Computer Science Project: Report 2015-2016

I. INTRODUCTION

The CS group looks forward to its largest expansion in many years: during the Fall Semester 2016, two new PI's, Divesh Agarwal and Joe Fitzsimons are expected to join the group.

Divesh has graduated from ETH Zürich, and has spent the last four years as postdoc at CUNY in New York and at the Ecole Polytechnique in Lausanne. Simultaneously with his work at CQT, he will be Assistant Professor in the School of Computing at NUS. His specialities are coding theory and lattice based post quantum cryptography. We expect him to lead a new research direction around these areas.

Joe is currently Assistant Professor at the Singapore University of Technology and Design. He is affiliated with CQT since 2010, first as a Senior Research Fellow, since 2013 as Research Assistant Professor. In 2013 he has obtained a five years NRF Fellowship on *Methods for verifying quantum computation*. His research focuses on the use of quantum mechanics to reinforce security of networked computation.

Unfortunately we were not able to secure a tenure track position for Itai Arad in Singapore, and he will take an Assistant Professor position at Technion in October 2016. We thank Itai for his numerous contributions to our group's work in the last few years, in particular in the area of *Hamiltonian Complexity*. Fortunately, he will come back as a regular visitor in the future.

As in the previous years, Troy Lee's NRF Fellowship on *Quantum query complexity, communication complexity, and semidefinite programming* is handled by NTU with a formal project agreement between NTU and CQT. The research fellows working in the area of *Extended Formulation Complexity* are employed by NTU, and are seconded to CQT.

The CS group has organized a 6 weeks program between 18 January - 28 February 2016 in the Institute for Mathematical Sciences at NUS on the subject of *Semidefinite and Matrix Methods for Optimization and Communication*. During the program we held three weeklong workshops, respectively on *Log Rank Conjecture*, on *Positive Semidefinite Rank* and on *Approximation Algorithms*. The total number of participants was above 60, and the program by general agreement was a big success.

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**: Anupam Prakash, Jamie Sikora, Antonios Varvitsiotis, Zhaohui Wei.
4. **Ph.D students**: Anurag Anshu, Priyanka Mukhopadhyay, Supartha Podder, Ved Prakash (graduated in July 2015), Maharshi Ray, Aarthi Sundaram, Siyi Yang (since July 2016). Associated was Ralph Bottesch (graduated in January 2016 at NTU).

B. Visitors

1. **Regular Visiting Researchers**: Dmitry Gavinsky (4 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**: Yang Siyi (Shanghai Jiao Tong University, 10 March 16 -21 April 16), Pavan Kumar Nandgiam (Indian Institute of Technology Bombay, 06 May 16 - 05 July 16), Aravind Reddy

Talla (Indian Institute of Technology Kanpur, 06 May 16 - 05 July 16), Sudarshan Shyam (Indian Institute of Technology Kharagpur, 11 May 16 - 15 July 16) Anshi (Indian Institute of Technology Delhi, 16 May 16 - 08 July 16) Vusirikala Venkata Satyanarayana (Indian Institute of Technology Guwahati, 20 May 16 - 22 July 16) Sushant Agarwal (Chennai Mathematical Institute, 30 May 16 - 25 July 16). Yupan Liu (Zhejiang University, Hangzhou, 1 July 16 - 3 Septembre 16)

3. **Temporary visitors**: Matthew Mc Kague (Otago, 24 August 15 - 25 August 15), Youming Qiao (Sydney, 31 August 15 - 18 September 15), Marco Tomamichel (Sydney, 26 August 15 - 4 September 15), Serge Massar (ULB, Belgium, 05 December 15 - 09 December 15), Ronald de Wolf (CWI, Amsterdam, 14 January 16 - 27 January 16), Alexander Belovs (University of Latvia, 17 January 16 - 21 February 16), Jrmie Roland (ULB, Brussels, 23 January 16 - 28 January 16), Ryan O'Donnell (Carnegie Mellon University, USA, 14 February 16 - 18 February 16), Nisheeth Vishnoi (Ecole Polytechnique de Lausanne, Switzerland, 15 February 16 - 18 February 16), Hoeteck Wee (CNRS and ENS, Paris 15 March 16 - 17 March 16), Narayana P. Santhanam (University of Hawaii at Manoa, 04 May 16 - 08 May 16), Michel de Rougemont (Université Paris Diderot, France, 09 May 16 - 12 May 16).

III. RESEARCH HIGHLIGHTS

A. Algorithms and Complexity

1. A canonical result about satisfiability theory is that the 2-SAT problem can be solved in linear time, despite the NP-hardness of the 3-SAT problem. In the quantum version of 2-SAT problem, we are given a family of 2-qubit projectors Π_{ij} on a system of n qubits, and the task is to decide whether the Hamiltonian $H = \Pi_{ij}$ has a 0-eigenvalue, or its smallest eigenvalue is larger than $1/n^{\alpha}$, for some positive constant α. The problem is not only a natural extension of the classical 2-SAT problem to the quantum case, but is also equivalent to the problem of finding the ground state of 2-local frustration-free Hamiltonians of spin 1/2, a well-studied model believed to capture certain key properties in modern condensed matter physics. While Bravyi has shown that the quantum 2-SAT problem has a classical polynomial-time algorithm, the running time of his algorithm is $O(n^4)$. In [11] we give a classical algorithm with linear running time in the number of local projectors, therefore achieving the best possible complexity.

2. What is the minimum amount of information and time needed to solve 2SAT? When the instance is known, it can be solved in polynomial time, but is this also possible without knowing the instance? Bei, Chen and Zhang (STOC '13) considered a model where the input is accessed by proposing possible assignments to a special oracle. This oracle, on encountering some constraint unsatisfied by the proposal, returns only the constraint index. It turns out that, in this model, even 1SAT cannot be solved in polynomial time unless P = NP. In [9] we consider a model in which the input is accessed by proposing probability distributions over assignments to the variables. The oracle then returns the index of the constraint that is most likely to be violated by this distribution. We show that the information obtained this way is sufficient to solve 1SAT in polynomial time, even when the clauses can be repeated. For 2SAT, as long as there are no repeated clauses, in polynomial time we can even learn an equivalent formula for the hidden instance and hence also solve it. Furthermore, we extend these results to the quantum regime. We show that in this setting 1QSAT can be solved in polynomial time up to constant precision, and 2QSAT can be learnt in polynomial time up to inverse polynomial precision.

3. In [6], we investigated properties of frustration free local hamiltonian systems on a lattice. We simplified the proof of the 'detectability lemma', which is an important tool for the study of area law and exponential decay of correlation in such systems and has also found application in various other scenarios, including dissipative systems and quantum circuits. Using a converse for the detectability lemma (which makes the lemma tight up to constant factors), we provided a recipe for mapping any frustration-free 2-local hamiltonian with a given spectral gap gamma onto an another local hamiltonian (a coarse grained hamiltonian) with constant spectral gap and locality $\sqrt{1/\gamma}$, such that ground spaces of both local hamiltonians coincide.

4. Schubert polynomials were discovered by A. Lascoux and M. Schützenberger in the study of cohomology rings of flag manifolds in the 1980s. These polynomials generalize Schur polynomials, and form a linear basis of multivariate polynomials. In 2003, Lenart and Sottile introduced skew Schubert polynomials, which generalize skew Schur polynomials, and expand in the Schubert basis with the generalized Littlewood-Richardson coefficients. In the work [48] we initiate the study of these two families of polynomials from the perspective of computational complexity theory. We first observe that skew Schubert polynomials, and therefore Schubert polynomials, are in #P (when evaluating on non-negative integral inputs) and VNP (the class 'Valiant's NP' is the class of polynomials f of polynomial degree such that given a monomial we can determine its coefficient in f efficiently, with a polynomial size circuit.). Our main result is a deterministic algorithm that computes the expansion of a polynomial f of degree d in $Z[x_1, ..., x_n]$ in the basis of Schubert polynomials, assuming an oracle computing Schubert polynomials. This algorithm runs in time polynomial in n, d, and the bit size of the expansion. This generalizes, and derandomizes, the sparse interpolation

algorithm of symmetric polynomials in the Schur basis by Barvinok and Fomin. In fact, our interpolation algorithm is general enough to accommodate any linear basis satisfying certain natural properties. Applications of the above results include a new algorithm that computes the generalized Littlewood-Richardson coefficients.

5. In [32, 33] we studied the complexity of the problem of deciding whether an m-tuple of n by n matrices belongs to the null-cone of the polynomial invariants of the simultaneous action of the group $SL_n \times SL_n$ over various ground fields. There are various aspects of this problem: it is equivalent to computing the noncommutative rank (i.e., the rank over the free skew field) of a matrix whose entries are linear polynomials; it is related to finding a subspace which is mapped by all the matrices to a smaller dimensional space; and, over the field of complex numbers, it is also related to testing a certain property of completely positive operators. Independently, over the the complex numbers, Garg, Gurvits, Oliveira and Wigderson (2015) managed to find a deterministic polynomial time solution for the decision problem. We followed a completely different approach in [33], where we developed certain fundamental tools for algorithms solving *constructive versions* of the problems listed above over arbitrary fields and used them in a procedure which works in polynomial time if one of the input matrices has sufficiently large rank. By constructibility we mean that the algorithm outputs high rank noncommutative substitutions as well as pairs of subspaces which certify that the rank cannot be higher. One of our tools became an important ingredient of a proof a bound of generators for the ring of polynomial invariants of $SL_n \times SL_n$ in a paper of Derksen and Makam (2015). Finally in [32], by developing an algorithmic counterpart of a technique of Derksen and Makam, we succeeded to give an unconditionally polynomial time deterministic procedure.

B. Interactive Proofs, Zero Knowledge, Quantum Games

1. In [54], we analyze the dimension of an unknown quantum system in a device-independent manner, i.e., using only the measurement statistics. This is an important task in quantum physics and quantum information theory as the underlying dimension of a quantum system is widely considered to be a fundamental physical property and also a valuable computational resource. In this work, we consider this problem in the prepare-and-measure scenario, i.e., where Alice prepares one of finitely many states, Bob performs one of finitely many measurements (each with finitely many outcomes). Our main result is a lower bound on the dimension of Alice's prepared quantum states which is a function that only depends on the corresponding measurement statistics. Furthermore, we show that our bound performs well on several examples. In particular, we show that our bound provides new insights into the notion of dimension witness. Lastly, we show that the sets of probabilities arising from this setting by measuring fixed-dimensional quantum states are not always convex.

2. The quantum PCP (QPCP) conjecture states that all problems in QMA, the quantum analogue of NP, admit quantum verifiers that only act on a constant number of qubits of a polynomial size quantum proof and have a constant gap between completeness and soundness. Despite an impressive body of work trying to prove or disprove the quantum PCP conjecture, it still remains widely open. The above-mentioned proof verification statement has also been shown equivalent to the QMA-completeness of the Local Hamiltonian problem with constant relative gap. Nevertheless, unlike in the classical case, no equivalent formulation in the language of multi-prover games is known. In [28], we propose a new type of quantum proof systems, the Pointer QPCP, where a verifier first accesses a classical proof that he can use as a pointer to which qubits from the quantum part of the proof to access. We define the Pointer QPCP conjecture, that states that all problems in QMA admit quantum verifiers that first access a logarithmic number of bits from the classical part of a polynomial size proof, then act on a constant number of qubits from the quantum part of the proof, and have a constant gap between completeness and soundness. We define a new QMA-complete problem, the Set Local Hamiltonian problem, and a new restricted class of

quantum multi-prover games, called CRESP games. We use them to provide two other equivalent statements to the Pointer QPCP conjecture: the Set Local Hamiltonian problem with constant relative gap is QMA-complete; and the approximation of the maximum acceptance probability of CRESP games up to a constant additive factor is as hard as QMA. This is the first equivalence between a quantum PCP statement and the inapproximability of quantum multi-prover games.

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

1. In [2] we showed several new separations in query complexity. We overturned the long held belief that the largest separation possible between quantum query complexity and deterministic query complexity for a total function is quadratic, by giving an example of a function with a fourth power separation between these measures. The same function also gives a quadratic separation between the zero-erro randomized and deterministic query complexities. This separation is optimal and overturns the Saks-Wigderson conjecture that the largest possible separation between these measures is $n^{.753\cdots}$ versus n, given by the binary AND-OR tree. Variations of this function give new separations between several other query complexity measures, including: the first super-linear separation between bounded-error and zero-error randomized complexity, larger gaps between exact quantum query complexity and deterministic/randomized query complexities, and a fourth power separation between approximate degree and bounded-error randomized complexity. All of these examples are variants of a function recently introduced by Göös, Pitassi, and Watson which they used to separate the unambiguous 1-certificate complexity from deterministic query complexity and to resolve the famous Clique versus Independent Set problem in communication complexity.

2. While exponential separations are known between quantum and randomized communication complexity for partial functions (Raz, STOC 1999), the best known separation between these measures for a total function is quadratic, witnessed by the 'disjointness function'. In [7], we give the first super-quadratic separation between quantum and randomized communication complexity for a total function, giving an example exhibiting a power 2.5 gap. We also present a nearly optimal quadratic separation between randomized communication complexity and the logarithm of the partition number, improving upon the previous best power 1.5 separation due to Göös, Jayram, Pitassi, and Watson. Our results are the communication analogues of separations in query complexity proved using the recent 'cheat sheet framework' of Aaronson, Ben-David, and Kothari (STOC 2016). Our main technical results are randomized communication and information complexity lower bounds for a family of functions, called 'lookup functions', that generalize and port the cheat sheet framework to communication complexity.

3. In [20] we have presented a partial function *Shape*, which can be computed by a protocol sending entangled simultaneous messages of poly-logarithmic size, and whose classical two-way complexity is lower bounded by a polynomial. The question about existence of a function with such properties has been posed by Klartag and Regev in 2010 and settled by this work.

4. The concepts of quantum correlation complexity and quantum communication complexity were recently proposed to quantify the minimum amount of resources needed in generating bipartite classical or quantum states in the single-shot setting. The former is the minimum size of the initially shared state σ on which local operations by the two parties (without communication) can generate the target state ρ, and the latter is the minimum amount of communication needed when initially sharing nothing. In the paper [35], we generalize these two concepts to multipartite cases, for both exact and approximate state generation, characterize some of these complexity measures, and investigate the relation between them.

5. Let H be a (non-empty) graph on n vertices, possibly containing isolated vertices. Let $f_H(G) = 1$ iff the input graph G on n vertices contains H as a (not necessarily induced) subgraph. Let α_H denote the cardinality of a maximum independent set of H. In [42] we show that $Q(f_H) = \Omega\left(\sqrt{\alpha_H \cdot n}\right)$, where $Q(f_H)$ denotes the quantum query complexity of

f_H. As a consequence we obtain lower bounds for $Q(f_H)$ in terms of several other parameters of H such as the average degree, minimum vertex cover, chromatic number, and the critical probability. We also use the above bound to show that $Q(f_H) = \Omega(n^{3/4})$ for any H, improving on the previously best known bound of $\Omega(n^{2/3})$ We also study the Subgraph Homomorphism Problem, denoted by $f_{[H]}$, and show that $Q(f_{[H]}) = \Omega(n)$. Finally we extend our results to the 3-uniform hypergraphs.

6. In [39] we investigate the problem *Quantum Unique Nondisjointness*, which is a candidate to separate the communication complexity classes QMA and QCMA. Such a separation is elusive as of now. In this problem Alice and Bob each receive an $n/4$-dimensional subspace, which are promised to be either orthogonal to each other, or have a 1-dimensional intersection and are orthogonal otherwise (the latter being the 1-inputs). We determine the quantum, randomized, and QMA complexities of the problem exactly (the QMA-complexity is logarithmic). We then show an upper bound of $O(n^{1/3})$ on the QCMA complexity, and prove that this bound is tight for a reasonable class of QCMA protocols, namely those, in which the proof depends on the intersecting space only. This is done by embedding a large classical Disjointness instance after fixing Merlin's proof. The geometrical statement underlying this embedding is that every large subset of the unit sphere contains an orthonormal set of a certain size.

D. Extended Formulation Complexity

1. In a breakthrough result, Lee, Raghavendra, and Steurer showed that proving lower bounds on semidefinite extension complexity can be reduced to showing lower bounds on the sum-of-squares degree of certain functions. In order, to show strong quantitative bounds, one needs to bound even the sum-of-squares degree needed to *approximate* a function. In [45], we undertake a systematic study of the approximate sum-of-squares degree, both in the case of ℓ_∞ and ℓ_1 approximation. For a general family of symmetric quadratic functions, we show tight upper and lower bounds on their ℓ_∞ approximate sum-of-squares degree. In the case of ℓ_1 approximation, we give upper bounds which show that the bound of Lee, Raghavendra, and Steurer in this case is tight.

2. An $n \times n$ matrix X is called completely positive semidefinite (cpsd) if there exist $d \times d$ Hermitian positive semidefinite matrices $\{P_i\}_{i=1}^n$ (for some $d > 0$) such that $X_{ij} = \mathrm{tr}(P_i P_j)$, for all $i, j \in \{1, \ldots, n\}$. The cpsd-rank of a cpsd matrix is the smallest $d \geq 1$ for which such a representation is possible. In [51] we initiate the study of the cpsd-rank which we motivate twofold. First, the cpsd-rank is a natural non-commutative analogue of the completely positive rank. Second, the cpsd-rank is physically motivated as it can be used to upper and lower bound the size of a quantum system needed to generate a quantum behavior. In this work we present several properties of the cpsd-rank. Unlike the completely positive rank which is at most quadratic in the size of the matrix, no general upper bound is known on the cpsd-rank of a cpsd matrix. In fact, for any $n \geq 1$, we construct a cpsd matrix of size $2n$ whose cpsd-rank is $2^{\Omega(\sqrt{n})}$. Furthermore, we study cpsd-graphs, i.e., graphs G with the property that every doubly nonnegative matrix whose support is given by G is cpsd. We show that a graph is cpsd if and only if it has no odd cycle of length at least 5 as a subgraph.

3. In [26] we exhibit an n-node graph whose 'independent set polytope' requires extended formulations of size exponential in $\frac{n}{\log n}$. Previously, no explicit examples of n-dimensional 0/1-polytopes were known with extension complexity larger than exponential in $\sqrt{n}$. Our construction is inspired by a relatively little-known connection between extended formulations and (monotone) circuit depth.

IV. TEACHING AND OUTREACH

A. Teaching

1. Rahul Jain course on *Advanced Algorithms* (CS 6234), NUS, Spring 2016
2. Hartmut Klauck course on *Computational Economics* (MH4320), NTU, Fall 2015.
3. Troy Lee course on *Linear Algebra* I, NTU, Fall 2015.

B. Outreach

1. CQT has offered a five day workshop in June 2015 in quantum technologies and cryptography for high-school students. Students have studied advanced concepts in mathematics, quantum physics, classical and quantum cryptography, and have seen experiments demonstrating quantum phenomena. From the CS group Supartha Podder, Anupam Prakash, Maharshi Ray, Jamie Sikora, Aarthi Sundaram and Antonios Varvitsiotis have participated in the workshop.
2. Rahul Jain was a local organizer for the event "Shannon Centenary" co-organized by IEEE Information Theory Society, NUS, CQT and NTU in 2016.
3. Rahul Jain participated in NUS outreach events for students and parents.
4. Anurag Anshu was part of an outreach event in December 2015, organized in Art and Science Museum at Marina Bay Sands where he demonstrated bubble computer and billiard computer to audience.

V. APPENDIX

A. Invited and contributed talks

1. Itai Arad

   Invited talks at *6th Biennial Conference of the Toronto Centre for Quantum Information & Quantum Control and the Fields Institute*, Toronto, August 2015; *EU QALGO Workshop on Quantum Algorithms*, Riga, Latvia, September 2015.

2. Dmitry Gavinsky

   Invited talk at *Workshop on Semidefinite and Matrix Methods for Optimization and Communication*, IMS, NUS, Singapore, January 2016.

   Contributed talks at *19th International Workshop on Randomization and Computation (RANDOM'2015)*, Princeton University, August 2015; *48th Symposium on the Theory of Computing*, Cambridge, USA, June 2016.

3. Rahul Jain

   Invited talks at *6th International Conference on Information and Communication Technology Convergence*, Jeju, Korea, October 2015; *Trustworthy Quantum Information 2016*, Shanghai, June 2016.

4. Iordanis Kerenidis

   Invited talks at *5th International Conference on Quantum Cryptography*, Tokyo, September 2015; IMS *Workshop on Semidefinite and Matrix Methods for Optimization and Communication*, NUS, Singapore, January 2016; *Central Workshop of Nexus of Information and Computation Theories Semester*, Institut Henri Poincare, Paris, February 2016.

5. Troy Lee

   Invited talks at *Workshop on Quantum Computational Complexity*, Kyoto, July 2015; *Workshop on Semidefinite and Matrix Methods for Optimization and Communication*, IMS, NUS, Singapore, January 2016.

   Contributed talks at *42nd International Colloquium on Automata, Languages and Programming*, Kyoto, Japan, July 2015; *48th Symposium on the Theory of Computing*, Cambridge, USA, June 2016.

6. Anupam Prakash

   Invited talk at *EU QALGO Workshop on Quantum Algorithms*, Riga, Latvia, September 2015.

   Contributed talk at *31st Conference on Computational Complexity*, Tokyo, June 2016.

7. Supartha Podder

   Contributed talk at *33rd International Symposium on Theoretical Aspects of Computer Science*, Orléans, France, February 2016.

8. Miklos Santha

   Invited talks at *EU QALGO Workshop on Quantum Algorithms*, Riga, Latvia, September 2015; *Heilbronn and QALGO Workshop on Quantum Algorithms*,Cambridge, UK, April 2016; *Hong Kong Workshop on Quantum Information and Foundations*, Hong Kong, May 2016.

9. Jamie Sikora

   Invited talks at *BQP workshop at the Tokyo Institute of Technology*, Tokyo, Japan, December 2015; *Quantum Computational Complexity Workshop at Kyoto University*, Kyoto, Japan, July 2015; *42nd International Colloquium on Automata, Languages, and Programming*, Kyoto, Japan, July 2015.

10. Aarthi Sundaram

    Contributed talks at *19th International Conference on Quantum Information Processing*, Banff, Canada, January 2016; *43rd International Colloquium on Automata, Languages and Programming*, Roma, Italy, July 2016; *41st International Symposium on Mathematical Foundations of Computer Science* Krakow, Poland, August 2016.

11. Antonis Varviotis

    Invited talks at *Zero-error information, Operators, and Graphs*, Barcelona, November 2015; *Semidefinite and Matrix Methods for Optimization and Communication*, Singapore, February 2016; *20th Conference of the International Linear Algebra Society*, Leuwen, July 2016; *DIMACS Workshop on Distance Geometry: Theory and Applications*, New Jersey, July 2016.

    Contributed talks at 22*nd International Symposium on Mathematical Programming*, Pittsburgh, July 2015; *European Conference on Combinatorics, Graph Theory and Applications,* Bergen, September 2015; *5th International Conference on Continuous Optimization*, Tokyo, August 2016.

12. Shengyu Zhang

    Invited talks talk at *Workshop on Semidefinite and Matrix Methods for Optimization and Communication*, IMS, NUS, Singapore, January 2016; *Hong Kong Workshop on Quantum Information and Foundations*, Hong Kong, May 2016; *1st Post-Quantum Cryptography Asia Forum*, China, June 2016.

B. Professional activities

1. Rahul Jain was on the PC of TAMC 2016, ICALP 2016, STACS 2016 and QIP2016. He is Associate Editor in the Journal of Computer and System Sciences (JCSS) since January 2016. He co-organized the IMS workshop on *Semidefinite and Matrix Methods for Optimization and Communication*, NUS, Singapore, Jan - Feb 2016.

2. Iordanis Kerenidis was on the PC of QCRYPT 2016, QIP 2016, TQC 2016, ICITS 2016 and SCN 2016. He is in the editorial board of *International Journal of Quantum Information.*

3. Hartmut Klauck co-organized the IMS workshop on *Semidefinite and Matrix Methods for Optimization and Communication*, NUS, Singapore, Jan - Feb 2016.

4. Troy Lee was on the PC of QIP 2016, and co-organized the IMS workshop on *Semidefinite and Matrix Methods for Optimization and Communication*, NUS, Singapore, Jan - Feb 2016.

5. Miklos Santha was on the PC of CSR 2016. He is in the steering committee of FCT and in the editorial board of *International Journal of Quantum Information.* He co-organized the IMS workshop on *Semidefinite and Matrix Methods for Optimization and Communication*, NUS, Singapore, Jan - Feb 2016.

6. Jamie Sikora was on the PC of TQC 2016.

7. Shengyu Zhang was on the PC of COCOON 2016 and TAMC 2016. He is in the editorial board of *Theoretical Computer Science* and *International Journal of Quantum Information.*

[1] D. Aharonov, A. Chailloux, M. Ganz, I. Kerenidis, and L. Magnin. A simpler proof of the existence of quantum weak coin flipping with arbitrarily small bias. *SIAM Journal on Computing*, 45(3):633–679, 2016.

[2] A. Ambainis, K. Balodis, A. Belovs, T. Lee, M. Santha, and J. Smotrovs. Separations in query complexity based on pointer functions. In *Proceedings of the 48th Annual Symposium on the Theory of Computing*, pages 800–813, 2016.

[3] A. Anshu. A chernoff-type bound for local hamiltonian systems on a quantum lattice. Technical Report quant-ph/1508.07873, arXiv, 2015.

[4] A. Anshu. A lower bound on expected communication cost of quantum state redistribution. Technical Report quant-ph/1506.06380, arXiv, 2015.

[5] A. Anshu, I. Arad, and A. Jain. How local is the information in MPS/PEPS tensor networks? *ArXiv e-prints, arXiv:1603.06049*, Mar. 2016.

[6] A. Anshu, I. Arad, and T. Vidick. Simple proof of the detectability lemma and spectral gap amplification. *Physical Review B*, 93:205142, 2016.

[7] A. Anshu, A. Belovs, S. Ben-David, M. Göös, R. Jain, R. Kothari, T. Lee, and M. Santha. Separations in communication complexity using cheat sheets and information complexity. In *Proceedings of the 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS) (to appear)*, 2016.

[8] A. Anshu, A. Garg, A. Harrow, and P. Yao. Lower bound on expected communication cost of quantum huffman coding. Technical Report quant-ph/1605.04601, arXiv, 2016.

[9] I. Arad, A. Bouland, D. Grier, M. Santha, A. Sundaram, and S. Zhang. On the complexity of probabilistic trials for hidden satisfiability problems. Technical Report 1606.03585, arXiv, 2016. To appear in Proc. MFCS 2016.

[10] I. Arad, Z. Landau, U. Vazirani, and T. Vidick. Rigorous RG algorithms and area laws for low energy eigenstates in 1D. *ArXiv e-prints, arXiv:1602.08828*, Feb. 2016.

[11] I. Arad, M. Santha, A. Sundaram, and S. Zhang. Linear time algorithm for quantum 2SAT. In *Proceedings of the 43rd International Colloquium on Automata, Languages and Programming*, 2016.

[12] N. Balaji, S. Datta, R. Kulkarni, and S. Podder. Graph properties in node-query setting: effect of breaking symmetry. In *Mathematical Foundations of Computer Science 2016 - 41th International Symposium (MFCS)*, 2016.

[13] R. Bottesch, D. Gavinsky, and H. Klauck. Correlation in hard distributions in communication complexity. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM)*, pages 544–572, 2015.

[14] R. Bottesch, D. Gavinsky, and H. Klauck. Equality, revisited. In *Mathematical Foundations of Computer Science 2015 - 40th International Symposium, MFCS*, pages 127–138, 2015.

[15] G. Braun, R. Jain, T. Lee, and S. Pokutta. Information-theoretic approximations of the nonnegative rank. *Computational Complexity*, 2016.

[16] A. Chailloux, I. Kerenidis, S. Kundu, and J. Sikora. Optimal bounds for parity-oblivious random access codes. *New Journal of Physics*, 18(4):045003, 2016.

[17] A. Chailloux, I. Kerenidis, and B. Rosgen. Quantum commitments from complexity assumptions. *Computational Complexity*, 25(1):103–151, 2016.

[18] S. Fiorini, T. Huynh, G. Joret, and A. Varvitsiotis. The excluded minors for isometric realizability in the plane. Technical Report /1511.08054, arXiv, 2015.

[19] L. Fontes, R. Jain, I. Kerenidis, S. Laplante, M. Lauriere, and J. Roland. Relative discrepancy does not separate information and communication complexity. In *International Colloquium on Automata, Languages, and Programming*, pages 506–516. Springer Berlin Heidelberg, 2015.

[20] D. Gavinsky. Entangled simultaneity versus classical interactivity in communication complexity. In *Proceedings of the 48th Symposium on Theory of Computing (STOC)*, pages 877–884. ACM New York, 2015.

[21] D. Gavinsky, S. Lovett, M. Saks, and S. Srinivasan. A tail bound for read-k families of functions. *Random Structures and Algorithms*, 47:99–108, 2015.

[22] D. Gavinsky and P. Pudlák. On the joint entropy of d-wise-independent variables. *Commentationes Mathematicae Universitatis Carolinae (to appear)*, 2016.

[23] R. Gay, I. Kerenidis, and H. Wee. Communication complexity of conditional disclosure of secrets and attribute-based encryption. In *Annual Cryptology Conference*, pages 485–502. Springer Berlin Heidelberg, 2015.

[24] S. Gharibian and J. Sikora. Ground state connectivity of local hamiltonians. In *Automata, Languages, and Programming: 42nd International Colloquium, ICALP 2015, Kyoto, Japan, July 6-10, 2015, Proceedings, Part I*, pages 617–628. Springer Berlin Heidelberg, 2015.

[25] C. Godsil, D. E. Roberson, B. Rooney, R. Šámal, and A. Varvitsiotis. Unique vector colorings: Rigidity, least eigenvalue frameworks, and 1-walk-regular graphs. Technical Report 1512.04972, arXiv, 2015.
[26] M. Göös, R. Jain, and T. Watson. Extension complexity of independent set polytopes. In *Proceedings of the 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS) (to appear)*, 2016.
[27] M. Grassl, L. Kong, Z. Wei, Z. Yin, and B. Zeng. Quantum error-correcting codes for qudit amplitude damping. Technical Report arXiv:1509.06829, arXiv, 2015.
[28] A. B. Grilo, I. Kerenidis, and A. Pereszlényi. Pointer quantum pcps and multi-prover games. In *Proceedings of MFCS*, 2016.
[29] A. B. Grilo, I. Kerenidis, and J. Sikora. QMA with subset state witnesses. *Chicago Journal of Theoretical Computer Science*, (4), 2016.
[30] P. Harsha, R. Jain, and J. Radhakrishnan. Partition bound is quadratically tight for product distributions. In *Proceedings of the 43rd International Colloquium on Automata, Languages, and Programming (ICALP) (to appear)*, 2016.
[31] G. Ivanyos, M. Karpinski, Y. Qiao, and M. Santha. Generalized Wong sequences and their applications to Edmonds' problems. *Journal of Computer and Systems Sciences*, 81:1373–1386, 2015.
[32] G. Ivanyos, Y. Qiao, and K. Subrahmaniam. Constructive noncommutative rank computation in deterministic polynomial time over fields of arbitrary characteristics. Technical Report 1512.03531v4 [cs.CC], arXiv, 2015.
[33] G. Ivanyos, Y. Qiao, and K. Subrahmaniam. Non-commutative Edmonds' problem and matrix semi-invariants. *Computational Complexity (to appear)*, 2016.
[34] G. Ivanyos and M. Santha. On solving systems of diagonal polynomial equations over finite fields. In *Proceedings of the 9th International Frontiers of Algorithmics Workshop*, pages 125–137, 2015.
[35] R. Jain, Z. Wei, P. Yao, and S. Zhang. Multipartite quantum correlation and communication complexities. *Computational complexity (to appear)*, 2016.
[36] I. Kerenidis, S. Laplante, V. Lerays, J. Roland, and D. Xiao. Lower bounds on information complexity via zero-communication protocols and applications. *SIAM Journal on Computing*, 44(5):1550–1572, 2015.
[37] I. Kerenidis, M. Lauriere, F. L. Gall, and M. Rennela. Information cost of quantum communication protocols. *Quantum Information and Computation*, 16(3&4):0181–0196, 2016.
[38] I. Kerenidis and A. Prakash. Quantum recommendation systems. Technical Report quant-ph/1603.08675, arXiv, 2016.
[39] H. Klauck. The complexity of quantum disjointness. *Manuscript*, 2016.
[40] H. Klauck and S. Podder. The power of unbounded-width polynomial-size branching program. *Manuscript*, 2016.
[41] R. Kothari, D. Racicot-Desloges, and M. Santha. Separating decision tree complexity from subcube partition complexity. In *Proceedings of the 19th International Workshop on Randomization and Computation*, pages 915–930, 2015.
[42] R. Kulkarni and S. Podder. Quantum query complexity of subgraph isomorphism and homomorphism. In *33rd Symposium on Theoretical Aspects of Computer Science (STACS)*, pages 48:1–48:13, 2016.
[43] T. Lee, N. Leonardos, M. Saks, and F. Wang. Hellinger volume and number-on-the-forehead communication complexity. *Journal of Computer and System Sciences*, 2016.
[44] T. Lee, F. Magniez, and M. Santha. Improved query algorithms for triangle finding and associativity testing. *Algorithmica*, 2015.
[45] T. Lee, A. Prakash, R. de Wolf, and H. Yuen. On the sum-of-squares degree of symmetric quadratic functions. In *Proceedings of 31st Conference on Computational Complexity*, 2016. arXiv:1601.02311.
[46] M. Magniez, A. Nayak, M. Santha, J. Sherman, G. Tardos, and D. Xiao. Improved bounds for the randomized decision tree complexity of recursive majority. *Random Structures and Algorithms*, 48:612–638, 2016.
[47] L. Mančinska, D. E. Roberson, and A. Varvitsiotis. On deciding the existence of perfect entangled strategies for nonlocal games. *Chicago Journal of Theoretical Computer Science*, pages 1–16, 2016.
[48] P. Mukhopadhyay and Y. Qiao. Sparse multivariate polynomial interpolation in the basis of Schubert polynomials. *Computational Complexity (to appear)*, 2016.
[49] A. Nayak, J. Sikora, and L. Tunçel. A search for quantum coin-flipping protocols using optimization techniques. *Mathematical Programming*, 156(1):581–613, 2016.
[50] C. Perry, R. Jain, and J. Oppenheim. Communication tasks with infinite quantum-classical separation. *Phys. Rev. Lett. (PRL)*, 115(030504), 2015.
[51] A. Prakash, J. Sikora, A. Varvitsiotis, and Z. Wei. Completely positive semidefinite rank. arXiv:1604.07199, 2016.
[52] J. Sikora. Simple, near-optimal quantum protocols for die-rolling based on integer-commitment. arXiv:1605.08156, 2016.
[53] J. Sikora and A. Varvitsiotis. Linear conic formulations for two-party correlations and values of

nonlocal games. *Mathematical Programming, Series A (to appear)*, 2016.
[54] J. Sikora, A. Varvitsiotis, and Z. Wei. Device-independent dimension tests in the prepare-and-measure scenario. arXiv:1606.03878, 2016.