Computer Science Project: Report 2012-2013

I. RESEARCH HIGHLIGHTS

A. Algorithms and Complexity

1. In [2] we give an algorithm to compute approximate Nash equilibria that generalizes and improves many previous works. One component of this work is a technique used by Troy Lee and Adi Shraibman to lower bound quantum communication complexity with entanglement. The approximation algorithm works more broadly for any optimization problem of the form $\max q^t Ap$ over probability vectors p, q. The idea of the algorithm is to reduce solving this quadratic optimization problem to a sequence of linear programs by enumerating over an ϵ-net for the convex hull of the columns of A.

2. Understanding the structure and complexity of ground states of local Hamiltonians is one of the central problems in Condensed Matter Physics and Quantum Complexity Theory. In gapped systems, it has been long conjectured that the entanglement entropy of a region scales like the area of its boundary rather than its volume, the so-called area law conjecture. To date, it has only been proven for 1D systems by a celebrated result due to Hastings (2007). In [3] we exponentially improve Hastings result by inventing a new technique that captures strong locality aspects of the ground state of gapped systems. This technique is further used to derive a sub-exponential algorithm for finding the ground states of such systems, and it offers the prospects of proving the area-law conjecture for higher dimensions.

3. In [11] we devise two deterministic polynomial-time algorithms which solve the following two problems: given a linear subspace $\mathcal{B}$ of n by n matrices over a field $\mathbb{F}$, (1) determine the maximum rank among matrices in $\mathcal{B}$ when $\mathcal{B}$ is spanned by unknown rank-one matrices; (2) decide if there exists a nonsingular matrix in $\mathcal{B}$ when $\mathcal{B}$ is triangularizable. Both algorithms work over the rational numbers and over finite fields, given that the field size is at least $n+1$. We generalize a classical mathematical tool called Wong sequences to achieve these results, and the first algorithm answers an open question of L. Gurvits. We note that Chitambar et al. showed the equivalence between the problem of deciding the existence of nonsingular matrices in $\mathcal{B}$, and the problem of multipartite to bipartite entanglement transformations.

4. In [23] we investigate a new model of computation for data centres handling huge amounts of data. In this model k machines perform local computations (the input is too large for a single machine's memory) and inputs are assigned to machines randomly. Then they exchange results during communication rounds, whose number dominates the overall cost. The bandwidth of messages is restricted, and in typical applications problem sizes can be petabytes while message lengths are gigabytes. We show how to achieve speedups up to a factor of $\Omega(k)$ for many graph problems, and better speedups ($\Omega(k^2)$) for some sparse graph problems. Matching lower bounds are provided via communication complexity arguments, and most of the lower bounds even hold for quantum machines.

5. In [6] we initialize systematic studies of the trial-and-error methodology from an algorithmic perspective. We define a new model to study the computational complexity of CSP search problems on unknown inputs, where candidate solutions are proposed and for each of them the index of an unsatisfied constraint is received. A wide range of computational problems are studied and the study reveals that different levels of difficulty are imposed. A natural next step direction is to consider power and limits of quantum algorithms in this model.

B. Interactive Proofs, Zero Knowledge, Quantum Games

1. In [32] we establish a set of sufficient conditions under which the following holds: Given two instances of conic optimization problems (C_1 and C_2) and another conic optimization problem that arises from tensor product of individual optimization problems (denoted by $C_1 \otimes C_2$), the optimum value of $C_1 \otimes C_2$ is the product of the optimum values of C_1 and C_2. The result generalizes perfect parallel repetition theorems for XOR games, quantum interactive proof systems, and SepQMA(poly). It also covers the results of earlier papers of Mittal and Szegedy in FCT 2007 and Lee and Mittal in ICALP 2008.

2. In [31] we show that in term of the quantum communication needed in order to achieve a perfectly blind quantum computation, the protocol of Broadbent, Fitzsimons and Kashefi [FOCS 09], comes within a factor of $\frac{8}{3}$ of optimal when the client is restricted to preparing single qubits. We also show, that when the client has a more sophisticated device it is possible to achieve blindness with exponentially less quantum communication.

3. In [18] we show that almost all known lower bound methods for communication complexity are also lowerbounds for the information complexity. The key idea of our result is a new connection between communication rectangles and zero communication protocols. A priori, it is surprising that protocols with no communication can actually provide some insight on the communication or information complexity of a function. However, this model, which has been extensively used inquantum information for the study of non-local games and Bell inequalities, turns out to be a very powerful tool for the study of classical communication and information complexity

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

1. In [10, 13, 17] we investigate the important direct-product conjecture for communication protocols. We show direct product results for classical communication complexity in terms of widely used lower bound methods implying direct product results for almost all well-studied functions like set-disjointness, inner-product, gap-hamming distance, greater-than, vector-in-subspace, tribes, hidden-matching. Our techniques may potentially extend to imply direct-product results for quantum communication complexity.

2. In [16] we investigate the so-called correlation-complexity for generating bipartite quantum states and classical distributions. The correlation complexity of a bipartite state ρ is the minimum size of a bipartite state σ that Alice and Bob can share and produce ρ by doing local operations. We show characterization of (exact and approximate) correlation-complexity in terms of (exact and approximate) well studied combinatorial and information theoretic measures like non-negative rank, positive-semi-definite rank, Schmidt-rank, Wyner's common information, thereby exhibiting interesting relationships between them.

3. In [25] we propose an approach to the Evasiveness Conjecture (EC) for monotone transitive Boolean functions that asserts that such functions are evasive for decision trees, that is one can not hope to save even a single query in the worst case. More specifically, we formulate a seemingly weaker version of the EC (which we call as weak-EC) and show that it is equivalent to the original one. Moreover, we show that it suffices to rule out certain computationally simple, namely monotone-NC^1, counter-examples to this weaker version. Finally, we rule out AC^0 counter-examples to the Weak-EC and also rule out monotone-TC^0 counter-examples under a conjecture of Benjamini and Kalai asserting their noise stability.

II. GROUP MEMBERS AND VISITORS

A. Permanent group members

1. Principal Investigators: Rahul Jain, Hartmut Klauck, Miklos Santha.

2. Senior Research Fellows: Itai Arad, Troy Lee.

3. Research Fellows: Thomas Decker (until December 2012), Matthew McKague (until February 2013), Raghav Kulkarni, Carlos A. Perez-Delgado, Youming Qiao, Sarvagya Upadhya.

4. Ph.D students: Anurag Anshu, Priyanka Mukhopadhyay, Attila Pereszlényi, Supartha Podder, Ved Prakash, Aarthi Sundaram, Penghui Yao (graduation expected in 2013).

B. Visitors

1. Regular Visiting Researchers: Gabor Ivanyos (three months per year), Iordanis Kerenidis (two months per year), Shengyu Zhang (two months per year).

2. Interns: Navin Chandak (IIT Mumbai), Zhou Jun (NUS), Rahul Kumar Sahu (IIT Roorkee), Aya Mohamed (American University in Cairo), Pratik Soni (Bits Pilani University).

3. Temporary visitors: Shashank Kaushik (IIT Bangalore, 18 Jun 12 – 14 Aug 12), Sophie Laplante (Université Paris Diderot, 22 Jul 12 – 4 Aug 12 and 21 Jul 13 – 30 Jul 13) Prahladh Harsha (Tata Institute of Fundamental Research, 13 Sep 12 – 12 Oct 12), Dmitry Gavinsky (NEC Research USA, 5 Oct 12 – 17 Oct 12), Xiaoming Sun (Chinese Academy of Sciences, 28 Oct 12 – 3 Nov 12), Sourav Chakraborty (Chennai Mathematical Institute, 28 Nov 12 – 14 Dec 12), Igor Shparlinski (Macquarie University, 4 Dec 12 – 12 Dec 12), Peter Frankl (Hungarian Academy of Sciences, 7 Jan 13 – 11 Jan 13), Ashwin Nayak (University of Waterloo, 12 Jan 13 – 19 Jan 13), Alexander Belovs (University of Latvia, 26 Jan 13 – 22 Feb 13), Anurag Anshu (IIT Guwahati 2 Feb 13 – 10 Feb 13), Steve Brierley (University of Bristol, 3 Feb 13 – 13 Feb 13) Ansis Rosmanis (IQC Waterloo, 13 Feb 13 – 20 Mar 13), Yuan Zhou (Carnegie Mellon University, 19 Feb 13 – 24 Feb 13), Virginie Lerays (Université Paris Diderot, 25 Feb 13 – 22 Mar 13), Michel de Rougemont (Université Paris Sorbonne, 21 Apr 13 – 27 Apr 13), Seung Woo Shin (UC Berkeley, 1 Jun 13 – 18 Jul 13), Anupam Prakash (UC Berkeley, 1 Jun 13 – 18 Jul 13), Shion Chaudhury (Chennai Mathematical Institute, 17 Jun 13 – 23 Jun 13), Sebastian Pokutta (Georgia Institute of Technology, 26 Jun 13 – 7 Jul 13).

III. TALKS AND CONFERENCES

A. Invited and contributed talks

1. Rahul Jain invited talk at the *ELC Tokyo Complexity Workshop*, Tokyo Institute of Technology, Tokyo, Japan, March, 2013; contributed talk at the *13th Asian Quantum Information Science Conference*, Chennai, India, August 2013.

2. Iordanis Kerenidis keynote talk at *Theory of Quantum Computation, Communication and Cryptography*, Guelph, May 2013, invited talk at *Destination Europe Conference*, San Francisco, December 2012, contributed talk at *16th Workshop Quantum Information and Processing*, Beijing, China, January 2013.

3. Hartmut Klauck contributed talk at *30th Symposium on Theoretical Aspect of Computer Science* Kiel, March 2013.

4. Raghav Kulkarni contributed talks at *4th Innovations in Theoretical Computer Science* Berkeley, January 2013 and *10th Theory and Applications of Models of Computation* Hong Kong, May 2013.

5. Troy Lee invited talks at *DIQIP/QCS workshop* Paris, May 2013 and at *Astar*, Singapore, February 2013; contributed talks at *STOC 2013*, Palo Alto, June 2013, at *SODA*, New Orleans, Januar y 2013, and at *FSTTCS*, Hyderabad, December 2012.

6. Ved Prakash contributed talk at *4th Innovations in Theoretical Computer Science* Berkeley, January 2013.

7. Miklos Santha invited talks at the *Japanese - French Workshop on Quantum Information*, Paris, France, March 2013, and at *DIQIP/QCS workshop*, Paris, France, May 2013; contributed talks at the *16th Workshop Quantum Information and Processing*, Beijing, China, January 2013, and at the *8th International Conference on Algorithms and Complexity*, Barcelona, 2013.

B. Conference attendance

1. Rahul Jain FOCS 2012, AQIS 2013.

2. Iordanis Kerenidis FOCS 2012, QIP 2012, TQC 2013.

3. Hartmut Klauck CCC 2012, STACS 2013, ITCS 2013, QIP 2013.

4. Raghav Kulkarni ITCS 2013, TAMC 2013.

5. Troy Lee FSTTCS 2012, SODA 2013, CCC 2013, STOC 2013

6. Miklos Santha QIP 2013, CIAC 2013, STOC 2013.

7. Shengyu Zhang QIP 2013, STOC 2013.

IV. AWARDS

1. Troy Lee has received the NRF Fellowship 2013 "Quantum query complexity, communication complexity, and semidefinite programming".

2. Iordanis Kerenidis has received the 2013 ERC Starting Grant No 306537 "Quantum Communication and Cryptography".

V. PROFESSIONAL ACTIVITIES

1. Rahul Jain was on the PC of FSTTCS 2012 and TAMC 2013.

2. Iordanis Kerenidis was on the PC of STACS 2012, ICITS 2013 and ICALP 2014. He is in the editorial board of International Journal of Quantum Information.

3. Hartmut Klauck and Troy Lee organized (with Leroy Beasley and Dirk Oliver Theis) the Dagstuhl workshop 13082 "Communication Complexity, Linear Optimization, and lower bounds for the nonnegative rank of matrices" during February 17–22, 2013.

4. Troy Lee was on the PC of QIP 2013, the 28th IEEE Conference on Computational Complexity, 2013 and TQC 2013.

5. Miklos Santha was on the PC of STOC 2013. He is in the steering committee of "Fundamentals of Computation Theory" and in the editorial board of International Journal of Quantum Information.

6. Shengyu Zhang was on the PC of ISAAC 2013. He is in the editoral board of Theoretical Computer Science and International Journal of Quantum Information.

VI. OUTREACH

1. Troy Lee assisted in making a display on quantum cryptography at X-periment Public Science Fair, Singapore, 2013.

---

[1] D. Aharonov, I. Arad, and T. Vidick. Guest column: the quantum PCP conjecture. *ACM SIGACT News*, 44(2):47–79, 2013.

[2] N. Alon, T. Lee, A. Shraibman, and S. Vempala. The approximate rank of a matrix and its algorithmic applications. In *Proceedings of the 45th ACM Symposium on the Theory of Computing*. ACM, 2013.

[3] I. Arad, A. Kitaev, Z. Landau, and U. Vazirani. An area law and sub-exponential algorithm for 1D systems. *arXiv preprint arXiv:1301.1162*, 2013.

[4] I. Arad, Z. Landau, and U. Vazirani. Improved one-dimensional area law for frustration-free systems. *Physical Review B*, 85(19):195145, 2012.

[5] S. Bandyopadhyay, R. Jain, J. Oppenheim, and C. Perry. Conclusive exclusion of quantum states. Technical Report arXiv:1306.4683, arXiv, 2013.

[6] X. Bei, N. Chen, and S. Zhang. On the complexity of trial and error. In *Proceedings of the 45th ACM Symposium on the Theory of Computing*, pages 31–40. ACM, 2013.

[7] T. Decker, P. Høyer, G. Ivanyos, and M. Santha. Polynomial time quantum algorithms for certain bivariate hidden polynomial problems. Technical Report 1305.1543, arXiv, May 2013.

[8] M. Elkin, H. Klauck, D. Nanongkai, and G. Pandurangan. Quantum lower bounds for distributed network computing. Technical Report arxiv:1207.5211, arXiv, 2012.

[9] A. Gupta, N. Kayal, and Y. Qiao. Random arithmetic formulas can be reconstructed efficiently (extended abstract). In *Proceedings of the 28th IEEE Conference on Computational Complexity*. IEEE, 2013.

[10] P. Harsha and R. Jain. A strong direct product theorem for the tribes function via the smooth-rectangle bound. Technical Report arXiv:1302.0275, arXiv, 2013.

[11] G. Ivanyos, M. Karpinski, M. Santha, and Y. Qiao. Generalized Wong sequences and their applications to Edmonds' problems. Technical Report http://eccc.hpi-web.de/report/2013/103/, ECCC, 2013.

[12] G. Ivanyos, H. Klauck, T. Lee, M. Santha, and R. de Wolf. New bounds on the classical and quantum communication complexity of some graph properties. In *Proceedings of 32nd FSTTCS*, pages 148–159, 2012.

[13] R. Jain. New strong direct product results in communication complexity. *Journal of the ACM*, 2013. To appear.

[14] R. Jain, I. Kerenidis, G. Kuperberg, M. Santha, O. Sattath, and S. Zhang. On the power of a unique quantum witness. *Theory of Computing*, 8(17):375–400, 2012.
[15] R. Jain, A. Pereszlényi, and P. Yao. A direct product theorem for the two-party bounded-round public-coin communication complexity. In *IEEE 53rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 167–176, 2012.
[16] R. Jain, Y. Shi, Z. Wei, and S. Zhang. Efficient protocols for generating bipartite classical distributions and quantum states. *IEEE Transactions of Information Theory*, 59, 2013. Extended abstract in proceedings of the ACM-SIAM Symposium on Discrete Algorithms (SODA), pp. 1503-1512, 2013.
[17] R. Jain and P. Yao. A strong direct product theorem in terms of the smooth rectangle bound. Technical Report arXiv:1209.0263, arXiv, 2012.
[18] I. Kerenidis, S. Laplante, V. Lerays, J. Roland, and D. Xiao. Lower bounds on information complexity via zero-communication protocols and applications. In *Proceedings of the 53rd Annual Symposium on Foundations of Computer Science*. IEEE, 2012.
[19] I. Kerenidis, M. Lauriere, and D. Xiao. New lower bounds for privacy in communication complexity. Technical Report http://eccc.hpi-web.de/report/2013/015/, ECCC, 2013.
[20] I. Kerenidis and S. Wehner. Long distance two-party quantum cryptography made simple. *Quantum Information and Computation*, 12, 2012.
[21] I. Kerenidis and S. Zhang. A quantum protocol for sampling correlated equilibria unconditionally and without a mediator. In *Theory of Quantum Computation, Communication and Cryptography*, 2012.
[22] H. Klauck and R. de Wolf. Fooling one-sided quantum protocols. In *30th Sympositum on Theoretical Aspects of Computer Science (STACS)*, pages 424–433, 2013.
[23] H. Klauck, D. Nanongkai, G. Pandurandan, and P. Robinson. On the distributed complexity of large-scale graph processing. Technical report, 2013.
[24] H. Klauck and V. Prakash. Streaming computations with a loquacious prover. In *4th Innovations in Theoretical Computer Science (ITCS) conference*, pages 305–320, 2013.
[25] R. Kulkarni. Evasiveness through a circuit lens. In *ITCS*, pages 139–144, 2013.
[26] R. Kulkarni, Y. Qiao, and X. Sun. Any monotone property of 3-uniform hypergraphs is weakly evasive. In *Proceedings of the 10th International Conference on Theory and Applications of Models of Computation*, pages 224–235. Springer Berlin Heidelberg, 2013.
[27] R. Kulkarni and M. Santha. Query complexity of matroids. In *8th International Conference on Algorithms and Complexity*, pages 300–311, 2013.
[28] T. Lee, F. Magniez, and M. Santha. Learning graph based quantum query algorithms for finding constant-size subgraphs. *Chicago Journal of Theoretical Computer Science*, 2012(10):1–21, Dec. 2012.
[29] T. Lee, F. Magniez, and M. Santha. Improved algorithms for triangle finding and associativity testing. In *Proceedings of 23rd ACM-SIAM SODA*, 2013.
[30] F. Magniez, A. Nayak, P. C. Richter, and M. Santha. On the hitting times of quantum versus random walks. *Algorithmica*, 63(1-2):91–116, 2012.
[31] A. Mantri, C. A. Perez-Delgado, and J. F. Fitzsimons. Optimal blind quantum computation. *arXiv preprint arXiv:1306.3677*, 2013.
[32] R. Mittal, J. Sikora, and S. Upadhyay. Product theorems in cone programs. Manuscript, 2013.
[33] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis. Multiparty entanglement verification resistant against dishonest parties. *Phys. Rev. Letters*, 108, 2012.
[34] A. Pereszlényi. On quantum interactive proofs with short messages. *Chicago Journal of Theoretical Computer Science*, 2012(9):1–10, Dec. 2012.
[35] A. Pereszlényi. One-sided error QMA with shared EPR pairs—a simpler proof. Technical Report 1306.5406, arXiv, June 2013. Talk at AQIS '13.
[36] C. A. Pérez-Delgado, M. E. Pearce, and P. Kok. Fundamental limits of classical and quantum imaging. *Physical Review Letters*, 109(12):123601, 2012.
[37] Z. Wei and S. Zhang. Full characterization of quantum correlated equilibria. *Quantum Information and Computation*, 13:0846–0860, 2013.