Computer Science Project: Report 2014-2015

I. INTRODUCTION

Relatively stable year with not many changes. Rahul Jain is on sabbatical since January 2015. Troy Lee's NRF Fellowship *Quantum query complexity, communication complexity, and semidefinite programming* is handled by NTU, there is a formal project agreement between NTU and CQT under which the research fellows employed by NTU on this grant are seconded to CQT. The interaction between CQT and NUS is smooth. We very much wish that Itai Arad become the 5th PI of the CS group, and we have taken various steps to secure him a tenure track position in the NUS Physics Department.

The new research direction *Extended Formulation Complexity* introduced last year is now in full development together with the other three traditional research areas. Under the direction of Itai Arad the direction *Hamiltonian Complexity* is also strongly present in our research agenda.

II. GROUP MEMBERS AND VISITORS

A. Permanent group members

1. Principal Investigators: Rahul Jain, Hartmut Klauck, Troy Lee, Miklos Santha.
2. Senior Research Fellow: Itai Arad.
3. Research Fellows: Raghav Kulkarni, Anupam Prakash (since March 2015), Jamie Sikora, Sarvagya Upadhya (until February 2015), Antonios Varvitsiotis, Zhaohui Wei.
4. Ph.D students: Anurag Anshu, Vamsi Krishna Devabathini, Priyanka Mukhopadhyay, Attila Pereszlényi (graduated in January 2015), Supartha Podder, Ved Prakash, Aarthi Sundaram.

B. Visitors

1. Regular Visiting Researchers: Dmitry Gavinsky (3 months per year), Prahladh Harsha (1 month), Gábor Ivanyos (3 months), Iordanis Kerenidis (2 months), Thomas Vidick (1 month), Shengyu Zhang (2 months).
2. Interns: Kushal Chawla, Palak Jain, Palak Jain, Tomas Vyskocil.
3. Temporary visitors: Phong Nguyen (Tsinghua University, 17 Aug 14 - 22 Aug 14), Kati Friedl (Technical University of Budapest, 29 Sep 14 - 11 Oct 14), Som Bandyopadhyay (Center for Astroparticle Physics and Space Science, 06 Oct 14 - 11 Oct 14), Aram Harrow (MIT, 03 Dec 14 - 08 Dec 14), Cyril Stark (MIT, 06 Jan 15 - 09 Jan 15), Robin Kothari (MIT, 17 Jan 15 - 30 Jan 15), Frédéric Magniez (Université Paris Diderot, 18 Jan 15 - 24 Jan 15), Ronald de Wolf (CWI, Amsterdam, 18 Jan 15 - 24 Jan 15), Stacey Jeffery (Caltech, 19 Jan 15 - 23 Jan 15), Marco Tomamichel (University of Sydney, 09 Feb 15 - 13 Feb 15), Alexander Belov (University of Latvia, 15 Mar 15 - 14 May 15), Richard Jozsa (University of Cambridge, 24 Mar 15 - 31 Mar 15), Michel de Rougemont (Université Paris Diderot, 06 May 15 - 08 May 15), Nikhil Balaji (CMI, 17 May 15 - 27 May 15), Samir Datta (CMI, 17 May 15 - 23 May 15).

III. RESEARCH HIGHLIGHTS

A. Algorithms and Complexity

1. In [25] we study a message-passing distributed computing model for graph processing, motivated by the increasing need for fast distributed processing of large-scale graphs such as the Web graph. Our model consists of a point-to-point communication network of k machines interconnected by bandwidth-restricted links. Communication is the costly operation and is

measured in rounds. The network is used to process arbitrary large graphs, whose n nodes are distributed randomly to the k machines ($k \ll n$). We show tight upper and lower bounds on the round complexity of many fundamental graph problems.

2. In [3] we study average case communication complexity under the restriction that the distribution on inputs has limited correlation. This study interpolates between the previously studied cases of product distributions and distributions with arbitrarily large amounts of correlation. We give tight upper and lower bounds for the classical and quantum complexities of the Disjointness Problem in this model. We also show, for the first time, how the one-way communication complexity model under product distributions on inputs differs from the PAC-learning model: the former allows exponentially better dependence on the error probability.

3. In [21] we studied the problem of finding nonzero solutions to systems of homogeneous diagonal polynomial equations over finite fields. A diagonal polynomial equation of degree d is an equation obtained from a linear equation by replacing the variables by their dth power. The problem can be considered as generalization of finding *Short Integer Solutions* to systems of linear equations. This latter problem serves as basis for certain cryptosystems supposed to remain secure against attacks by a quantum computer. We considered relaxed cases of solving diagonal systems where the degree of freedom (that is, the number of variables compared to a function of the number of equations and the degree d) is large enough to guarantee existence of solutions. For instance, the celebrated Chevalley–Warning Theorem gives that there is always a nonzero solution when the number of variables exceed the product of the degree and the number of equations. It is an open question whether a solution can be efficiently found under this condition. However, when the number of equations is constant, and the degree of freedom exceeds a certain polynomial of d, a solution can be efficiently found using existing techniques. Our main result is an efficient method for the case the degree d is constant and the number of variables exceed a certain bound polynomial in the number equations. Results of this flavor had only been previously known for the cases $d = 1, 2$. We used our algorithm as an important ingredient of a procedure to solve the hidden subgroup problem in a certain new class of groups on a quantum computer.

4. In [30] we introduced a new framework for understanding locality in gapped ground states of local Hamiltonians. Such ground states are important from a physical point of view since they describe the low temperature physics of many interesting systems. They are known to obey strong properties of locality such as area-laws of entanglement entropy and the exponential decay of correlation. Our work introduced a powerful new concept, *local reversibility*: a state $|\psi\rangle$ is called locality reversible if the action of any operator Γ on it, which is defined on L particles, can be (approximately) reversed by a sum of $O(\sqrt{L})$-local operators. Local reversibility is an indication for a relatively simple entanglement structure, since it implies that the $O(L)$-scale entanglement that was broken by Γ can be fixed by merely using operators of size $O(\sqrt{L})$, which in turn implies that we did not have a lot of $O(L)$ entanglement to begin with. Our main result shows that all unique ground states of gapped local Hamiltonains are locally reversible. On the other hand, we show that cat states and degenerate topologically ordered states are not locally reversible. Using the fact that unique gapped ground states are locally reversible we prove many new results: exponential concentration results on the fluctuations of local order parameters, upper bounds on the quality of the mean-field approximation, and a new inequality between critical exponents.

5. We studied two computational problems motivated by their connections to cryptography and information security. In [2], we consider solutions to restricted linear congruence $a_1x_1 + \cdots + a_kx_k \equiv b \pmod{n}$, with $(x_i, n) = t_i$ $(1 \leq i \leq k)$, where $a_1, \ldots, a_k, b$, $n \geq 2$ are arbitrary integers. Using properties of Ramanujan sums and of the finite Fourier transform of arithmetic functions, we give an explicit formula for the number of solutions of this linear congruence. We then propose an authenticated encryption scheme based on an ε-almost-universal (ε-AU) family of hash functions, and by applying the formula, we analyze the integrity of this scheme. In [41], we study the problem of anonymizing data by column suppression. Meyerson and Williams showed that this problem is NP-hard for $k \geq 3$. The complexity of this problem for $k = 2$ remained open. In this note, we show that 2-anonymizing data by suppressing the minimum number of columns is also NP-hard. In fact, we prove a stronger claim that this problem is NP-hard to approximate within a factor of $\Omega(\log m)$, where m is the number of columns in the table.

6. Given a matrix $A \in \mathbb{R}^{n\times p}$ with SVD $A = U\Sigma V^T$ where r is the rank of A, the statistical leverage scores of A are the squared ℓ_2-norms of rows of U, and the matrix coherence is the largest statistic leverage score. The i-th leverage score measures the importance of the row i, and these quantities play an important role in many machine learning algorithms. In [34] we introduce an efficient quantum algorithm to approximate s_i in time $O(\log n)$ when A is sparse and the ratio between A's largest singular value and smallest non-zero singular value is constant. This gives an exponential speedup over the best known classical algorithms.

7. In [7] we study some central graph problems such asReachabilityand Matching in thedynamicsetting. In this setting the edges of the graphs are continuously being added and deleted, and the goal is to build a polynomial size data-structure that helps in updating the solution efficiently. Immerman and Patnaik (1996), motivated by application in database, had conjectured thatReachabilityin graphsrequiresonlyfirst-order formulaupdates. We resolve this conjecture in affirmative. Moreover, we obtain a non-uniformfirst-orderupdate algorithm for Maximum Matching as well. Our main techniques are exploiting the connections of these problems to linear algebra and approaching them via bounded-dept circuits. We then show that bounded depth circuits are equivalent tofirst-orderformulae indynamicsetting for domain independent queries. This opens a fruitful avenue of exploring other graph theoretic andand linear algebraic problems in the same light.

B. Interactive Proofs, Zero Knowledge, Quantum Games

1. Nonlocality enables two parties to win specific games with probabilities strictly higher than allowed by any classical theory. Nevertheless, all known such examples consider games where the two parties have a common interest, since they jointly win or lose the game. The main question we ask in [39] is whether the nonlocal feature of quantum mechanics can offer an advantage in a scenario where the two parties have conflicting interests. We answer this in the affirmative by presenting a simple conflicting interest game, where quantum strategies outperform classical ones. Moreover, we show that our game has a fair quantum equilibrium with higher payoffs for both players than in any fair classical equilibrium. Finally, we play the game using a commercial entangled photon source and demonstrate experimentally the quantum advantage.

2. The last two decades have witnessed a rapid development of quantum information processing, a new paradigm which studies the power and limit of quantum advantages in various information processing tasks. Problems such as when quantum advantage exists, and if existing, how much it could be, are at a central position of these studies. In a broad class of scenarios, there are, implicitly or explicitly, at least two parties involved, who share a state, and the correlation in this shared state is the key factor to the efficiency under concern. In these scenarios, the shared entanglement or discord is usually what accounts for quantum advantage. In [44] we examine a fundamental problem of this nature from the perspective of game theory, a branch of applied mathematics studying selfish behaviors of two or more players. We exhibit a natural zero-sum game, in which the chance for any player to win the game depends only on the ending correlation. We show that in a certain classical equilibrium, a situation in which no player can further increase her payoff by any local classical operation, who- ever first uses a quantum computer has a big advantage over its classical opponent. The equilibrium is fair to both players and, as a shared correlation, it does not contain any discord, yet a quantum advantage still exists. This indicates that at least in game theory, the previous notion of discord as a measure of non-classical correlation needs to be reexamined, when there are two players with different objectives.

3. In [14], motivated by the study of reconfiguration problems in computer science, we study the quantum version which we call *ground state connectivity of local Hamiltonians*. Quantum Hamiltonian Complexity is a rapidly growing area of research lying in the intersection of complexity theory and condensed matter physics. A main task in Quantum Hamiltonian Complexity is to quantify the complexity of finding states of low energy. In this paper, we study a related problem which is to quantify the complexity of determining whether two states of low energy are "connected" or not. We show that the complexity of this problem varies greatly as the parameters defining the problem vary. In particular, we use ground state connectivity to find a very natural QCMA-complete problem, a goal which has generally

proven difficult since the conception of QCMA (a quantum generalization of NP) over a decade ago.

4. In [36] we consider the problem of deciding whether a nonlocal game admits a perfect entangled strategy that uses projective measurements on a maximally entangled shared state. Via a polynomial-time Karp reduction, we show that independent set games are the hardest instances of this problem. Secondly, we show that if every independent set game whose entangled value is equal to one admits a perfect entangled strategy, then the same holds for all symmetric synchronous games. Finally we identify combinatorial lower bounds on the classical and entangled values of synchronous games in terms of variants of the independence number of appropriate graphs. Our results suggest that independent set games are representative of all nonlocal games when dealing with questions concerning perfect entangled strategies.

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

1. One of the very important open questions in communication complexity is whether the information complexity of a function equals its communication complexity? Information complexity measures the least amount of information the players must reveal to each other for computing the function in an interactive protocol. Communication complexity measures the least amount of communication the players must send to each other for computing the function in an interactive protocol. In [9], we examine whether any currently known techniques might be used to show a separation between the two notions. Recently, Ganor et al. [2014] provided such a separation in the distributional setting for a specific input distribution using a new lower bound method they introduced called the *relative discrepancy bound*. We show that in the non- distributional setting, the relative discrepancy bound is, in fact, smaller than the information complexity, and hence it cannot be used to separate information and communication complexity. In addition, in the distributional case, we provide an equivalent linear program formulation for relative discrepancy and relate it to variants of the *partition bound* (introduced by Jain and Klauck [2011]), resolving also an open question regarding the relation of the partition bound and information complexity. Last, we prove the equivalence between the *adaptive relative discrepancy* (Ganor et al. [2014]) and the *public-coin partition bound* (Jain, Lee, Vishnoi [2014]), which implies that the logarithm of the adaptive relative discrepancy bound is quadratically tight with respect to communication.

2. In [10, 22] we investigated questions in streaming complexity, a model in which the input is scanned a few times and there is a limited processing space. Nearly tight bounds on the space requirements of streaming algorithms for various important problems were obtained for example for finding if a given expression is well parenthesized, reversal of a given stream etc. Information theoretic techniques and communication complexity arguments were used to obtain these bounds.

3. In [26] we show new upper and lower bounds for the Garden-Hose model, a model of memoryless and reversible communication, which has applications to position based quantum cryptography. In particular we disprove a previous conjecture that the Distributed Majority function needs quadratic size protocols (making this function unsuitable for even weak cryptographic applications), and show that superquadratic lower bounds for *any* function will be difficult to prove.

D. Extended Formulation Complexity

1. As explained in the report of last year, to prove NP-hard problems, say the travelling salesman problem (TSP), cannot be solved efficiently by semidefinite programming, the key is to lower bound the corresponding positive semidefinite rank (PSD-rank) is supexponential. In the paper [32] we prove partially this conjecture. We show that when the PSD factors for TSP are rank-1, the size of PSD decomposition is indeed exponential. Though later this problem has been solved completely by James Lee et al., our proof for this case is much simpler, and we believe the technique we use here still has an independent value.

2. Last year in the paper [33] we show several new lower bounds for PSD-rank, which depend on the values of a matrix and not only on its support structure, overcoming a limitation of some previous techniques. By combining the technique in this paper and the sufficient and necessary condition for a given correlation to be quantum discovered by Varvitsiotis and Sikora, in the paper [43] we find a simple and general lower bound for the minimal quantum system size for an arbitrary given quantum correlation, which is a fundamental problem in quantum physics and quantum information theory, and has been believed to be very hard. We apply the new bound onto several famous examples, including PR-box, CHSH inequality and the magic square game, and all the results are tight.

IV. TEACHING

1. Rahul Jain course on *Design and Analysis of Algorithms* (CS 3230), NUS, Fall 2014.
2. Hartmut Klauck course on *Algorithms and Theory of Computing* (MAS 714) NTU, Fall 2014.
3. Troy Lee course on *Linear Algebra* I, NTU, Fall 2014.
4. Jamie Sikora and Antonios Varvitsiotis course on *Quantum Information and Semidefinite Programming*, CQT, Spring 2015.

V. OUTREACH

1. Jamie Sikora participated in CQT's Quantum Cryptography Exhibit for SG50 in March 2015 and in a three-day workshop for JC students called "Generation Q-Camp" at CQT in June 2015.

VI. APPENDIX

A. Invited and contributed talks

1. Itai Arad invited talks at *18th Quantum Information Processing* workshop, Sydney, January 2015, *Quantum Hamiltonian Complexity Reunion workshop*, Simons' Institue, Berkeley, May 2015

2. Dmitry Gavinsky invited talks at BIRS workshop, *Hypercontractivity and Log Sobolev Inequalities in Quantum Information Theory.* Banff, February 2015; contributed talks at *3rd Annual Scientific Meeting of Computer Science Institute of Charles University*, Praha, December 2014, *French-Singaporean Majulab kickoff meeting*, NUS, Singapore, January 2015.

3. Iordanis Kerenidis invited talks at *PCQC Inauguration Workshop*, Paris, August 2014, *French-Singaporean Majulab kickoff meeting*, NUS, Singapore, January 2015, *9th French-Japanese Symposium "Frontiѐres de la sciences* Tokyo, January 2015, *Advances in Quantum Cryptography* workshop, Paris, March 2015.

4. Hartmut Klauck invited talks at *Communication Complexity and Applications* workshop, Banff International Research Station, August 2014, *NTU-VIASM Discrete Mathematics* workshop, Hanoi, Vietnam, December 2014, *French-Singaporean UMI Majulab kick-off meeting*, NUS, January 2015; contributed talk at *Information Theory in Complexity Theory and Combinatorics* workshop, Simons Institute, Berkeley, April 2015.

5. Raghav Kulkarni contributed talk at *39th International Symp. on Mathematical Foundations of Computer Science* (MFCS), Budapest, August 2014.

6. Troy Lee invited talk at *Cargese Workshop on Combinatorial Optimization*, Cargese, France, September 2014; contributed talk at *APPROX/RANDOM* 2014.

7. Supartha Podder contributed talks at *39th International Symp. on Mathematical Foundations of Computer Science* (MFCS), Budapest, August 2014, *34th Conference on Foundations of Software Technology and Theoretical Computer Science*, New Delhi, December 2014.

8. Ved Prakash contributed talks at *SIGMOD Symposium on Principles of Database Systems PhD Symposium*, Snowbird, US, June 2014, *41st International Colloquium on Automata, Languages and Programming*, Copenhagen, Denmark, July 2014.

9. Miklos Santha invited talks *French-Singaporean Majulab kickoff meeting*, NUS, Singapore, January 2015, *American Physical Society March meeting* 2015, San Antonio, March 2015, *12th Annual Conference on Theory and Applications of Models of Computation*, Singapore, May 2015; contributed talk at *4th French-Israeli FILOFOCS* workshop, Tel Aviv, May 2015, *9th International Frontiers of Algorithmics Workshop*, Guilin, July 2015.

10. Zhaohui Wei invited talk at *Cargese Workshop on Combinatorial Optimization*, Cargese, France, September 2014.

11. Shengyu Zhang contributed talk at *12th Annual Conference on Theory and Applications of Models of Computation*, Singapore, May 2015.

B. Conference attendance

1. Itai Arad QIP 2015

2. Rahul Jain QIP 2015.

3. Iordanis Kerenidis QIP 2015, TQC 2015.

4. Hartmut Klauck TQC 2014.

5. Raghav Kulkarni MFCS 2014.

6. Troy Lee APPROX/RANDOM 2014, QIP 2015.

7. Supartha Podder MFCS 2014, FSTTCS 2014, QIP 2015.

8. Ved Prakash QIP 2015.
9. Miklos Santha QIP 2015, TAMC 2015, FAW 2015.
10. Jamie Sikora QIP 2015.
11. Shengyu Zhang TAMC 2015.
12. Zhaohui Wei TAMC 2015.

C. Professional activities

1. Rahul Jain was on the PC of ISAAC 2014, TAMC 2015 (co-Chair).
2. Iordanis Kerenidis was on the PC TQC 2015. He is in the editorial board of *International Journal of Quantum Information*.
3. Hartmut Klauck co-organized the Dagstuhl Workshop "Limitations of convex programming", February 2015.
4. Troy Lee was on the PC of TQC 2015, and the co-organizer of the Dagstuhl workshop "Limitations of convex programming", February 2015.
5. Miklos Santha is in the steering committee of FCT and in the editorial board of *International Journal of Quantum Information*, and he co-organized the *French-Singaporean Majulab kick-off meeting*, NUS, Singapore, January 2015.
6. Venkatesh Srinivasan was on the PC and the the organizing committee of WADS 2015.
7. Shengyu Zhang was on the PC of TAMC 2015. He is in the editorial board of *Theoretical Computer Science* and *International Journal of Quantum Information*.

[1] N. Alon, T. Lee, and A. Shraibman. The cover number of a matrix and its algorithmic applications. In *Proceedings of APPROX/RANDOM*, pages 34–47. Leibniz International Proceedings in Informatics, 2014.

[2] K. Bibak, B. M. Kapron, V. Srinivasan, R. Tauraso, and L. Tóth. Restricted linear congruences and an authenticated encryption scheme. Technical Report 1503.01806 [math.NT], arXiv, 2015.

[3] R. Bottesch, D. Gavinsky, and H. Klauck. Correlation in hard distributions in communication complexity, 2015. Manuscript in preparation.

[4] R. Bottesch, D. Gavinsky, and H. Klauck. Equality, revisited. In *Proceedings of the 40th International Symposium on Mathematical Foundations of Computer Science*, 2015.

[5] F. Chen, T. Xiang, Y. Yang, C. Wang, and S. Zhang. Secure cloud storage hits distributed string equality checking: More efficient, conceptually simpler, and provably secure. In *Proceedings of the IEEE INFOCOM 2015*. IEEE, 2015.

[6] A. M. Childs and G. Ivanyos. Quantum computation of discrete logarithms in semigroups. *J. Math. Cryptology*, 8:405–416, 2014. Preprint reported last year.

[7] S. Datta, R. Kulkarni, A. Mukherjee, T. Schwentick, and T. Zeume. Reachability is in DynFO. Technical Report 1502.07467 [cs.LO], arXiv, 2015.

[8] T. Decker, G. Ivanyos, R. Kulkarni, Y. Qiao, and M. Santha. An efficient quantum algorithm for finding hidden parabolic subgroups in the general linear group. 2015. To appear in Theoretical Computer Science; Conference version reported last year.

[9] L. Fontes, R. Jain, I. Kerenidis, M. Lauriere, S. Laplante, and J. Roland. Relative discrepancy does not separate information and communication complexity. In *Proceedings of the 42nd International Colloquium on Automata, Languages, and Programming*. Springer, 2015.

[10] N. François, R. Jain, and F. Magniez. Input/output streaming complexity of reversal and sorting. In *Proceedings of the 18th International Workshop on Randomization and Computation (RANDOM)*, 2014.

[11] M. Friesen, A. Hamed, T. Lee, and D. Theis. Fooling sets and rank. *European Journal of Combinatorics*, 48:143–153, 2015.

[12] R. Gay, I. Kerenidis, and H. Wee. Communication complexity of conditional disclosure of secrets and attribute-based encryption. In *Proceedings of the 35th International Cryptology Conference*, 2015.

[13] M. Georgiou and I. Kerenidis. New constructions for quantum money. In *Proccedings of the 10th Conference on the Theory of Quantum Computation, Communication and Cryptography*. Leibniz International Proceedings in Informatics, 2015.

[14] S. Gharibian and J. Sikora. Ground state connectivity of local Hamiltonians. In *Proceedings of the 42nd International Colloquium on Automata, Languages, and Programming*. Springer, 2015.

[15] C. Godsil, D. Roberson, B. Rooney, R. Šámal, and A. Varvitsiotis. Graph cores via universal computability. In *Proceedings of the European Conference on Combinatorics, Graph Theory and Applications*. Electronic Notes in Discrete Mathematics, 2015.

[16] A. Grilo, I. Kerenidis, and J. Sikora. QMA with subset state witnesses. In *Proceedings of the 40th International Symposium on Mathematical Foundations of Computer Science*, 2015.

[17] L. Hogben, K. F. Palmowski, D. Roberson, and S. Severini. Orthogonal representations, projective rank, and fractional minimum positive semidefinite rank: Connections and new directions. Technical Report 1502.00016 [math.CO], arXiv, 2015.

[18] X. Hu, Y. Tao, Y. Yang, S. Zhang, and S. Zhou. On the I/O complexity of dynamic distinct counting. In *Proceedings of the 18th International Conference on Database Theory*, pages 265–276. Schloss Dagstuhl - Leibniz-Zentrum fur Informatik, 2015.

[19] G. Ivanyos, M. Karpinski, Y. Qiao, and M. Santha. Generalized Wong sequences and their applications to Edmonds' problems. Technical Report 1307.6429v2 [cs.CC], arXiv, 2015. To appear in J. Comput. Syst. Sci.; Conference version reported last year.

[20] G. Ivanyos, M. Karpinski, M. Santha, N. Saxena, and I. Shparlinski. Polynomial interpolation and identity testing from high powers over finite fields. Technical Report 1502.06631 [math.NT], arXiv, 2015.

[21] G. Ivanyos and M. Santha. On solving systems of diagonal polynomial equations over finite fields. Technical Report 1503.09016 [cs.CC], arXiv, 2015. To appear in Proc. FAW 2015.

[22] R. Jain and A. Nayak. The space complexity of recognizing well-parenthesized expression. *IEEE Transactions on Information Theory*, (60):1–23, 2014.

[23] J. Kaniewski, T. Lee, and R. de Wolf. Query complexity in expectation. In *Proceedings of the 42nd International Colloquium on Automata, Languages and Programming*. Springer, 2015. arXiv:1411.7280 [quant-ph].

[24] I. Kerenidis, M. Lauriere, F. L. Gall, and M. Rennela. Privacy in quantum communication complexity. Technical Report 1409.8488 [quant-ph], arXiv, 2014.

[25] H. Klauck, D. Nanongkai, G. Pandurangan, and P. Robinson. Distributed computation of large-scale graph problems. In *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 391–410, 2015.

[26] H. Klauck and S. Podder. New bounds for the garden-hose model. In *Proceedings of 34th International Conference on Foundation of Software Technology and Theoretical Computer Science*, pages 481–492, 2014.

[27] H. Klauck and S. Podder. Two results about quantum messages. In *Proceedings of 39th International Symposium on Mathematical Foundations of Computer Science 2014*, pages 445–456, 2014.

[28] R. Kothari, D. Racicot-Desloges, and M. Santha. Separating decision tree complexity from subcube partition complexity. Technical Report 1504.01339 [cs.CC], arXiv, 2015.

[29] R. Kulkarni, Y. Qiao, and X. Sun. On the power of parity queries in Boolean decision trees. In *Proceedings of 12th Theory and Applications of Models of Computation*, pages 99–109. Springer, 2015.

[30] T. Kuwahara, I. Arad, L. Amico, and V. Vedral. Local reversibility and entanglement structure of many-body ground states. Technical Report 1502.05330, arXiv, 2015.

[31] T. Lawson, A. Pappa, B. Bourdoncle, I. Kerenidis, D. Markham, and E. Diamanti. Reliable experimental quantification of bipartite entanglement without reference frames. *Phys. Rev. A*, 90:042336, 2014.

[32] T. Lee and Z. Wei. The square root rank of the correlation polytope is exponential. Technical Report 1411.6712 [cs.CC], arXiv, 2014.

[33] T. Lee, Z. Wei, and R. de Wolf. Some upper and lower bounds on psd-rank. Technical Report 1407.4308, arXiv, 2014.

[34] Y. Liu and S. Zhang. Fast quantum algorithms for least squares regression and statistic leverage scores. In *Proceedings of the 9th International Frontiers of Algorithmics Workshop (FAW)*, 2015.

[35] L. Mančinska, D. E. Roberson, and A. Varvitsiotis. Two characterizations of nonlocal games with perfect maximally entangled strategies. In *Proceedings of the 14th Asian Quantum Information Science Conference*, 2014.

[36] L. Mančinska, D. E. Roberson, and A. Varvitsiotis. Nonlocal games with restricted strategies, 2015. Manuscript in preparation.

[37] A. Nayak, J. Sikora, and L. Tunçel. Quantum and classical coin-flipping protocols based on bit-commitment and their point games. Technical Report 1504.04217 [quant-ph], arXiv, 2015.

[38] A. Nayak, J. Sikora, and L. Tunçel. A search for quantum coin-flipping protocols using optimization techniques. *Mathematical Programming*, 2015.

[39] A. Pappa, N. Kumar, T. Lawson, M. Santha, S. Zhang, E. Diamanti, and I. Kerenidis. Nonlocality and conflicting interest games. *Physical Review Letters*, 114:020401, 2015.

[40] D. E. Roberson. Conic formulations of graph homomorphisms. Technical Report 1411.6723 [math.CO], arXiv, 2015.

[41] A. Scott, V. Srinivasan, and U. Stege. k-attribute-anonymity is hard even for k=2. *Inf. Process. Lett.*, 115(2):368–370, 2015.

[42] J. Sikora and A. Varvitsiotis. Conic formulations for two-party correlations and values of nonlocal games, 2015. Manuscript in preparation.

[43] J. Sikora, A. Varvitsiotis, and Z. Wei. On the minimum dimension of a quantum state needed to produce a given correlation, 2015. Manuscript in preparation.

[44] Z. Wei and S. Zhang. Quantum game players can have advantage without discord. In *Proceedings of the 12th Annual Conference on Theory and Applications of Models of Computation*, pages 311–323. Springer, 2015.