Teze disertace
k získání vědeckého titulu “doktor věd”
ve skupině věd fyzikálně–matematických

Quantum-mechanical communication protocols: their limitations and super-classical capabilities

Komise pro obhajoby doktorských disertací v oboru
Matematické struktury

Jméno uchazeče: *Dmitry Gavinsky*

Pracoviště uchazeče: *Matematický ústav Akademie věd České republiky, oddělení matematické logiky a teoretické informatiky*

Místo a datum: *Praha, 1.12.2020.*

Contents

Abstract

Author's humble contribution to the research area of *quantum communication complexity* is presented.

A core goal in the field is identifying those communication regimes where the laws of quantum mechanics offer qualitative advantage in comparison to the power of classical models. One of the main differences between communication models is their topology – namely, the layout of communication channels. A number of works covered in Part II of this dissertation can be viewed as a sequence of steps aiming for an *ultimate separation*, that is, an example of a communication problem that can be solved efficiently in the weakest quantum communication model, while being hard for the strongest classical one.

It is also interesting to understand the *limitations* of quantum communication. Two woks that are covered in Part III of this dissertation bound the possible advantage of quantum communication over the classical one.

Another endeavour of quantum communication complexity is characterising the *complexity of concrete representative problems* in various models of interest. The two most important communication problems are *Equality (Eq)* and *Disjointness (Disj)*, and Part IV of this dissertation covers works that analyse the complexity of these two problems in various regimes.

Besides the physical nature of the available communication channels (either classical or quantum) and their layout, communication models can differ in terms of the *available shared resources*: either classical randomness or quantum entanglement. Several works that

study more subtle aspects of these resources are covered in Part V of this dissertation.

Quantum protocols are a special case of quantum algorithms, and we know how to prove that some quantum protocols outperform exponentially the best classical ones. This can be useful in those computational scenarios where quantum advantage over the classical counterpart is desired. In Part VI of this dissertation we cover several works where the study of quantum protocols was prolific in the fields of computational complexity, computational learning theory and computational cryptography.

Most of the works covered by this dissertation are forming natural sequences of incremental improvements, several of those sequences might even be seen as having converged to their natural goals. It is author's hope that this presentation will highlight some of the remaining interesting questions, as well as lead to new insights into them.

Chapter 1

Introduction

The observed reality may not be classical. Among the non-classical physical theories of nowadays, *quantum mechanics* is, probably, the most adequate: on the one hand, it is very accurate in predicting the *probabilities* of experimental outcomes (and there are reasons to believe that this is the best we can hope for prophesy-wise); on the other hand, quantum mechanics is compatible with other plausible physical theories in the regimes that we have tested experimentally or can hope to be able to test any time soon.

The significance of understanding quantum mechanics seems to be at least two-fold. On the one hand, the theory is among the frontiers of our observation-predicting capabilities, and the philosophical reflection of the possibility of a priori physical knowledge has led to some of the deepest ontological and epistemological doctrines so far. On the other hand, quantum – as opposed to classical – mechanics is intimately related to the problem of causation, which might be not as fundamental as the problem of a priori synthetic knowledge, but is nevertheless very important.

Thus, we are interested in identifying and investigating those experimental scenarios where the predictions of quantum mechanics are, so to say, *most non-classical.* This problem makes sense, in particular, in the computational context: e.g., we may ask whether *computational devices that are allowed to perform every operation admitted by quantum mechanics are qualitatively stronger than*

– *apparently, more limited – their classical counterparts.* While addressing this question, we would naturally like to accept only the most fundamental and intuitively-indisputable assumptions in the analysis.

1.1 Communication complexity

Many basic questions in computer science are still destitute of any mathematical understanding, which often results in making a priori assumptions that do not represent any fundamental intuition. Among the most yawning gaps is the field of *computational complexity*: in the original and most natural form it asks whether a given computational problem has an efficient algorithm in the model of *Turing machines* – while the researchers have collected quite a few impressive algorithms, the current ability to prove that a problem admits no efficient solution on a Turing machine does not exceed a couple of somewhat insightful but mathematically-trivial imitations of Cantor's diagonal argument.

A possible way to conduct well-grounded research in computational complexity nowadays is to study simpler computational models.[1] Among the richest models that we already know how to analyse – at least, in some cases – is the setting of *communication complexity*. Here is a brief informal introduction of its central concepts:

- In the model of *bipartite* communication there are two *players*, *Alice* and *Bob*, who receive one portion of input each: Alice gets x and Bob gets y. Their goal is to use the allowed type of communication (as described next) in order to compute an answer that would be correct with respect to the received pair (x, y).
- The three principal bipartite *layouts* are *two-way (interactive) communication*, *one-way communication* and *simultaneous message passing (SMP)*. In the first case the players can ex-

[1] Here simplicity does not necessarily mean being more limited computationally, but rather refers to informal *mathematical tractability*.

change messages interactively before answering, in the second case only Alice can send a message to Bob (who then answers), in the third case both Alice and Bob send one message each to a third participant – the *referee* (who then answers).

- Communication problems determine which answers are correct for the given input. The three main *types of problems* are *total functions*, *partial functions* and *relations*: in the first case there is exactly one correct answer for each possible pair of input values, and the set of those pairs equals the direct product of possible inputs of Alice and possible inputs of Bob; the second case is similar, but the set of possible inputs can be arbitrary; in the third case multiple correct answers for the same input values are allowed.
- An *efficient* solution is a communication protocol where the players use at most poly-logarithmic (in the input length) amount of communication and produce a right answer with high confidence.
- Communication models can be strengthened by *shared randomness*, which corresponds to allowing the players to use *mixed strategies* (this can be helpful only in the weakest among the layouts – the *SMP*), or by *shared entanglement*, which allows the players to share any (input-independent) quantum state and use it while running the protocol.[2]

[2] Sometimes in this work we call a model *bare* to emphasise that it allows no shared resources.

Chapter 2

Quantum communication complexity

Quantum communication complexity has been an active area of research over the last few decades. Among numerous results in the field, the most relevant to the context of demonstrating super-classical capabilities of quantum models are the following:

- In 1998 a *partial function* was demonstrated [BCW98] for which in *zero-error regime* quantum protocols had exponential advantage over the classical ones (both one-way and interactive).
- In 1999 a *partial function* was demonstrated [Raz99] that had an efficient *quantum two-way protocol*, but no efficient *classical two-way protocol*.
- In 2001 a *total function* was demonstrated [BCWdW01] that had an efficient *quantum simultaneous-messages protocol without shared randomness*, but no efficient *classical simultaneous-messages protocol without shared randomness*.
- In 2004 a *relation* was demonstrated [BYJK04] that had an efficient *quantum simultaneous-messages protocol without shared randomness*, but no efficient *classical one-way protocol*.
- In 2006 a *partial function* was demonstrated [GKK+08] that had an efficient *quantum one-way protocol*, but no efficient

classical one-way protocol.

- In 2007 a *multipartite relational problem* was demonstrated [GP08] that had an efficient *quantum simultaneous-messages protocol*, but no efficient *classical simultaneous-messages protocol* or *classical non-interactive one-way protocol.*
- In 2008 a *relation* was demonstrated [Gav08a] with an efficient *quantum one-way protocol*, but no efficient *classical two-way protocol.*
- In 2010 a *partial function* was demonstrated [KR11] with an efficient *quantum one-way protocol*, but no efficient *classical two-way protocol.*
- In 2016 a *partial function* was demonstrated [Gav20b] with an efficient *quantum simultaneous-messages protocol with shared entanglement*, but no efficient *classical two-way protocol.*
- In 2017 a *partial function* was demonstrated [Gav19] with an efficient *quantum simultaneous-messages protocol without shared randomness*, but no efficient *classical simultaneous-messages protocol*, even *with shared randomness.*
- In 2020 a *relation* was demonstrated [Gav20a] with an efficient *quantum simultaneous-messages protocol without shared randomness*, but no efficient *classical two-way protocol.*

Among the works listed above there are a few that represent the research conducted by the author and will be covered in Part II of this dissertation.

A core concrete goal in the field is identifying those communication regimes where the predictions of quantum mechanics are as far as possible from those of classical mechanics. The separations listed above can be viewed as a sequence of efforts aiming for an *ultimate separation* – a communication problem that can be solved efficiently in the *weakest* quantum communication model, while being hard for the *strongest* classical one.

Part II of this dissertation start with [GKK$^+$08], where the same regime of one-way communication is considered in both quantum and classical cases and the supremacy of the former is argued. In [Gav08a] a stronger separation is given – namely, a problem is presented for which a *weaker layout* of quantum communication – namely, one-way – offers exponential advantage over a *stronger layout* of classical communication – namely, two-way. In [Gav20b] the layout gap is made even wider: the *weakest bipartite layout* of quantum communication – namely, simultaneous message passing (*SMP*) – exhibits exponential advantage over two-way classical communication. The main drawback of [Gav20b] was the need of shared entanglement in order for an efficient quantum protocol to exist, and this has been addressed in the most recent separation [Gav20a] from the above list: there a relational problem is given that is easy for quantum *SMP*, but hard for classical two-way communication.

2.1 Limitations of quantum communication

Investigating the limitations of quantum communication models is very interesting. Although there are some known results that bound the possible advantage of quantum communication over the classical one, here our understanding is much more limited.

The following two woks represent author's research and will be presented in Part III of this dissertation:

- In 2005 two *bipartite relational problems* were demonstrated [GKRdW09] that had the following properties:
  - the first relation had an efficient *classical simultaneous-messages protocol with shared randomness*, but no efficient *quantum simultaneous-messages protocol without shared randomness* – this implied that quantum communication is, in general, not strong enough to replace shared randomness in efficient classical simultaneous-messages protocols;
  - the second relation had an efficient *classical simultaneous-messages protocol with shared entanglement*, but no efficient *quantum simultaneous-messages protocol without shared entanglement*, even *with shared randomness* – this implied that shared entanglement, even combined with classical communication, can be qualitatively stronger

than quantum communication.

- In 2008 it was proved [GRdW08] that the model of *simultaneous messages where one party is quantum and the other is classical* could never be qualitatively stronger than the model of *classical simultaneous message passing* with respect to *functional problems* – as opposed to the case of *relational problems*, where the quantum-classical model was already known to be exponentially stronger than its classical counterpart in some cases.

2.2 Quantum communication complexity of concrete problems

The results mentioned so far can be viewed as *structural*: they reflect the qualitative relation of the power of the analysed quantum communication models and their classical counterparts. Another endeavour of quantum communication complexity is characterising the complexity of concrete representative problems in various models of interest.

Arguably, the two most important and widely studied communication problems are

- *Equality (Eq)*, where Alice receives $\mathcal{X} \in \{0,1\}^n$, Bob receives $\mathcal{Y} \in \{0,1\}^n$ and their purpose is to decide whether $\mathcal{X} = \mathcal{Y}$, and
- *Disjointness (Disj)*, where Alice receives $\mathcal{X} \subseteq [n]$, Bob receives $\mathcal{Y} \subseteq [n]$ and their purpose is to decide whether $\mathcal{X} \cap \mathcal{Y} = \emptyset$.

Both *Eq* and *Disj* have been a subject of author's research:

- Computing $Eq(\mathcal{X}, \mathcal{Y})$ is easy in any randomised model that allows at least one message to be sent by Alice to Bob (or vice versa) – that is, analysing its communication complexity can be non-trivial (and in fact is often rather challenging) only in various *SMP*-regimes (one such example is the quantum-classical regime that was analysed in [GRdW08], as addressed above). In [GBK15b] we develop a new lower bound method for analysing the complexity of *Eq*, which allows us to obtain the following:

  - the tight lower bounds of $\Omega(\sqrt{n})$ for both *Eq* and its negation in the *non-deterministic version* of the quantum-classical *SMP*, where Merlin is also quantum – this is the strongest known version of *SMP* where the complexity of these problems remain high (previously known lower-bound techniques seem to be insufficient for this);
  - a unified view of the communication complexity of both *Eq* and its negation, allowing to obtain tight characterisation in all previously studied and a few newly introduced versions of SMP, including all possible combination of either quantum or randomised Alice, Bob and Merlin in the non-deterministic case.

  In the same paper [GBK15b] we presented new protocols for both *Eq* and its negation that achieved optimal trade-off complexities in some asymmetric versions of non-deterministic quantum-classical *SMP*.

- In [GBK15a] we studied the effect that the amount of correlation in the input distribution had on the communication complexity. In particular, we gave a tight characterisation of both the randomised and the quantum communication complexity of *Disj* under distributions with mutual information k, showing that it was, respectively, $\Theta\left(\sqrt{n(k+1)}\right)$ and $\widetilde{\Theta}\left(\sqrt[4]{n(k+1)}\right)$ for all $0 \leq k \leq n$.

These two works will be presented in Part IV of this dissertation.

2.3 Investigating subtle aspects of quantum communication protocols

Besides the physical nature of the available communication channels (either classical or quantum) and their layout (*SMP*, one-way or two-way), communication models can differ in several other aspects. A very important parameter of a model is the *availability of shared* *resources* (randomness or entanglement): as we saw in the beginning of this chapter, it can severely affect the resulting model strength.

There is a theorem by Newman [New91] stating that the number of shared random bits required for solving any communication problem with any constant-bounded error can be at most logarithmic in the input length. In [Gav08b] we proved that the same was not true with respect to the bits of entanglement: We presented a wide range of tight – up to poly-logarithmic factors – complexity trade-off evaluations that demonstrated the dependence between the available number of the bits of entanglement and the corresponding communication complexity. It followed that some communication problems required $n^{\Omega(1)}$ bits of entanglement for their asymptotically-optimal solution.

In [GIW13] we studied the role of shared randomness in the context of multi-party number-in-hand *SMP* communication. This setting demonstrated some interesting properties that had no direct analogues in the two-party regimes, both classical and quantum. Similarly to the bipartite case, here quantum communication cannot, in general, replace shared randomness; on the other hand, for $k \geq 3$ players the separations of [GIW13] are qualitatively stronger than the corresponding bipartite results (as discussed in Section 2.1):

- in the two-party case only a relational communication problem is known where shared randomness cannot be efficiently replaced by quantum communication, and for $k \geq 3$ we construct a partial function with such properties;
- in the two-party case the advantage of classical communication with shared randomness can be at most exponential in terms of the resulting complexity, while for $k \geq 3$ we show a gap of $O(1)$ vs. $n^{\Omega(1)}$: in particular, unlike in the bipartite case, it is not in general possible to use quantum communication for efficient simulation even of a three-bit three-party classical protocol with shared randomness.

A classical *SMP*-protocol with shared randomness can be replaced by a quantum *SMP*-protocol with at most exponential complexity overhead, the corresponding technique is called *quantum* *fingerprinting* [BCWdW01, Yao03]. In [GKdW06] we studied this technique in detail and demonstrated some of its strengths and weaknesses:

- it turned out that every many-round quantum protocol with unlimited shared entanglement could be simulated by a quantum protocol using neither shared randomness nor entanglement, with the resulting complexity overhead still being at most exponential;
- on the other hand, we tightly characterised the power of the quantum fingerprints by making a connection to arrangements of homogeneous half-spaces with maximal margin – a notion that had been studied in the context of computational learning theory; we used this correspondence between the two notions to prove that for almost all functions quantum fingerprinting protocols were exponentially worse even than classical deterministic protocols.

Works [GKdW06, Gav08b, GIW13] are presented in Part V of this dissertation.

2.4 Using quantum communication protocols in other computational scenarios

Quantum communication protocols are a special case of quantum algorithms, and we know how to prove that some quantum protocols outperform exponentially the best classical ones. This makes such protocols potentially useful in various quantum computational scenarios, where qualitative advantage over the classical counterparts is desired.

- In [CGJ09] we gave a protocol for a setting, closely reminding the *SMP* model: Alice and Bob were responding to random input values and it was possible to confirm that their responses were not maliciously collaborative in certain well-defined sense – even if the players were sharing entanglement (which they did not need for an honest action but could use in a conspiracy). That allowed us to make some interesting conclusions regarding the expressive power of a proof system where two possibly-dishonest provers could use shared entanglement in order to improve their cheating abilities.

- *Computational learning theory* is a mathematical study of protocols where a *student algorithm* interacts with a *teacher oracle* in order to deduce some knowledge. In [Gav12b] we defined a new model of quantum learning, where in order to be considered successful, the student had to be able to answer a polynomial number of testing queries. We demonstrated a relational concept class that was efficiently learnable in that model, while in any reasonable classical model exponential amount of training data would be required: that gave the first proof of the qualitative superiority of quantum over classical learning. The construction in [Gav12b] was based on the analysis of a special regime of one-way communication, which we called *single-input mode*, where Bob received no input: somewhat surprisingly, in the context of relational problems this regime became rather non-trivial and offered new insight into the framework of computational learning.
- The notion of *quantum money* seems to have been proposed with some engineering considerations in mind; nevertheless, it provides a rather natural challenge for theoretical investigation of quantum mechanics, as a classical construction is easily seen to be impossible: The goal is to design a (quantum) *asset protocol*, where genuineness would be guaranteed unconditionally by the *irreversibility* of certain evolutions in accordance with the assumed physical laws. In [Gav12a] we presented a quantum money scheme, where the asset-verification procedure only needed classical communication with a bank (all previously-known schemes had required a quantum communication channel for that). Both the construction and its analysis strongly relied on the earlier results from the area of quantum communication complexity: intuitively, the qualitative supremacy of certain one-way quantum protocol over any classical protocol was converted into the unconditional

security of the proposed quantum money scheme.

- In [GI13] we introduced a new type of primitive that we called *hiding fingerprints.* This was a mapping of binary strings of length n to $d << n$ qubits, such that
  - given any string y and a fingerprint of x, one could decide with high confidence whether $x = y$;
  - given a fingerprint of x, at most $o(1)$ bits of information about x could be extracted.

  These two requirements may even seem contradictory, and it is easy to see that classical schemes like that are not possible. We presented several quantum hiding fingerprinting schemes, achieving different combinations of the equality-testing confidence and the string-concealing confidentiality, and we demonstrated optimality of our constructions. Hiding fingerprints are naturally viewed as one-way protocols for the equality function (Eq) that must obey the additional confidentiality requirements: both the constructions and their analysis in [GI13] stemmed from this connection to quantum communication complexity.

Works [CGJ09, Gav12b, Gav12a, GI13] are presented in Part VI of this dissertation.

Chapter 3

Conclusions and further research

The most recent work covered by this dissertation is [Gav20a] (Chapter II.6). It demonstrates that quantum *SMP*, which is the weakest reasonable quantum model, can qualitatively outperform classical two-way communication, which is the strongest model of feasible classical communication.

What interesting questions are still worth asking?

- The problem that is analysed in [Gav20a] is a *relation* – that is, allowing multiple correct answer to the same pair of input values. It remains open to understand what are the strongest separations achievable via the more restricted types of communication problems – namely, *(partial) functions* and *total functions* (see Chapter II.6 for details).
- A weaker form of the above question is the following: Is this true that a quantum simultaneous-messages protocol cannot exponentially outperform a classical two-way protocol when that communication problem is a total function?
- One of the known limitations of quantum communication is given in [GKRdW09] (Chapter III.1): there it is shown that quantum communication is, in general, not strong enough to replace shared randomness in efficient classical simultaneous-

messages protocols. The communication problem that is analysed in order to demonstrate this is also a relational one. If the communication problem is functional, is it still the case that shared randomness can give qualitative advantage to a classical *SMP*-protocol over a quantum one that does not have access to shared randomness?

These and some other remaining questions can be viewed as rather detail-oriented: in particular, they are focused on the restricted types of communication problems, namely partial and total functions. It seems that the majority of the fundamental problems related to bipartite quantum communication complexity have now been resolved by the joint efforts of the scientific community. While author's humble contribution to that lucky venture is presented by the dissertation, it is also his hope that some of the remaining important questions will be highlighted and new insight will come up as a result of this writing.

Publications covered by the dissertation

[CGJ09] R. Cleve, D. Gavinsky, and R. Jain. Entanglement-Resistant Two-Prover Interactive Proof Systems and Non-Adaptive Private Information Retrieval Systems. *Quantum Information and Computation 9(7)*, pages 648–656, 2009.

[Gav08a] D. Gavinsky. Classical Interaction Cannot Replace a Quantum Message. *Proceedings of the 40th Symposium on Theory of Computing*, pages 95–102, 2008.

[Gav08b] D. Gavinsky. On the Role of Shared Entanglement. *Quantum Information and Computation 8(1-2)*, pages 82–95, 2008.

[Gav12a] D. Gavinsky. Quantum Money with Classical Verification. *Proceedings of the 27th IEEE Conference on Computational Complexity*, pages 42–52, 2012.

[Gav12b] D. Gavinsky. Quantum Predictive Learning and Communication Complexity with Single Input. *Quantum Information and Computation 12(7-8)*, pages 575–588, 2012.

[Gav19] D. Gavinsky. Quantum Versus Classical Simultaneity in Communication Complexity. *IEEE Transac-*

tions on Information Theory 65(10), pages 6466–6483, 2019.

[Gav20a] D. Gavinsky. Bare Quantum Simultaneity Versus Classical Interactivity in Communication Complexity. *Proceedings of the 52nd Symposium on Theory of Computing*, pages 401–411, 2020.

[Gav20b] D. Gavinsky. Entangled Simultaneity Versus Classical Interactivity in Communication Complexity. *IEEE Transactions on Information Theory 66(7)*, pages 4641–4651, 2020.

[GBK15a] D. Gavinsky, R. Bottesch, and H. Klauck. Correlation in Hard Distributions in Communication Complexity. *Proceedings of the 19th International Workshop on Randomization and Computation*, pages 544–572, 2015.

[GBK15b] D. Gavinsky, R. Bottesch, and H. Klauck. Equality, Revisited. *Proceedings of the 40th International Symposium on Mathematical Foundations of Computer Science*, pages 127–138, 2015.

[GI13] D. Gavinsky and T. Ito. Quantum Fingerprints that Keep Secrets. *Quantum Information and Computation 13(7-8)*, pages 583–606, 2013.

[GIW13] D. Gavinsky, T. Ito, and G. Wang. Shared Randomness and Quantum Communication in the Multi-Party Model. *Proceedings of the 28th IEEE Conference on Computational Complexity*, pages 34–43, 2013.

[GKdW06] D. Gavinsky, J. Kempe, and R. de Wolf. Strengths and Weaknesses of Quantum Fingerprinting. *Proceedings of the 21st IEEE Conference on Computational Complexity*, pages 288–298, 2006.

[GKK+08] D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, and R. de Wolf. Exponential Separations for One-Way Quantum Communication Complexity, with Applications to Cryptography. *SIAM Journal on Computing 38(5)*, pages 1695–1708, 2008.

[GKRdW09] D. Gavinsky, J. Kempe, O. Regev, and R. de Wolf. Bounded-Error Quantum State Identification and Exponential Separations in Communication Complexity. *SIAM Journal of Computing 39(1)*, pages 1–24, 2009.

[GP08] D. Gavinsky and P. Pudlák. Exponential Separation of Quantum and Classical Non-Interactive Multi-Party Communication Complexity. *Proceedings of the 23rd IEEE Conference on Computational Complexity*, pages 332–339, 2008.

[GRdW08] D. Gavinsky, O. Regev, and R. de Wolf. Simultaneous Communication Protocols with Quantum and Classical Messages. *Chicago Journal of Theoretical Computer Science*, article 7, 2008.

Bibliography *

[AA05] S. Aaronson and A. Ambainis. Quantum Search of Spatial Regions. *Theory of Computing 1(1)*, pages 47–79, 2005.

[Aar04] S. Aaronson. Limitations of Quantum Advice and One-Way Communication. *Proceedings of the 19th IEEE Conference on Computational Complexity*, pages 320–332, 2004.

[Aar06] S. Aaronson. QMA/qpoly $\subseteq$ PSPACE/poly: De-Merlinizing Quantum Protocols. *Proceedings of the 21st IEEE Conference on Computational Complexity*, 2006.

[Aar07] S. Aaronson. The Learnability of Quantum States. *Proceedings of the Royal Society of London 2088*, A463, 2007.

[Aar09] S. Aaronson. Quantum Copy-Protection and Quantum Money. *Proceedings of the 24th IEEE Conference on Computational Complexity*, pages 229–242, 2009.

[AC12] S. Aaronson and P. Christiano. Quantum Money from Hidden Subspaces. *Proceedings of the 44th Symposium on Theory of Computing*, To appear, 2012.

* This is a combined bibliography of the dissertation, excluding the author's works that it covers and personal communication references.

[ADR02] Y. Aumann, Y. Z. Ding, and M. O. Rabin. Everlasting Security in the Bounded Storage Model. *IEEE Transactions on Information Theory 48*, pages 1668–1680, 2002.

[Amb96] A. Ambainis. Communication Complexity in a 3-Computer Model. *Algorithmica 16(3)*, pages 298–301, 1996.

[AMS99] N. Alon, Y. Matias, and M. Szegedy. The Space Complexity of Approximating the Frequency Moments. *Journal of Computer and Systems Sciences 58(1)*, pages 137–147, 1999.

[AMY14] N. Alon, S. Moran, and A. Yehudayoff. Sign Rank, VC-Dimension and Spectral Gaps. http://www.eccc.uni-trier.de/report/2014/135, 2014.

[ANTSV02] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani. Dense Quantum Coding and Quantum Finite Automata. *Journal of the ACM 49(4)*, pages 496–511, 2002.

[AV79] D. Angluin and L. Valiant. Fast Probabilistic Algorithms for Hamiltonian Paths and Matchings. *Journal of Computer and System Sciences 18*, pages 155–193, 1979.

[AW08] S. Aaronson and A. Wigderson. Algebrization: A New Barrier in Complexity Theory. *Proceedings of the 40th Symposium on Theory of Computing*, pages 731–740, 2008.

[BB84] C. H. Bennett and G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, 1984.

[BBBW83] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner. Quantum Cryptography, or Unforgeable Subway Tokens. *Advances in Cryptology – Proceedings of Crypto 82*, pages 267–275, 1983.

[BBR88] C. H. Bennett, G. Brassard, and J-M. Robert. Privacy Amplification by Public Discussion. *SIAM Journal on Computing 17(2)*, pages 210–229, 1988.

[BCMdW10] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf. Nonlocality and Communication Complexity. *Reviews of Modern Physics 82(1)*, pages 665–698, 2010.

[BCW98] H. Buhrman, R. Cleve, and A. Wigderson. Quantum vs. Classical Communication and Computation. *Proceedings of the 30th Symposium on Theory of Computing*, pages 63–68, 1998.

[BCWdW01] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf. Quantum Fingerprinting. *Physical Review Letters 87(16)*, article 167902, 2001.

[Bec75] W. Beckner. Inequalities in Fourier Analysis. *Annals of Mathematics 102*, pages 159–182, 1975.

[BFL90] L. Babai, L. Fortnow, and C. Lund. Non-Deterministic Exponential Time Has Two-Prover Interactive Protocols. *Proceedings of the 31st Annual Symposium on Foundations of Computer Science*, pages 16–25, 1990.

[BFS86] L. Babai, P. Frankl, and J. Simon. Complexity Classes in Communication Complexity Theory. *Proceedings of the 27th Annual Symposium on Foundations of Computer Science*, pages 337–347, 1986.

[Bha97] R. Bhatia. Matrix Analysis. *Springer, Graduate Texts in Mathematics, 169*, 1997.

[BHL+05] C. H. Bennett, P. Hayden, D. Leung, P. W. Shor, and A. Winter. Remote Preparation of Quantum States. *IEEE Transactions on Information Theory 51(1)*, pages 56–74, 2005.

[BJ95] N. Bshouty and J. Jackson. Learning DNF over the Uniform Distribution using a Quantum Example Oracle. *Proceedings of the 8th Annual Conference on Computational Learning Theory*, pages 118–127, 1995.

[BK97] L. Babai and P. G. Kimmel. Randomized simultaneous messages: Solution of a problem of Yao in communication complexity. *Proceedings of the 12th IEEE Conference on Computational Complexity*, pages 239–246, 1997.

[Bon70] A. Bonami. Etude des coefficients de Fourier des fonctions de $Lp(G)$. *Annales de l'Institute Fourier 20(2)*, pages 335–402, 1970.

[BS74] J. Bondy and M. Simonovits. Cycles of Even Length in Graphs. *Journal of Combinatorial Theory, Series B, 16*, pages 87–105, 1974.

[BTN01] A. Ben-Tal and A. Nemirovski. Lectures on Modern Convex Optimization. *SIAM*, 2001.

[Buh00] H. Buhrman. Quantum computing and communication complexity. *EATCS Bulletin 70*, pages 131–141, 2000.

[BV04] S. Boyd and L. Vandenberghe. Convex Optimization. *Cambridge University Press*, 2004.

[BYJK04] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis. Exponential Separation of Quantum and Classical One-Way Communication Complexity. *Proceedings of 36th*

Symposium on Theory of Computing, pages 128–137, 2004.

[BYJKS02a] Z. Bar-Yossef, T. S. Jayram, R. Kumar, and D. Sivakumar. An information statistics approach to data stream and communication complexity. *Proceedings of the 43th Annual Symposium on Foundations of Computer Science*, pages 209–218, 2002.

[BYJKS02b] Z. Bar-Yossef, T. S. Jayram, R. Kumar, and D. Sivakumar. Information Theory Methods in Communication Complexity. *Proceedings of 17th IEEE Conference on Computational Complexity*, pages 93–102, 2002.

[CB97] R. Cleve and H. Buhrman. Substituting Quantum Entanglement for Communication. *Physical Review Letters A 56(2)*, pages 1201–1204, 1997.

[CFL83] A. Chandra, M. Furst, and R. Lipton. Multi-party protocols. *Proceedings of the 15th Symposium on Theory of Computing*, pages 94–99, 1983.

[CG88] B. Chor and O. Goldreich. Unbiased Bits from Sources of Weak Randomness and Probabilistic Communication Complexity. *SIAM Journal on Computing 17(2)*, pages 230–261, 1988.

[CGKS95] B. Chor, O. Goldreich, E. Kushilevitz, and M. Sudan. Private Information Retrieval. *Journal of the ACM*, pages 41–50, 1995.

[CHTW04] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and Limits of Nonlocal Strategies. *Proceedings of the 19th IEEE Conference on Computational Complexity*, pages 236–249, 2004.

[CR11] A. Chakrabarti and O. Regev. An Optimal Lower Bound on the Communication Complexity of Gap-

Hamming-Distance. *Proceedings of the 43rd Symposium on Theory of Computing*, pages 51–60, 2011.

[CSUU07] R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay. Perfect Parallel Repetition Theorem for Quantum XOR Proof Systems. *Proceedings of the 22nd IEEE Conference on Computational Complexity*, pages 109–114, 2007.

[CT91] T. M. Cover and J. A. Thomas. Elements of Information Theory. *Wiley*, 1991.

[DDN00] D. Dolev, C. Dwork, and M. Naor. Non-Malleable Cryptography. *SIAM Journal on Computing 30(2)*, pages 391–437, 2000.

[DG99] S. Dasgupta and A. Gupta. An Elementary Proof of the Johnson-Lindenstrauss Lemma. *Technical Report TR-99-006, Berkeley, CA*, 1999.

[DG03] S. Dasgupta and A. Gupta. An Elementary Proof of a Theorem of Johnson and Lindenstrauss. *Random Structures and Algorithms 22(1)*, pages 60–65, 2003.

[DM04] S. Dziembowski and U. Maurer. Optimal Randomizer Efficiency in the Bounded Storage Model. *Journal of Cryptology 17(1)*, pages 5–26, 2004.

[dW02] R. de Wolf. Quantum Communication and Complexity. *Theoretical Computer Science 287(1)*, pages 337–353, 2002.

[Eld03] Y. C. Eldar. A Semidefinite Programming Approach to Optimal Unambiguous Discrimination of Quantum States. *IEEE Transactions on Information Theory 49*, pages 446–456, 2003.

[Fei91] U. Feige. On the Success Probability of Two Provers in One-Round Proof Systems. *Proceedings of the*

6th Annual Conference on Structure in Complexity Theory, pages 116–123, 1991.

[FGH+10] E. Farhi, D. Gosset, A. Hassidim, A. Lutomirski, and P. Shor. Quantum Money from Knots. http://arxiv.org/abs/1004.5127, 2010.

[FHS11] O. Fawzi, P. Hayden, and P. Sen. From Low-Distortion Norm Embeddings to Explicit Uncertainty Relations and Efficient Information Locking. *Proceedings of the 43st Symposium on Theory of Computing*, to appear, 2011.

[FIM+01] J. Feigenbaum, Y. Ishai, T. Malkin, K. Nissim, M. Strauss, and R. Wright. Secure multiparty computation of approximations. *Springer, Lecture Notes in Computer Science 2076*, pages 927–938, 2001.

[FKL+01] J. Forster, M. Krause, S. Lokam, R. Mubarakzjanov, N. Schmitt, and H-U. Simon. Relations between communication complexity, linear arrangements, and computational complexity. *Proceedings of the 21th FSTTCS*, pages 171–182, 2001.

[FL92] U. Feige and L. Lovász. Two-Prover One-Round Proof Systems: Their Power and Their Problems. *Proceedings of the 24th Symposium on Theory of Computing*, pages 733–744, 1992.

[For01] J. Forster. A linear lower bound on the unbounded error probabilistic communication complexity. *Proceedings of the 16th IEEE Conference on Computational Complexity*, pages 100–106, 2001.

[Fre92] Y. Freund. An improved boosting algorithm and its implications on learning complexity. *Proceedings of the 5th Annual Conference on Computational Learning Theory*, pages 391–398, 1992.

[FRS94] L. Fortnow, J. Rompel, and M. Sipser. On the Power of Multi-Prover Interactive Protocols. *Theoretical Computer Science 134*, pages 545–557, 1994.

[FSSS03] J. Forster, N. Schmitt, H-U. Simon, and T. Suttorp. Estimating the optimal margins of embeddings in Euclidean half spaces. *Machine Learning, 51*, pages 263–281, 2003.

[FvdG99] C. A. Fuchs and J. van de Graaf. Cryptographic Distinguishability Measures for Quantum-Mechanical States. *IEEE Transactions on Information Theory 45(4)*, pages 1216–1227, 1999.

[Gas04] W. Gasarch. A Survey on Private Information Retrieval. *EATCS Bulletin 82*, pages 72–107, 2004.

[GS86] S. Goldwasser and M. Sipser. Private Coins versus Public Coins in Interactive Proof Systems. *Proceedings of the 18th Symposium on Theory of Computing*, pages 59–86, 1986.

[GS03] A. Golinsky and P. Sen. A Note on the Power of Quantum Fingerprinting. *quant-ph/0510091*, 2003.

[Hås01] J. Håstad. Some Optimal Inapproximability Results. *Journal of the ACM 48(4)*, pages 798–859, 2001.

[HJMR10] P. Harsha, R. Jain, D. McAllester, and J. Radhakrishnan. The Communication Complexity of Correlation. *IEEE Transactions on Information Theory 56(1)*, pages 438–449, 2010.

[HLSW04] P. Hayden, D. Leung, P. W. Shor, and A. Winter. Randomizing Quantum States: Constructions and Applications. *Communications in Mathematical Physics 250(2)*, pages 371–391, 2004.

[Hol73] A. S. Holevo. Bounds for the Quantity of Information Transmitted by a Quantum Communication Channel. *Problemy Peredachi Informatsii 9(3)*, pages 3–11, 1973.

[HOT81] F. Hiai, M. Ohya, and M. Tsukada. Sufficiency, KMS Condition and Relative Entropy in von Neumann Algebras. *Pacific Journal of Mathematics 96*, pages 99–109, 1981.

[HW07] J. Håstad and A. Wigderson. The Randomized Communication Complexity of Set Disjointness. *Theory of Computing 3(1)*, pages 211–219, 2007.

[IK10] R. Impagliazzo and V. Kabanets. Constructive Proofs of Concentration Bounds. *Proceedings of APPROX-RANDOM*, pages 617–631, 2010.

[IKP+08] T. Ito, H. Kobayashi, D. Preda, X. Sun, and A. C-C. Yao. Generalized Tsirelson Inequalities, Commuting-Operator Provers, and Multi-Prover Interactive Proof Systems. *Proceedings of the 23rd IEEE Conference on Computational Complexity*, 2008.

[ILL89] R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-Random Generation from One-Way Functions. *Proceedings of the 21st Symposium on Theory of Computing*, pages 12–24, 1989.

[IW03] P. Indyk and D. Woodruff. Tight Lower Bounds for the Distinct Elements Problem. *Proceedings of the 44th Annual Symposium on Foundations of Computer Science*, pages 283–289, 2003.

[JKN08] R. Jain, H. Klauck, and A. Nayak. Direct Product Theorems for Classical Communication Complexity via Subdistribution Bounds. *Proceedings of the 40th Symposium on Theory of Computing*, 2008.

[JL84] W. Johnson and J. Lindenstrauss. Extensions of Lipschitz maps into a Hilbert space. *Contemporary Mathematics, 26*, pages 189–206, 1984.

[JRS02] R. Jain, J. Radhakrishnan, and P. Sen. Privacy and Interaction in Quantum Communication Complexity and a Theorem about the Relative Entropy of Quantum States. *Proceedings of the 43rd Annual Symposium on Foundations of Computer Science*, pages 429–438, 2002.

[JRS03] R. Jain, R. Radhakrishnan, and J. Sen. A Lower Bound for the Bounded Round Quantum Communication Complexity of Set Disjointness. *Proceedings of the 44th Annual Symposium on Foundations of Computer Science*, pages 220–229, 2003.

[JRS05] R. Jain, J. Radhakrishnan, and P. Sen. Prior Entanglement, Message Compression and Privacy in Quantum Communication. *Proceedings of the 20th IEEE Conference on Computational Complexity*, pages 285–296, 2005.

[JRW94] R. Jozsa, D. Robb, and W. K. Wootters. Lower Bound for Accessible Information in Quantum Mechanics. *Physical Review A 49(2)*, pages 668–677, 1994.

[Juk01] S. Jukna. Extremal Combinatorics With Applications in Computer Science. *Springer-Verlag*, 1st edition, 2001.

[JUW09] R. Jain, S. Upadhyay, and J. Watrous. Two-Message Quantum Interactive Proofs Are in PSPACE. *Manuscript*, 2009.

[JZ09] R. Jain and S. Zhang. New Bounds on Classical and Quantum One-Way Communication Complexity. *Theoretical Computer Science 410(26)*, pages 2463–2477, 2009.

[KdW04] I. Kerenidis and R. de Wolf. Exponential Lower Bound for 2-Query Locally Decodable Codes via a Quantum Argument. *Journal of Computer and System Sciences 69(3)*, pages 395–420, 2004.

[Ker07] I. Kerenidis. Quantum Multiparty communication complexity and circuit lower bounds. *4th Annual Conference on Theory and Applications of Models of Computation*, 2007.

[KKL88] J. Kahn, G. Kalai, and N. Linial. The Influence of Variables on Boolean Functions. *Proceedings of the 29th Annual Symposium on Foundations of Computer Science*, pages 68–80, 1988.

[KKM+08] J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick. Entangled Games Are Hard to Approximate. *Proceedings of the 49th Annual Symposium on Foundations of Computer Science*, 2008.

[Kla00a] H. Klauck. On Quantum and Probabilistic Communication: Las Vegas and One-Way Protocols. *Proceedings of the 32nd Symposium on Theory of Computing*, pages 644–651, 2000.

[Kla00b] H. Klauck. Quantum communication complexity. *Proceedings of the Workshop on Boolean Functions and Applications*, pages 241–252, 2000.

[Kla01] H. Klauck. One-Way Communication Complexity and the Neciporuk Lower Bound on Formula Size. http://arxiv.org/abs/cs.cc/0111062, 2001.

[KM03] H. Kobayashi and K. Matsumoto. Quantum Multi-Prover Interactive Proof Systems with Limited Prior Entanglement. *Journal of Computer and System Sciences 66(3)*, pages 429–450, 2003.

[KMR05] R. König, U. Maurer, and R. Renner. On the Power of Quantum Memory. *IEEE Transactions on Information Theory 51(7)*, pages 2391–2401, 2005.

[KMY03] H. Kobayashi, K. Matsumoto, and T. Yamakami. Quantum Merlin-Arthur Proof Systems: Are Multiple Merlins More Helpful to Arthur? *Proceedings of the 14th International Symposium on Algorithms and Computation*, pages 189–198, 2003.

[KN97] E. Kushilevitz and N. Nisan. Communication Complexity. *Cambridge University Press*, 1997.

[KNR99] I. Kremer, N. Nisan, and D. Ron. On Randomized One-Round Communication Complexity. *Computational Complexity 8(1)*, pages 21–49, 1999.

[KNTSZ01] H. Klauck, A. Nayak, A. Ta-Shma, and D. Zuckerman. Interaction in Quantum Communication and the Complexity of Set Disjointness. *Proceedings of the 42nd Annual Symposium on Foundations of Computer Science*, pages 124–133, 2001.

[KP14] H. Klauck and S. Podder. Two Results about Quantum Messages. *Proceedings of the 39th International Symposium on Mathematical Foundations of Computer Science*, 2014.

[KR04] C. King and M-B. Ruskai. Comments on multiplicativity of maximal p-norms when $p = 2$. *Quantum Information, Statistics, Probability. Edited by O. Hirota*, 2004.

[KR11] B. Klartag and O. Regev. Quantum One-Way Communication Can Be Exponentially Stronger than Classical Communication. *Proceedings of the 43st Symposium on Theory of Computing*, pages 31–40, 2011.

[Kre95] I. Kremer. Quantum Communication. *Master's thesis*, 1995.

[KRT08] J. Kempe, O. Regev, and B. Toner. The Unique Games Conjecture with Entangled Provers is False. *Proceedings of the 49th Annual Symposium on Foundations of Computer Science*, 2008.

[KS92] B. Kalyanasundaram and G. Schnitger. The Probabilistic Communication Complexity of Set Intersection. *SIAM Journal on Discrete Mathematics 5(4)*, pages 545–557, 1992.

[KSdW04] H. Klauck, R. Spalek, and R. de Wolf. Quantum and Classical Strong Direct Product Theorems and Optimal Time-Space Tradeoffs. *Proceedings of the 45th Annual Symposium on Foundations of Computer Science*, pages 12–21, 2004.

[KT06] R. König and B. M. Terhal. The Bounded Storage Model in the Presence of a Quantum Adversary. http://arxiv.org/abs/quant-ph/0608101, 2006.

[KV94] M. Kearns and U. V. Vazirani. An Introduction to Computational Learning Theory. *MIT Press*, 1994.

[KW00] A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. *Proceedings of the 32nd Symposium on Theory of Computing*, pages 608–617, 2000.

[LAF+10] A. Lutomirski, S. Aaronson, E. Farhi, D. Gosset, J. A. Kelner, A. Hassidim, and P. W. Shor. Breaking and Making Quantum Money: Toward a New Quantum Cryptographic Protocol. *Proceedings of the 1st Symposium on Innovations in Computer Science*, pages 20–31, 2010.

[Leu09] D. Leung. A Survey on Locking of Bipartite Correlations. *Journal of Physics: Conference Series 143*, article 012008, 2009.

[lG06] F. le Gall. Exponential Separation of Quantum and Classical Online Space Complexity. *Proceedings of the 18th Symposium on Parallelism in Algorithms and Architectures*, pages 67–73, 2006.

[LMSS07] N. Linial, S. Mendelson, G. Schechtman, and A. Schraibman. Complexity Measures of Sign Matrices. *Combinatorica 27(4)*, pages 439–463, 2007.

[Lov00] L. Lovász. Semidefinite programs and combinatorial optimization. http://research.microsoft.com/users/lovasz/notes.htm, 2000.

[LPS88] A. Lubotzki, R. Phillips, and P. Sarnak. Ramanujan Graphs. *Combinatorica 8*, pages 261–277, 1988.

[LPSW07] N. Linden, S. Popescu, A. J. Short, and A. Winter. Quantum Nonlocality and Beyond: Limits From Nonlocal Computation. *Physical Review Letters 99*, 180502, 2007.

[LS09] N. Linial and A. Schraibman. Learning Complexity vs. Communication Complexity. *Combinatorics, Probability & Computing 18(1-2)*, pages 227–245, 2009.

[Lu04] C-J. Lu. Encryption Against Storage-Bounded Adversaries from On-Line Strong Extractors. *Journal of Cryptology 17(1)*, pages 27–42, 2004.

[Lut10] A. Lutomirski. An Online Attack Against Wiesner's Quantum Money. http://arxiv.org/abs/1010.0256, 2010.

[LUW95] F. Lazebnik, V. Ustimenko, and A. Woldar. A New Series of Dense Graphs of High Girth. *Bulletin of AMS 32*, pages 73–79, 1995.

[Mau92] U. Maurer. Conditionally-perfect secrecy and a provably-secure randomized cipher. *Journal of Cryptology 5(1)*, pages 53–66, 1992.

[May97] D. Mayers. Unconditionally Secure Quantum Bit Commitment is Impossible. *Physical Review Letters 78(17)*, pages 3414–3417, 1997.

[McD98] C. McDiarmid. Concentration. *Probabilistic Methods for Algorithmic Discrete Mathematics*, pages 195–248, 1998.

[MS10] M. Mosca and D. Stebila. Quantum Coins. *Error-Correcting Codes, Finite Geometries and Cryptography – American Mathematical Society*, pages 35–46, 2010.

[Mut05] M. Muthukrishnan. Data Streams: Algorithms and Applications. *Now Publishers*, 2005.

[MVW12] A. Molina, T. Vidick, and J. Watrous. Optimal Counterfeiting Attacks and Generalizations for Wiesner's Quantum Money. http://arxiv.org/abs/1202.4010, 2012.

[MWY15] M. Molinaro, D. Woodruff, and G. Yaroslavtsev. Amplification of One-Way Information Complexity via Codes and Noise Sensitivity. *Proceedings of the 42nd International Colloquium on Automata, Languages and Programming*, pages 960–972, 2015.

[Nay99] A. Nayak. Optimal Lower Bounds for Quantum Automata and Random Access Codes. *Proceedings of the 40th Annual Symposium on Foundations of Computer Science*, pages 369–377, 1999.

[NC00] M. Nielsen and I. Chuang. Quantum Computation and Quantum Information. *Cambridge University Press*, 2000.

[New91] I. Newman. Private vs. Common Random Bits in Communication Complexity. *Information Processing Letters 39(2)*, pages 67–71, 1991.

[NN93] J. Naor and M. Naor. Small-Bias Probability Spaces: Efficient Constructions and Applications. *SIAM Journal on Computing 22(4)*, pages 838–856, 1993.

[NS96] I. Newman and M. Szegedy. Public vs. Private Coin Flips in One Round Communication Games. *Proceedings of the 28th Symposium on Theory of Computing*, pages 561–570, 1996.

[Pop34] K. Popper. Logik der Forschung: Zur Erkenntnistheorie der modernen Naturwissenschaft. *Tübingen: Siebeck*, 1934.

[PS97] A. Panconesi and A. Srinivasan. Randomized Distributed Edge Coloring via an Extension of the Chernoff-Hoeffding Bounds. *SIAM Journal on Computing 26(2)*, pages 350–368, 1997.

[PYJ+11] F. Pastawski, N. Y. Yao, L. Jiang, M. D. Lukin, and J. I. Cirac. Unforgeable Noise-Tolerant Quantum Tokens. http://arxiv.org/abs/1112.5456, 2011.

[Raz92] A. Razborov. On the Distributional Complexity of Disjointness. *Theoretical Computer Science 106(2)*, pages 385–390, 1992.

[Raz95] R. Raz. A parallel repetition theorem. *Proceedings of the 27th Symposium on Theory of Computing*, pages 447–456, 1995.

[Raz99] R. Raz. Exponential Separation of Quantum and Classical Communication Complexity. *Proceedings of the 31st Symposium on Theory of Computing*, pages 358–367, 1999.

[Raz03] A. Razborov. Quantum Communication Complexity of Symmetric Predicates. *Izvestiya of the Russian Academy of Science, mathematics, 67(1)*, pages 159–176, 2003.

[Ren05] R. Renner. Security of Quantum Key Distribution. http://arxiv.org/abs/quant-ph/0512258, 2005.

[RK05] R. Renner and R. König. Universally Composable Privacy Amplification Against Quantum Adversaries. *Proceedings of the 2nd Theory of Cryptography Conference*, pages 407–425, 2005.

[RRS09] J. Radhakrishnan, M. Rötteler, and P. Sen. Random Measurement Bases, Quantum State Distinction and Applications to the Hidden Subgroup Problem. *Algorithmica 55(3)*, pages 490–516, 2009.

[Sam15] A. Samorodnitsky. On the Entropy of a Noisy Function. http://arxiv.org/abs/1508.01464, 2015.

[Sch02] R. E. Schapire. The boosting approach to machine learning: An overview. *MSRI Workshop on Nonlinear Estimation and Classification*, 2002.

[SG04] R. A. Servedio and S. Gortler. Equivalences and Separations Between Quantum and Classical Learnability. *SIAM Journal on Computing 33(5)*, pages 1067–1092, 2004.

[She08] A. Sherstov. Communication Complexity under Product and Nonproduct Distributions. *Proceedings of the 23rd IEEE Conference on Computational Complexity*, pages 64–70, 2008.

[Shi05] Y. Shi. Tensor Norms and the Classical Communication Complexity of Bipartite Quantum Measurements. *Proceedings of the 37th Symposium on Theory of Computing*, 2005.

[Sho97] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing 26(5)*, pages 1484–1509, 1997.

[Sin18] A. Sinclair. Randomness and Computation. *UC Berkeley*, lecture notes, 2018.

[ST13] M. Saglam and G. Tardos. On the Communication Complexity of Sparse Set Disjointness and Exists-Equal Problems. *Proceedings of the 54th Annual Symposium on Foundations of Computer Science*, pages 678–687, 2013.

[Sýk74] S. Sýkora. Quantum Theory and the Bayesian Inference Problems. *Journal of Statistical Physics 11(1)*, pages 17–27, 1974.

[TOI03] Y. Tokunaga, T. Okamoto, and N. Imoto. Anonymous Quantum Cash. *ERATO Conference on Quantum Information Science*, 2003.

[Vad04] S. Vadhan. Constructing Locally Computable Extractors and Cryptosystems in the Bounded-Storage Model. *Journal of Cryptology 17(1)*, pages 43–77, 2004.

[Val84] L. Valiant. A Theory of the Learnable. *Communications of the ACM 27(11)*, pages 1134–1142, 1984.

[VB96] L. Vandenberghe and S. Boyd. Semidefinite programming. *SIAM Review, 38*, pages 49–95, 1996.

[Ver12] R. Vershynin. Introduction to the Non-Asymptotic Analysis of Random Matrices. *Chapter 5 of: Compressed Sensing, Theory and Applications. Edited by Y. Eldar and G. Kutyniok*, pages 210–268, 2012.

[Wat03] J. Watrous. PSPACE Has Constant-Round Quantum Interactive Proof Systems. *Theoretical Computer Science 292(3)*, pages 575–588, 2003.

[Wat08] J. Watrous. Quantum Computational Complexity. http://arxiv.org/abs/0804.3401, 2008.

[Wie83] S. Wiesner. Conjugate Coding. *SIGACT News 15(1)*, pages 78–88, 1983.

[WZ82] W. K. Wootters and W. H. Zurek. A Single Quantum Cannot be Cloned. *Nature 299*, pages 802–803, 1982.

[Yao77] A. C-C. Yao. Probabilistic Computations: Toward a Unified Measure of Complexity. *Proceedings of the 18th Annual Symposium on Foundations of Computer Science*, pages 222–227, 1977.

[Yao79] A. C-C. Yao. Some Complexity Questions Related to Distributive Computing. *Proceedings of the 11th Symposium on Theory of Computing*, pages 209–213, 1979.

[Yao93] A. C-C. Yao. Quantum Circuit Complexity. *Proceedings of the 34th Annual Symposium on Foundations of Computer Science*, pages 352–360, 1993.

[Yao03] A. C-C. Yao. On the Power of Quantum Fingerprinting. *Proceedings of the 35th Symposium on Theory of Computing*, pages 77–81, 2003.