Computer Science Project: Report 2011-2012

I. GROUP MEMBERS AND VISITORS

The composition of the group:

1. Principal Investigators: Rahul Jain, Hartmut Klauck, Miklos Santha.
2. Post-docs: Thomas Decker (until December 2012), Matthew McKague (until December 2012), Raghav Kulkarni (starts in September 2012), Carlos A. Perez-Delgado, Youming Qiao (since August 2012), Sarvagya Upadhya.
3. Ph.D students: Attila Pereszlényi, Supartha Podder, Ved Prakash, Aarthi Sundaram (since July 2012), Penghui Yao.
4. Visiting Researchers: Itai Arad (Senior Research Fellow, starts in November 2012), Gábor Ivanyos (regularly two months per year), Iordanis Kerenidis (regularly two months per year), Troy Lee (Senior Research Fellow), Shengyu Zhang (regularly two months per year).

II. RESEARCH

A. Summary of achievements

1. Algorithms and Complexity

1. In one model studied heavily in distributed computing several processors are interconnected by bandwidth restricted communication links into a network, but every processor knows only the edges leading to its immediate neighbors. There are 'local' problems that can be solved efficiently even in networks of large diameter, but 'global' problems (like computing a minimum spanning tree) always require at least time proportional to the diameter, and such lower bounds are easy to show even in the case of quantum distributed networks, where the processors are quantum computers, the links allow quantum communication, and the processors may (possibly) share arbitrary entangled states. However, for many problems much stronger lower bounds hold.

   In [4] we extend recent lower bounds on problems like computing the minimum spanning tree to the quantum setting, and even improve upon existing previous classical lower bounds. Our main result is that for many interesting verification and optimization problems a lower bound of $\sqrt{n/(B \log n)}$ holds, where B is the bandwidth of the communication links, even in networks of logarithmic diameter.

   A key ingredient in the proof is the simulation of a suitable network by a new three-player type of communication protocol, called the server model. Alice and Bob receive inputs like in the usual two-player communication complexity model, but there is a third party, the server, who cannot see the inputs. Alice and Bob cannot communicate directly, only via the server. Communications from Alice and Bob to the server incur the usual cost, while the server can communicate to Alice and Bob at no cost (and e.g., set up arbitrary entanglement between the three parties for free). It turns out that known quantum communication complexity techniques apply to this model, while it remains unclear if the server model is really more powerful than entanglement assisted two-player communication complexity.

2. Learning graphs are a very successful model recently introduced by Belovs for designing quantum query algorithms. In his paper introducing them, Belovs showed that the element distinctness algorithm of Ambainis could be designed in this framework, and gave an improved algorithm for determining if a graph contains a triangle. He gave an algorithm to detect a triangle making $O(n^{1.297\cdots})$ queries, improving the previous bound of $O(n^{1.3})$ of Magniez, Santha, Szegedy. In two papers [20, 21], we study the power of learning graphs for detecting constant-sized subgraphs. In the first paper, we give a general algorithm for detecting a k-vertex subgraph that improves the previous bound of $n^{2-2/k}$. In the second paper, we

develop a more sophisticated class of learning graph algorithms. This allows us to improve the algorithm for detecting triangles to $O(n^{1.27})$. We also show how these algorithms can be used in general for problems with constant sized one-certificates, not just graph properties. We use this to give the first algorithm for testing if an operation $\circ : S \times S \to S$ is associative that beats the $n^{3/2}$ trivial application of Grover's algorithm. Our algorithm makes $O(n^{10/7})$ many queries.

3. [18] studies a model of cloud computing for data streaming problems. In this model a space bounded machine wishes to process a data stream to compute some function of the data, assisted by another party that also processes the stream online, but is not space bounded. The two parties communicate, but the results provided by the 'cloud'/prover should be verifiable in the sense of an interactive proof. While in previous work the *total* amount of communication between the prover and the verifying streaming algorithm was restricted, we relax this requirement to small communication *overhead*, which we believe to be more in line with current technology. This allows to give much more simple algorithms for some problems like computing the median and checking whether a streamed matrix has full rank, but also algorithms for problems that are not known to be solvable in models that require small total communication, like the longest increasing subsequence problem. We also show that sometimes an additional verification phase after the end of the data stream is necessary, e.g. for the tight approximation of the infinity frequency moment.

4. The preprint [5] is a new, full version with substantial changes of a conference paper from 2003 on solving the hidden subgroup problem in a wide class of solvable groups on quantum computers in polynomial time. The manuscript contains a new, elegant variant of a procedure which reduces the HSP of solvable groups to a special hidden shift problem in Abelian group as well as novel applications of the method, such as a subexponential time hidden subgroup algorithm in general solvable groups which works in quasi-polynomial time in solvable groups of constant exponent.

5. In [15] we have provided fast parallel approximation algorithm for mixed packing and covering semidefinite programs, where the covering constraints are linear and packing constraints are semidefinite. This extends on our previous work on fast parallel approximation algorithm for positive semidefinite programs ("A parallel approximation algorithm for positive semidefinite programming." R. Jain and P. Yao. The 52nd Annual IEEE Symposium on Foundations of Computer Science (FOCS) 2011) by providing fast parallel approximation algorithm for a larger class. Also our current algorithm is conceptually simpler and significantly faster than the previous work.

Future Work: We are working on a new quantum algorithm for special cases of the hidden polynomial problem related to certain nilpotent groups of nilpotency class higher than 2 and possible applications to other instances of the hidden polynomial problems. We would also like to to clarify the relationship between learning graphs and resistance networks, and further apply this computational model to various problems including Merkle's puzzles. We wish to extend the work in [15] to arrive at fast parallel approximation algorithm for mixed packing and covering semidefinite programs where both the packing and covering constraints are semidefinite.

2. Interactive Proofs, Zero Knowledge, Quantum Games

1. In [35], a simple yet rich model of quantum strategic games is proposed, and quantitative questions such as how much advantage playing quantum strategies can provide are studied. The paper also defines correlation complexity as a complexity-theoretic version of the Bell-style theorems to differentiate the power of shared classical randomness and quantum entanglement. In follow-up work [34], a sufficient and necessary condition of a state being a quantum correlated equilibrium is given, and in [14], a full characterization of the quantum correlation complexity is shown. Other work about quantum games include [17], which designs a protocol to reach a correlated equilibrium by quantum communications among the selfish players, and [37], which demonstrates in both theory and experiments the power of using quantum strategies in a more fair setting.

2. In [17] we have studied the notion of correlated equilibria of classical games and have shown that allowing quantum communication prior to the game, enables the quantum agents to achieve such an equilibrium, hence largely improving over what is possible classically (which is either a Nash equilibrium or a computational correlated equilibrium). This provides another example of a major advantage of quantum information processing: quantum communication enables players to achieve a real correlated equilibrium, which is impossible with classical communication.

3. In [29] we have shown that in the unconditional security model, a single quantum strong coin flip with security guarantees that are strictly better than in any classical protocol is possible to implement with current technology. Our protocol takes into account all aspects of an experimental implementation like losses, multi-photon pulses emitted by practical photon sources, channel noise, detector dark counts and finite quantum efficiency. Our protocol is in principle implementable using attenuated laser pulses, with no need for entangled photons or any other specific resources.

4. The paper [33] studies bit-commitment and coin flipping in the device-independent model. In the distrustful quantum cryptography model the different parties have conflicting interests and do not trust one another. Nevertheless, they trust the quantum devices in their labs. The aim of the device-independent approach to cryptography is to do away with the necessity of making this assumption, and, consequently, significantly increase security. It is an open question whether the scope of the device-independent approach also extends to protocols in the distrustful cryptography model, thereby rendering them 'fully' distrustful. In our work, we showed that at least for bit-commitment and coin flipping - two of the most basic primitives within the model - the answer is positive.

5. In [12] we have provided a conceptually simpler and much shorter proof of the 'Substate theorem'. The Substate theorem, which was first shown in (R. Jain, J. Radhakrishnan and P. Sen. "A new information-theoretic property about quantum states with an application to privacy in quantum communication." Journal of ACM (JACM), Volume 56, Issue 6, Article No.: 33, September, 2009), provides a useful handle on a fundamental information theoretic quantity called the 'Relative entropy' between two quantum states. It has found many applications over the years in communication and cryptography. Our new proof is obtained by using the minimax and semidefinite programming duality.

6. In [6] we consider three variants of quantum Merlin-Arthur proof systems with multiple Merlins. Our first result shows that the expressive power of such proof systems where each Merlin sends logarithmic-size proofs is equal to QCMA. Our second result concerns with the class BellQMA(poly), characterized by a verifier who first applies unentangled, non-adaptive measurement on each proof, followed an efficient quantum verification circuit on the measurement outcomes. We show that if the number of outcomes per proof is polynomial, then the proof system can be simulated by QMA. Finally, we give an alternate proof of a result of Harrow and Montanaro [FOCS, p:633-642 (2010)]. Using cone programming duality, we show that the class SepQMA(poly), where verifier's measurement operator corresponding to outcome 'accept' is a fully separable operator, admits perfect parallel repetition theorem.

7. We consider several aspects of interaction between classical verifiers and uncharacterized quantum devices. In [28] we establish bounds on such quantum devices in terms of the extent to which they can violate the CHSH inequality. In a more general scenario, [27] considers the role that complex numbers play in the computational power of various quantum computing models. In particular we consider the interactive proof models QMIP, QIP, QMA and QSZK. In all cases we find that restricting to real numbers does not change the power of the model. Finally, [26] considers the recursive Fourier sampling problem, historically the first to show an exponential speedup of quantum computing over classical. We show that there is an interactive proof system for this problem in which the prover can be quantum polynomially time bounded.

8. A central question in physics for the last 20 years has been what are the fundamental capabilities of quantum precision measurement. Usually, the ultimate limits in quantum metrology are associated with the notion of the Heisenberg limit expressed in terms of the physical resources used in the measurement procedure. Over the years, a variety of different physical

resources were introduced, leading to a confusion about the meaning of the Heisenberg limit. The confusion was compounded when several authors claimed to show methods that could break the Heisenberg limit. We set out to solve this conundrum by refining the definition limit such that it becomes a fundamental, unbroken and unbreakable, limit of quantum metrology. Our approach was to introduce a universal resource count. This leads to the ultimate formulation of the Heisenberg limit for quantum metrology. Our work is explained in detail in [36]

9. Quantum imaging is a young area that promises many advantages over classical protocols. Unlike metrology, however, little is known about the ultimate bounds on imaging protocols. In particular, it has so far been unknown how to compare classical and quantum imaging procedures. We developed a framework in which it is possible to ascertain the limits of any imaging system, both classical and quantum. This allows us to define a figure of merit on various protocols in a wide range of applications, and compare them directly. We also present the fundamental limit on the resolution in the form of Cramér-Rao bounds for classical and quantum imaging. The resolution can be estimated from the image itself. A pre-print of our results can be found in [30]

10. Several variants of quantum interactive proofs systems (QIP) and quantum Arthur-Merlin games (QMA) were studied. One modification one can make to the class QIP is to restrict some messages to be short. As opposed to the usual setting, where the messages can be polynomial in length, short here means that some messages are only allowed to be logarithmic. These restrictions are usually not interesting in the classical setting, as the verifier can simply eliminate the logarithmic-length message by enumerating all possibilities. This is not the case in the quantum setting. However, in some cases it is known that the sort messages can be eliminated. Some of these cases have been studied by Beigi, Shor and Watrous. They raised the open question that if in one of the setting the short message is replaced by a 'short interaction' then is it true that the short interaction can be eliminated? A positive answer to this is given in [31]. The study of another variant of QIP and QMA were initiated by Ito, Kobayashi and Watrous. They considered cases where the gap between the completeness and soundness parameter is very small, meaning inverse-exponential or even smaller. They showed that the power of QIP increases to EXP in this case. We considered this modification in the case of QMA[k], i.e., QMA with k unentangled provers. We showed that in this case the expressive power of the class will become equal to NEXP, and it is still true if the verifier can only measure each proofs separately. This work is done in [32].

Future Work: We wish to further explore the power of different models of interactive proofs specially in the setting of low soundness gap (exponentially small/unbounded). We wish to further explore different aspects of quantum strategic games.

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

1. A fundamental question in complexity theory is how the resources needed to solve many independent instances of a problem scale with those needed for one instance. When faced with solving k-independent instances of a problem one can always run the algorithm for one instance k times in parallel. This requires k times the resources and, if the original success probability was p, will have success probability p^k. A strong direct product theorem for a computational model states that this naive procedure is the best possible—any algorithm for solving k instances of a problem, even using k times the resources needed for one instance, will have exponentially small success probability. This is a very powerful statement and known to be true only for very few computational models. In [22] we show a strong direct product theorem for the model of quantum query complexity. For boolean functions we are able to show an even stronger result known as an XOR lemma: given k times the resources needed to compute a boolean function with bounded-error, any quantum query algorithm will have exponentially small advantage (in k) over random guessing in computing the parity of the function on k independent instances.

2. We have also studied direct product theorems in communication complexity. In [13] we have settled the direct product conjecture in the affirmative for all relations for bounded round public-coin communication protocols. This work builds on previous work [11] in which we

have settled this conjecture in the affirmative for all relations in the public-coin one-way model of communication. In [11] we have also provided a direct product result for the two-way public-coin model which as an application implies direct product for many functions and relations including the well studied "set disjointness" function.

3. The paper [19] studies the power of quantum communication protocols with one-sided error and entanglement. While the complexity of well-known functions like equality and disjointness was resolved a decade ago by de Wolf in the model without entanglement (but with one-sided error), it turns out that at least the complexity of equality was widely open if one allows entanglement to be shared by Alice and Bob. The reason is as follows: lower bound methods for quantum communication complexity fall into two categories: norm-based and rank-based. Norm-based methods (all subsumed by the γ_2 method) directly apply to the model with entanglement, due to the linearity of norms. Rank-based methods however do not directly apply to protocols with entanglement. Equality is the prototypical problem for which the γ_2 method does not yield large lower bounds. We resolve this by using the venerable "fooling set" method to prove new lower bounds on the one-sided error quantum communication complexity in the presence of entanglement, giving tight lower bounds for equality and disjointness.

   The proof proceeds by simulating protocols via nonlocal games, and directly analyzing the effect of measurements on any given entangled state.

4. [8] considers the communication complexity of a number of graph properties where the edges of the graph G are distributed between Alice and Bob (i.e., each receives some of the edges as input). The main results are:

   (a) An $\Omega(n)$ lower bound on the quantum communication complexity of deciding whether an n-vertex graph G is connected, nearly matching the trivial classical upper bound of $O(n \log n)$ bits of communication.

   (b) A deterministic upper bound of $O(n^{3/2} \log n)$ bits for deciding if a bipartite graph contains a perfect matching, and a quantum lower bound of $\Omega(n)$ for this problem.

   (c) A $\Theta(n^2)$ bound for the randomized communication complexity of deciding if a graph has an Eulerian tour, and a $\Theta(n^{3/2})$ bound for the quantum communication complexity of this problem.

5. In [14] we study the correlation complexity (or equivalently, the communication complexity) of generating a bipartite quantum state ρ. When ρ is a pure state, we completely characterize the complexity for approximately generating ρ by a corresponding approximate rank, closing a gap left in Ambainis, Schulman, Ta-Shma, Vazirani and Wigderson (SIAM Journal on Computing, 32(6):1570-1585, 2003). When ρ is a classical distribution P, we tightly characterize the complexity of generating P by the *psd-rank*, a measure recently proposed by Fiorini, Massar, Pokutta, Tiwary and de Wolf (STOC 2012). We also present a characterization of the complexity of generating a general quantum state.

6. In [16] we show that almost all known lower bound methods for randomized communication complexity are also lower bounds for the internal information complexity, a measure that is always at most as large as the randomized communication and that has applications to direct sum theorems and in cryptography. In particular, we derive a relaxed version of the partition bound of Jain and Klauck and prove that it lower bounds the information complexity of any function. Our relaxed partition bound subsumes all norm based methods (e.g. the γ_2 method) and rectangle-based methods (e.g. the rectangle/corruption bound, the smooth rectangle bound, and the discrepancy bound), except the partition bound.

7. Linear programming is a jewel of computer science, both efficient to solve from a theoretical perspective and enormously successful in practice. Linear programming is often used as an integral component of algorithms to solve large scale NP-hard problems that arise in practice, and showing that an NP-hard problem has a polynomial size linear programming formulation would imply P=NP.

   A beautiful theorem of Yannakakis going back 20 years relates the size of linear programming formulations to a quantity known as non-negative rank. This is like the rank, but requires all the vectors in the factorization to be non-negative. A recent paper used this connection

to show super polynomial lower bounds on the size of linear programming formulations for the Traveling Salesman Problem (TSP).

An analog to the theorem of Yannakakis also holds for the size of semidefinite programming formulations, with the rank quantity now becoming the positive semidefinite rank. This is a little studied notion and appears quite difficult to lower bound. Most lower bounds on nonnegative rank—including those used for the application TSP—are support based bounds, meaning they only use the zero/non-zero structure of the matrix. In [23], we study support based lower bounds for positive semidefinite rank, and characterize their power. There is an interesting connection to quantum communication complexity: the positive semidefinite rank is characterized by the (logarithm of the) quantum communication complexity of a protocol that computes the matrix in expectation; the best support based lower bound is equal to the (logarithm of the) nondeterministic quantum communication complexity.

Future Work: Our plans include developing lower bound methods for the nonnegative and positive semidefinite rank, to clarify the relationship between information complexity and various lower bound methods for communication complexity, to study the direct product question for variations of the partition bound, and to further study the power of quantum and classical interactive proofs in communication complexity.

B. Selected invited talks

1. Rahul Jain, invited speaker at the *Workshop on Recent Progress in Quantum Algorithms*, University of Waterloo and Perimeter Institute, Waterloo, Canada, April, 2012.
2. Rahul Jain, contributed talk at the *15th Workshop Quantum Information and Processing*, Montreal, Canada, December 2011.
3. Iordanis Kerenidis, featured talk at the *15th Workshop Quantum Information and Processing*, Montreal, Canada, December 2011. Title "Optimal bounds for quantum bit commitment".
4. Troy Lee, featured talk at the *15th Workshop Quantum Information and Processing*, Montreal, Canada, December 2011. Title "A strong direct product theorem for quantum query complexity".
5. Troy Lee, featured talk at the *15th Workshop Quantum Information and Processing*, Montreal, Canada, December 2011. Title "Quantum query complexity of state conversion".
6. Miklos Santha, contributed talk at the *15th Workshop Quantum Information and Processing*, Montreal, Canada, December 2011. Presented talk on "Hidden Symmetry Subgroup Problems".
7. Miklos Santha, invited speaker at *2nd Heilbronn Quantum Algorithms Day*, Bristol, UK, February 2012.
8. Miklos Santha, invited speaker at the *French - Israeli Workshop on Foundations of Computer Science*, Paris, France, May 2012.
9. Miklos Santha, invited speaker at the *Conference on Quantum Computing of the Fédération de Recherches Mathématiques de Paris*, Paris, France, May 2012.
10. Miklos Santha, invited speaker at *Workshop on Quantum Computer Science*, Barcelona, Spain, May 2012.

III. OTHERS

1. Awards

1. Rahul Jain received Young Researcher Award, National University of Singapore, 2012 (http://www.nus.edu.sg/uawards/2012/winners/rahul_jain.html).

2. Professional Activities

1. Rahul Jain is on the program committee of the 32nd IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2012).

2. Hartmut Klauck was on the program committee of the 27th IEEE Conference on Computational Complexity (CCC 2012).

3. Miklos Santha was on the programme committe of 6th Conference on Theory of Quantum Computation, Communication and Cryptography (TQC 2011) and of the 5th International Computer Science Symposium in Russia (CSR 2011).

4. Miklos Santha is member of the editorial board of the International Journal of Quantum Information.

3. Outreach

1. Rahul Jain participated in the SoC-Vietnam workshop 2012, orgranized by School of Computing, National University of Singapore, held at Ho-Chi-Minh city, Vietnam, March 2012.

2. Rahul Jain participated in the annual student outreach program by School of Computing, National University of Singapore, 2012.

3. Troy Lee demonstrated soap bubble computers to explain P and NP to NUS alumni and their children at Alumni Day.

---

[1] Xiaohui Bei, Ning Chen, Shengyu Zhang. On the Complexity of Trial and Error. arXiv:1205.1183.

[2] Aleksandrs Belovs and Troy Lee. Quantum Algorithm for k-distinctness with Prior Knowledge on the Input. arXiv:1108.3022

[3] Jop Briet, Harry Buhrman, Troy Lee and Thomas Vidick. All Schatten spaces endowed with the Schur product are Q-algebras. *Journal of Functional Analysis*, Vol. 262, Issue 1, pp. 1-9, 2012.

[4] Michael Elkin, Hartmut Klauck, Danupon Nanongkai and Gopal Pandurangan. Quantum Distributed Network Computing: Lower Bounds and Techniques. arXiv:1207.5211.

[5] K. Friedl, G. Ivanyos, F. Magniez, M. Santha and P. Sen. Hidden translation and orbit coset in quantum computing. arXiv:quant-ph/0211091v2.

[6] Sevag Gharibian, Jamie Sikora, and Sarvagya Upadhyay. QMA variants with polynomially many provers. arxiv: 1108.0617

[7] G. Ivanyos. Finding hidden Borel subgroups of the general linear group. Quantum Information and Computation Vol. 12, pp. 0661-0669, 2012.

[8] G. Ivanyos, Hartmut Klauck, Troy Lee, Miklos Santha and Ronald de Wolf. New bounds on the classical and quantum communication complexity of some graph properties. arXiv:1204.4956.

[9] G. Ivanyos, L. Rónyai, M. Karpinski and N. Saxena. Trading GRH for algebra: algorithms for factoring polynomials and related structures. Matematics of Computation Vol. 81, pp. 493-531, 2012.

[10] G. Ivanyos, L. Sanselme and M. Santha. An efficient quantum algorithm for the hidden subgroup problem in nil-2 groups. Algorithmica Vol. 62, pp. 480-498, 2012.

[11] R. Jain. New strong direct product results in communication complexity. ECCC-TR11-024, 2011.

[12] R. Jain and A. Nayak. Short proofs of the quantum Substate Theorem. *IEEE Transactions on Information Theory*, Volume: 58 , Issue: 6, pp. 3664 - 3669, 2012.

[13] R. Jain, A. Pereszlényi and P. Yao. A direct product theorem for bounded-round public-coin randomized communication complexity. In proceedings of the *53rd Annual IEEE Symposium on Foundations of Computer Science* (FOCS) 2012.

[14] R. Jain, Y. Shi, Z. Wei and S. Zhang. Correlation/Communication complexity of generating bipartite states, 2012. arXiv:1203.1153.

[15] R. Jain and P. Yao. A parallel approximation algorithm for mixed packing and covering semidefinite programs, 2012. arXiv:1201.6090.

[16] Iordanis Kerenidis, Sophie Laplante, Virginie Lerays, Jeremie Roland, David Xiao. Lower bounds on information complexity via zero-communication protocols and applications. *53rd Annual Symposium on Foundations of Computer Science* (FOCS), 2012.

[17] Iordanis Kerenidis, Shengyu Zhang. A quantum protocol for sampling correlated equilibria unconditionally and without a mediator. *Theory of Quantum Computation, Communication and Cryptography* (TQC), 2012.
[18] Hartmut Klauck and Ved Prakash. Streaming Computations with a Loquacious Prover. Manuscript.
[19] Hartmut Klauck and Ronald de Wolf. Fooling One-Sided Quantum Protocols. arXiv:1204.4619.
[20] Troy Lee, Frederic Magniez and Miklos Santha. A learning graph based quantum query algorithm for finding constant-size subgraphs. arXiv:1109.5135
[21] Troy Lee, Frederic Magniez and Miklos Santha. Improved quantum query algorithms for triangle finding and associativity testing. Submitted to SODA 2013.
[22] Troy Lee and Jeremie Roland. A strong direct product theorem for quantum query complexity. *In Proceedings of the 27th IEEE Conference on Computational Complexity.* arXiv:1104.4468
[23] Troy Lee and Dirk Oliver Theis. Support based bounds for positive semidefinite rank. arXiv:1203.3961.
[24] F. Magniez, A. Nayak, P. Richter and M. Santha. On the hitting times of quantum versus random walks. *Algorithmica*, Vol. 63, No.1, pp. 91-116, 2012.
[25] F. Magniez, M. de Rougemont, M Santha and X. Zeitoun. The complexity of approximate Nash equilibrium in congestion games with negative delays. *7th Workshop on Internet and Network Economics*, pp. 266-277, 2011.
[26] Matthew McKague. Interactive proofs with efficient quantum prover for recursive Fourier sampling. arXiv:1012.5699.
[27] Matthew McKague. On the power quantum computation over real Hilbert spaces. arXiv:1109.0795.
[28] Matthew McKague, Tzyh Haur Yang, Valerio Scarani. Robust Self Testing of the Singlet. arXiv:1203.2976.
[29] Anna Pappa, André Chailloux, Eleni Diamanti, Iordanis Kerenidis. Practical quantum coin flipping. *Phys. Rev. A* 84, 052305, 201
[30] Carlos A. Perez-Delgado, Mark E. Pearce, Pieter Kok Cramer-Rao. Bounds for Classical and Quantum Imaging. arXiv:1204.5209.
[31] Attila Pereszlényi. On quantum interactive proofs with short messages. arXiv:1109.0964.
[32] Attila Pereszlényi. Multi-Prover Quantum Merlin-Arthur Proof Systems with Small Gap. arXiv:1205.2761.
[33] J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, S. Massar. Fully Distrustful Quantum Bit Commitment and Coin Flipping. *Phys. Rev. Letters* 106, 220501, 20
[34] Zhaohui Wei, Shengyu Zhang. On characterizing quantum correlated equilibria. arXiv:1105.5353.
[35] Shengyu Zhang. Quantum Strategic Game Theory. *Proceedings of the 3rd Innovations in Theoretical Computer Science (ITCS)*, pp. 39-59, 2012
[36] Marcin Zwierz, Carlos A. Perez-Delgado, and Pieter Kok. Ultimate limits to quantum metrology and the meaning of the Heisenberg limit. *Phys. Rev. A 85*, 042112 (2012)
[37] Chong Zu, Yuexuan Wang, Xiuying Chang, Zhaohui Wei, Shengyu Zhang, Luming Duan. Experimental demonstration of quantum gain in a zero-sum game. *New Journal of Physics*, Vol. 14, pp. 39-59, 2012.