164.

13. Frederic Magniez, A. Nayak, M. Santha, and David Xiao. (2011). Improved Bounds for the Randomized Decision Tree Complexity of Recursive Majority. Proceedings of ICALP 1, 317-329.

14. Andre Chailloux, I. Kerenidis, and B. Rosgen. (2011). Quantum Commitments from Complexity Assumptions. Proceedings of ICALP 73-85.

15. T. Lee, Rajat Mittal, Ben Reichardt, Robert Spalek, and M. Szegedy. (2011). Quantum query complexity of state conversion. Proceedings of IEEE FOCS

16. R. Jain, and S. Zhang. (2011). The influence lower bound via query elimination. Theory of Computing

17. R. Jain, and P. Yao. (2011). A Parallel Approximation Algorithm for Positive Semidefinite Programming. Proceedings of IEEE FOCS

18. H. Klauck. (2011). On Arthur Merlin Games in Communication Complexity. Proceedings of IEEE CCC 189-199.

19. Marc Kaplan, I. Kerenidis, Sophie Laplante, and Jeremie Roland. (2010). Non-Local Box Complexity and Secure Function Evaluation. Quantum Information and Computation 11, 40-69.

20. Andre Chailloux, I. Kerenidis, and Jamie Sikora. (2010). Lower Bounds for Quantum Oblivious Transfer. Proceedings of FSTTCS

21. Earl T. Campbell, and J. Fitzsimons. (2010). An introduction to one-way quantum computing in distributed architectures. Int. J. Quant. Info. 8, 219-258.

22. R. Jain. (2010). Resource requirements of private quantum channels and consequences for oblivious remote state preparation. Journal of Cryptology 1-13.

23. G. Ivanyos, M. Karpinski, and N. Saxena. (2010). Deterministic polynomial time algorithms for matrix completion problems. SIAM Journal of Computing 39, 3736-3751.

24. T. Lee, and S. Zhang. (2010). Composition theorems in communication complexity . Proceedings of ICALP

25. M. Schaffry, E.M. Gauger, J.J.L. Morton, J. Fitzsimons, S.C. Benjamin, and B.W. Lovett. (2010). Quantum metrology with molecular ensembles. Phys. Rev. A 82, 042114.

26. Y. Matsuzaki, S.C. Benjamin, and J. Fitzsimons. (2010). Distributed quantum computation with arbitrarily poor photon detection. Phys. Rev. A 82, 010302.

27. R. Jain, H. Klauck, and M. Santha. (2010). Optimal Direct Sum Results for Deterministic and Randomized Decision Tree Complexity. Inf. Proc. Lett 110, 893-897.

28. R. Jain, I. Kerenidis, G. Kuperberg, O. Sattath, M. Santha, and S. Zhang. (2010). On the power of unique quantum witness. Proceedings of ICS

29. R. Jain, Z. Ji, S. Upadhyay, and J. Watrous. (2010). QIP = PSPACE. Proceedings of ACM STOC 573-582.

30. R. Jain, and H. Klauck. (2010). The Partition Bound for Classical Communication Complexity and Query Complexity. Proceedings of IEEE CCC 247.

31. R. Jain, H. Klauck, and S. Zhang. (2010). Depth-Independent Lower bounds on Communication Complexity of Read-Once Boolean Functions. COCOON 16,

32. H. Klauck. (2010). A strong direct product theorem for disjointness. Proceedings of ACM STOC 77-86.

33. Y. Matsuzaki, S.C. Benjamin, and J. Fitzsimons. (2010). Probabilistic growth of large entangled states with low error accumulation. Phys. Rev. Lett. 104, 050501.

34. M. Santha. (2010). Quantization of Random Walks: Search Algorithms and Hitting Time. Proceedings of CSR, 343.