Quantum Proofs

Thomas Vidick
California Institute of Technology
vidick@cms.caltech.edu

John Watrous
University of Waterloo
john.watrous@uwaterloo.ca

now
the essence of knowledge
Boston — Delft

Foundations and Trends® in Theoretical Computer Science

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

T. Vidick and J. Watrous. *Quantum Proofs*. Foundations and Trends® in Theoretical Computer Science, vol. 11, no. 1-2, pp. 1–215, 2015.

This Foundations and Trends® issue was typeset in LaTeX using a class file designed by Neal Parikh. Printed on acid-free paper.

ISBN: 978-1-68083-127-6

Foundations and Trends® in Theoretical Computer Science
Volume 11, Issue 1-2, 2015

Editorial Scope

Topics

Foundations and Trends® in Theoretical Computer Science publishes surveys and tutorials on the foundations of computer science. The scope of the series is broad. Articles in this series focus on mathematical approaches to topics revolving around the theme of efficiency in computing. The list of topics below is meant to illustrate some of the coverage, and is not intended to be an exhaustive list.

- Algorithmic game theory
- Computational algebra
- Computational aspects of combinatorics and graph theory
- Computational aspects of communication
- Computational biology
- Computational complexity
- Computational geometry
- Computational learning
- Computational Models and Complexity
- Computational Number Theory
- Cryptography and information security
- Data structures
- Database theory
- Design and analysis of algorithms
- Distributed computing
- Information retrieval
- Operations research
- Parallel algorithms
- Quantum computation
- Randomness in computation

Information for Librarians

Foundations and Trends® in Theoretical Computer Science, 2015, Volume 11, 4 issues. ISSN paper version 1551-305X. ISSN online version 1551-3068. Also available as a combined paper and online subscription.

Foundations and Trends® in
Theoretical Computer Science
Vol. 11, No. 1-2 (2015) 1–215

DOI: 10.1561/0400000068

the essence of knowledge

Quantum Proofs

Thomas Vidick
California Institute of Technology
vidick@cms.caltech.edu

John Watrous
University of Waterloo
john.watrous@uwaterloo.ca

Foundations and Trends® in
Theoretical Computer Science
Vol. 11, No. 1-2 (2015) 1–215

DOI: 10.1561/0400000068

the essence of knowledge

Quantum Proofs

Thomas Vidick
California Institute of Technology
vidick@cms.caltech.edu

John Watrous
University of Waterloo
john.watrous@uwaterloo.ca

Contents

Abstract

Quantum information and computation provide a fascinating twist on the notion of proofs in computational complexity theory. For instance, one may consider a quantum computational analogue of the complexity class NP, known as QMA, in which a quantum state plays the role of a proof (also called a certificate or witness), and is checked by a polynomial-time quantum computation. For some problems, the fact that a quantum proof state could be a superposition over exponentially many classical states appears to offer computational advantages over classical proof strings. In the interactive proof system setting, one may consider a verifier and one or more provers that exchange and process quantum information rather than classical information during an interaction for a given input string, giving rise to quantum complexity classes such as QIP, QSZK, and QMIP* that represent natural quantum analogues of IP, SZK, and MIP. While quantum interactive proof systems inherit some properties from their classical counterparts, they also possess distinct and uniquely quantum features that lead to an interesting landscape of complexity classes based on variants of this model.

In this survey we provide an overview of many of the known results concerning quantum proofs, computational models based on this concept, and properties of the complexity classes they define. In particular, we discuss non-interactive proofs and the complexity class QMA, single-prover quantum interactive proof systems and the complexity class QIP, statistical zero-knowledge quantum interactive proof systems and the complexity class QSZK, and multiprover interactive proof systems and the complexity classes QMIP, QMIP*, and MIP*.

T. Vidick and J. Watrous. *Quantum Proofs*. Foundations and Trends® in Theoretical Computer Science, vol. 11, no. 1-2, pp. 1–215, 2015.
DOI: 10.1561/0400000068.

1

Introduction

The topic of this survey, *quantum interactive proof systems*, draws upon three different notions—quantum information, interaction, and proofs—whose combination forms a fascinating recipe best presented in the reverse order.

We begin with the notion of *proofs* in complexity theory. This notion has been central to complexity theory from its early beginnings, relating closely to the fundamental distinction between *efficient construction* and *efficient verification*. In greater detail, it has long been recognized that for some computational problems whose solutions may be difficult to obtain, it may nevertheless be possible to efficiently *verify* the correctness of a solution, given some additional information (representing a *proof*) that aids in this verification. The complexity class NP represents a formalization of this notion—it includes those decision problems for which positive instances can be efficiently verified given a suitable proof string (and for which negative instances are never incorrectly verified as positive ones).

The distinction between efficient construction and efficient verification appears, for instance, in work of Edmonds [55] from 1965 (although not in his more famous 1965 paper [56]), where he describes the *princi-*

ple of the absolute supervisor: a supervisor can ask his or her assistant to carry out a potentially lengthy search procedure for some computational problem (potentially "killing" the assistant with work!), and at the end of the day the assistant is expected to provide sufficient information so that his or her solution can be "verified with ease" by the supervisor.

The more modern terminology used to describe this situation is that of a *prover* and *verifier*: the prover represents the assistant, while the verifier represents the supervisor in Edmonds' story. With respect to this terminology, our sympathies are generally reversed: the verifier, faced with limitations on its computational abilities, simply wants to know whether or not a given input is a positive instance of a fixed decision problem, while the computationally unrestricted prover is untrustworthy and will try to convince the verifier that the input is a positive instance, irrespective of the truth.

The importance of what is now known as the P vs NP question, which essentially asks if there are indeed problems for which the efficient construction of a solution is impossible while an efficient verification is possible, was in fact implicitly noted some time prior to Edmonds' work—in a letter written to John von Neumann in the mid-1950s, Kurt Gödel observed the striking consequences that would result from an efficient solution to a certain problem in first-order logic that is now known to be NP-complete. The development of the theory of NP-completeness, by Cook [49], Levin [122], and Karp [105] in the early 1970s, placed the notion of proofs in computational complexity on a firm mathematical foundation.

Next, we add a second ingredient: *interaction*. The notion of an *interactive proof system* was introduced independently by Goldwasser, Micali, and Rackoff [71, 72] and Babai [19, 22] in the 1980s. Babai was following a similar line of thought that led to the introduction of P and NP: the identification of structural features that allow a fine classification of the difficulty of solving classes of computational problems (in this case, problems related to groups). Goldwasser, Micali, and Rackoff arrived at the notion from a different angle. They introduced a notion of "knowledge complexity" of an interactive proof (informally, the amount of information about a problem instance conveyed by the interaction beyond the problem's solution) and gave an example of a simple problem (testing quadratic residuosity) for which there existed a *zero-knowledge* interactive proof.

The simplest type of interactive proof system represents an interaction between a prover and verifier, which are similar characters to the ones introduced in the non-interactive setting above, except that now we imagine that they may engage in a discussion rather than the prover simply providing the verifier with information. In particular, the verifier may ask the prover questions and demand acceptable responses in order to be satisfied. As before, one views that the prover's aim is to convince the verifier that a given input string is a positive instance to a fixed decision problem (or, equivalently, that an input string possesses a fixed property of interest). The verifier's goal is to check the validity of the prover's argument, accepting only in the event that it is indeed convinced that the input string is a positive problem instance, and rejecting if not.

It turns out that the (classical) interactive proof system model only represents a departure from the non-interactive setting described above when the verifier makes use of *randomness*—in which case we must generally be satisfied with the verifier gathering overwhelming statistical evidence, but not having absolute certainty, in order to conclude that the prover's argument is valid. (When no randomness is used, the prover may as well attempt to convince the verifier to accept non-interactively by simply presenting a complete transcript of the conversation they would have had by interacting, which the verifier can efficiently check for validity by itself.) As in the non-interactive case, we also make the standard assumption that the prover's computational abilities are greater than the verifier's (or, at the very least, that the prover has access to information that the verifier lacks). The class IP is representative of the case in which the verifier is required to run in polynomial time and the prover is computationally unrestricted. The characterization IP=PSPACE [124, 150] cements the tight relationship between interactive proofs and computation, justifying its position as a fundamental concept in computational complexity theory.

Many variants of interactive proof systems have been considered that impose additional conditions on the interaction, place more stringent limits on the prover's abilities, or consider interactions between more diverse sets of parties, such as a verifier interacting with multiple cooperating or competing provers. Prominent examples include the class SZK of problems that have zero-knowledge interactive proofs and the class MIP of problems whose solution can be determined by a polynomial-time verifier interacting with multiple cooperating provers, restricted only in their inability to communicate with one other.

Finally, we finish off with a curious catalyst: *quantum information*. The Church–Turing thesis plays a foundational role in computer science by postulating that computability is model independent: whether based on the concept of a Turing machine, first-order logic, or any "purely mechanical process," the classes of functions whose values can be "effectively calculated" are identical. The development of quantum computing in the 1990s posed the first serious threat to this thesis. Impetus for the consideration of computational procedures based on the laws of quantum mechanics was provided by Shor's discovery of an efficient *quantum* algorithm for factoring [151, 152], a problem for which no efficient classical probabilistic algorithm is known. The study of the relation between P (or BPP) and BQP, the class of problems that can be decided in polynomial time by a quantum Turing machine, is among the most interesting and mysterious problems in modern complexity theory. The difficulty of this question prompts the introduction of "quantum analogues" of the most important classical complexity classes in an attempt to identify problems for which the consideration of quantum processes induces a strict separation.

One prominent example is the complexity class QMA of decision problems whose positive instances have *quantum proofs* that can be verified by an efficient quantum procedure. Aside from the fundamental problem of understanding the physical substrate of computation, the consideration of quantum mechanical states as proofs provides a fascinating window into some of the most subtle features of quantum physics. An essential way in which quantum states differ from their classical counterparts is in one's ability to recover information that is present in the mathematical description of the state. In quantum mechanics this ability is limited by the uncertainty principle—for example, both the momentum and position of an electron can be determined with high precision in principle, but there is a fundamental limit to the accuracy with which those two properties can be *simultaneously* determined. Thus, the study of QMA sheds light on the many areas of physics in which the properties of quantum states play an important role, from the theory of superconductors to that of black holes.

Stir vigorously, and you have a recipe for quantum interactive proofs. Beyond the class QMA already discussed, quantum interactive proofs reflect the richness of the classical model on which they are based, providing a powerful lens on the properties of quantum mechanics and quantum information. For example, single-prover quantum interactive proofs, corresponding to the class QIP, have the distinguishing property that they can be parallelized to three message interactions, and this property (unlikely to hold for classical interactive proofs) makes crucial use of the superposition principle of quantum mechanics. The no-cloning theorem plays an important role in the study of the class QSZK of problems having quantum zero-knowledge interactive proofs by hindering the construction of "simulators" essential to the study of classical zero-knowledge. By allowing multiple cooperating provers to share quantum entanglement, the class QMIP* provides a complexity-theoretic viewpoint on the nonlocal properties of entanglement.

Having set a rather ambitious stage for this survey, we proceed with a more concrete description of what is to come.

Chapter 2 introduces some preliminary material. While it is assumed that the reader will be familiar with the basics of complexity theory and quantum computing, we have made an effort to state and explain the facts that play an important role in the results to be discussed, directing the reader to standard textbooks for background material.

In Chapter 3 we begin with the consideration of the class QMA of languages that have efficiently verifiable quantum proofs. This class satisfies many of the desirable features of NP, such as strong error amplification procedures and a rich set of complete problems. It also has many variants restricting, or extending, the types of proofs allowed and the power of the verifier; a small but representative set of such variants is discussed in the chapter.

Chapter 4 considers single-prover quantum interactive proof systems. An important tool in the study of the associated class QIP is a semidefinite programming formulation of the verifier's maximum acceptance probability. We introduce this formulation and use it to establish a parallel repetition property of QIP as well as to give an essentially self-contained proof of the characterization QIP=PSPACE.

In Chapter 5 we consider the class QSZK of quantum zero-knowledge interactive proofs. One aspect in which these proof systems differ from their classical counterparts is the difficulty of extending the key techniques (such as rewinding) that are systematically used in the classical setting, and we describe known quantum analogues for such techniques.

The final chapter, Chapter 6, is devoted to quantum multi-prover interactive proofs. It will be seen that the consideration of entanglement between multiple provers leads to a failure of the most basic intuition on which the classical theory is built (most important of which are the technique of oracularization and the characterization MIP=NEXP). We describe ways to work around this failure by fighting fire with fire, devising techniques that make positive use of the provers' ability to share entanglement.

This survey is mainly intended for non-specialists having a basic background in complexity theory and quantum information. A typical reader may be a student or researcher in either area desiring to learn about the fundamentals of the (actively developing) theory of quantum interactive proofs. In most cases we have not included full proofs of the main results we present, but whenever possible we have either included detailed sketches of the key ideas behind the proofs, or have attempted to describe their most salient elements in simplified settings. Each chapter ends with notes that provide references for the results discussed in the chapter as well as a brief survey of related results and pointers to the literature.

References

[1] S. Aaronson, S. Beigi, A. Drucker, B. Fefferman, and P. Shor. The power of unentanglement. *Theory of Computing*, 5(1):1–42, 2009.

[2] S. Aaronson and A. Drucker. A full characterization of quantum advice. *SIAM Journal on Computing*, 43(3):1131–1183, 2014.

[3] S. Aaronson and G. Kuperberg. Quantum versus classical proofs and advice. *Theory of Computing*, 3(7):129–157, 2007.

[4] L. Adleman, J. DeMarrais, and M. Huang. Quantum computability. *SIAM Journal on Computing*, 26(5):1524–1540, 1997.

[5] D. Aharonov, I. Arad, Z. Landau, and U. Vazirani. The detectability lemma and quantum gap amplification. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, pages 417–426, 2009.

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

[7] D. Aharonov, M. Ben-Or, F. Brandão, and O. Sattath. The pursuit for uniqueness: extending Valiant–Vazirani theorem to the probabilistic and quantum settings. Available as arXiv e-Print 0810.4840, 2008.

[8] D. Aharonov, D. Gottesman, S. Irani, and J. Kempe. The power of quantum systems on a line. *Communications in Mathematical Physics*, 287(1):41–65, 2009.

[9] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 20–30, 1998.

[10] D. Aharonov and O. Regev. Lattice problems in NP ∩ coNP. *Journal of the ACM*, 52(5):749–765, 2005.

[11] W. Aiello and J. Håstad. Statistical zero-knowledge languages can be recognized in two rounds. *Journal of Computer and System Sciences*, 42(3):327–345, 1991.

[12] A. Ambainis. On physical problems that are slightly more difficult than QMA. In *Proceedings of the 29th Conference on Computational Complexity*, pages 32–43, 2014.

[13] A. Ambainis, A. Rosmanis, and D. Unruh. Quantum attacks on classical proof systems: The hardness of quantum rewinding. In *55th Annual IEEE Symposium on Foundations of Computer Science*, pages 474–483, 2014.

[14] P. Aravind. A simple demonstration of Bell's theorem involving two observers and no probabilities or inequalities. Available as arXiv.org e-Print quant-ph/0206070, 2002.

[15] S. Arora and B. Barak. *Complexity Theory: A Modern Approach*. Cambridge University Press, 2009.

[16] S. Arora and S. Kale. A combinatorial, primal-dual approach to semidefinite programs. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 227–236, 2007.

[17] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM*, 45(3):501–555, 1998.

[18] S. Arora and S. Safra. Probabilistic checking of proofs: a new characterization of NP. *Journal of the ACM*, 45(1):70–122, 1998.

[19] L. Babai. Trading group theory for randomness. In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, pages 421–429, 1985.

[20] L. Babai. Local expansion of vertex-transitive graphs and random generation in finite groups. In *Proceedings of the 23rd Annual ACM Symposium on Theory of Computing*, pages 164–174, 1991.

[21] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.

[22] L. Babai and S. Moran. Arthur–Merlin games: a randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36(2):254–276, 1988.

[23] L. Babai and E. Szemerédi. On the complexity of matrix group problems I. In *Proceedings of the 25th Annual IEEE Symposium on Foundations of Computer Science*, pages 229–240, 1984.

[24] M. Bavarian, T. Vidick, and H. Yuen. Anchoring games for parallel repetition. Available as arXiv.org e-Print 1509.07466, 2015.

[25] S. Beigi, P. Shor, and J. Watrous. Quantum interactive proofs with short messages. *Theory of Computing*, 7:101–117, 2011.

[26] J. Bell. On the Einstein–Podolsky–Rosen paradox. *Physics*, 1:195–200, 1964.

[27] A. Ben-Aroya, O. Schwartz, and A. Ta-Shma. Quantum expanders: Motivation and construction. *Theory of Computing*, 6(3):47–79, 2010.

[28] M. Ben-Or, E. Feig, D. Kozen, and P. Tiwari. A fast parallel algorithm for determining all roots of a polynomial with real roots. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing*, pages 340–349, 1986.

[29] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi-prover interactive proofs: how to remove intractability assumptions. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing*, pages 113–131, 1988.

[30] M. Ben-Or, A. Hassidim, and H. Pilpel. Quantum multi prover interactive proofs with communicating provers. In *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 467–476, 2008.

[31] D. Bini and V. Pan. Computing matrix eigenvalues and polynomial zeros where the output is real. *SIAM Journal on Computing*, 27(4):1099–1115, 1998.

[32] H. Blier and A. Tapp. All languages in NP have very short quantum proofs. In *Proceedings of the 2009 3rd International Conference on Quantum, Nano and Micro Technologies*, pages 34–37, 2009.

[33] M. Blum, M. Luby, and R. Rubinfeld. Self-testing/correcting with applications to numerical problems. *Journal of Computer and System Sciences*, 47(3):549–595, 1993.

[34] A. Bookatz. QMA-complete problems. *Quantum Information & Computation*, 14(5&6):361–383, 2014.

[35] A. Borodin. On relating time and space to size and depth. *SIAM Journal on Computing*, 6:733–744, 1977.

[36] A. Borodin, S. Cook, and N. Pippenger. Parallel computation for well-endowed rings and space-bounded probabilistic machines. *Information and Control*, 58:113–136, 1983.

[37] F. Brandão, M. Christandl, and J. Yard. A quasipolynomial-time algorithm for the quantum separability problem. In *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing*, pages 343–352, 2011.

[38] Mark Braverman and Ankit Garg. Small value parallel repetition for general games. In *Proceedings of the 47th Annual ACM on Symposium on Theory of Computing*, pages 335–340. ACM, 2015.

[39] S. Bravyi. Efficient algorithm for a quantum analogue of 2-SAT. *Contemporary Mathematics*, 536:33–48, 2011.

[40] N. Brunner, S. Pironio, A. Acin, N. Gisin, A. Méthot, and V. Scarani. Testing the dimension of Hilbert spaces. *Physical Review Letters*, 100:210503, 2008.

[41] A. Cabello. Bell's theorem without inequalities and without probabilities for two observers. *Physical Review Letters*, 86:1911–1914, 2001.

[42] A. Chailloux and G. Scarpa. Parallel repetition of entangled games with exponential decay via the superposed information cost. In *Automata, Languages, and Programming*, volume 2014 of *Lecture Notes in Computer Science*, pages 296–307. Springer, 2014.

[43] A. Chiesa and M. Forbes. Improved soundness for QMA with multiple provers. *Chicago Journal of Theoretical Computer Science*, 2013:1–23, 2013.

[44] J. Clauser, M. Horne, A. Shimony, and R. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880–884, 1969.

[45] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca. Quantum algorithms revisited. *Proceedings of the Royal Society*, A454:339–354, 1998.

[46] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of the 19th Conference on Computational Complexity*, pages 236–249, 2004.

[47] R. Cleve, W. Slofstra, F. Unger, and S. Upadhyay. Perfect parallel repetition theorem for quantum XOR proof systems. *Computational Complexity*, 17(2):282–299, 2008.

[48] A. Connes. Classification of injective factors cases II_1, II_∞, III_λ, $\lambda \neq 1$. *Annals of Mathematics*, 104(1):73–115, 1976.

[49] S. Cook. The complexity of theorem proving procedures. In *Proceedings of the 3rd Annual ACM Symposium on Theory of Computing*, pages 151–158, 1971.

[50] T. Cooney, M. Junge, C. Palazuelos, and D. Pérez-García. Rank-one quantum games. *Computational Complexity*, 24(1):133–196, 2011.

[51] T. Cubitt and A. Montanaro. Complexity classification of local Hamiltonian problems. In *Proceedings of the 55th Annual IEEE Symposium on Foundations of Computer Science*, pages 120–129, 2014.

[52] I. Damgård and C. Lunemann. Quantum-secure coin-flipping and applications. In *Advances in Cryptology – ASIACRYPT 2009*, volume 5912 of *Lecture Notes in Computer Science*, pages 52–69. Springer, 2009.

[53] I. Dinur and D. Steurer. Analytical approach to parallel repetition. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, pages 624–633, 2014.

[54] I. Dinur, D. Steurer, and T. Vidick. A parallel repetition theorem for entangled projection games. In *Proceedings of the 29th Conference on Computational Complexity*, pages 197–208, 2014.

[55] J. Edmonds. Minimum partition of a matroid into independent subsets. *Journal of Research of the National Bureau of Standards Section B: Mathematics and Mathematical Physics*, 69B(1–2):67–72, 1965.

[56] J. Edmonds. Paths, trees, and flowers. *Canadian Journal of Mathematics*, 17(3):449–467, 1965.

[57] U. Feige, S. Goldwasser, L. Lovász, S. Safra, and M. Szegedy. Interactive proofs and the hardness of approximating cliques. *Journal of the ACM*, 43(2):268–292, 1996.

[58] U. Feige and J. Kilian. Two-prover protocols—low error at affordable rates. *SIAM Journal on Computing*, 30(1):324–346, 2000.

[59] U. Feige and L. Lovász. Two-prover one-round proof systems: Their power and their problems. In *Proceedings of the 24th Annual ACM Symposium on Theory of Computing*, pages 733–744, 1992.

[60] J. Fitzsimons and T. Vidick. A multiprover interactive proof system for the local Hamiltonian problem. In *Proceedings of the 6th Conference on Innovations in Theoretical Computer Science*, pages 103–112, 2015.

[61] L. Fortnow. The complexity of perfect zero-knowledge. In S. Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, pages 327–343. Greenwich: JAI Press, 1989.

[62] L. Fortnow. *Complexity-Theoretic Aspects of Interactive Proof Systems.* PhD thesis, Massachusetts Institute of Technology, 1989.

[63] L. Fortnow and J. Rogers. Complexity limitations on quantum computation. *Journal of Computer and System Sciences*, 59(2):240–252, 1999.

[64] L. Fortnow, J. Rompel, and M. Sipser. On the power of multi-prover interactive protocols. In *Proceedings of the 3rd Annual Structure in Complexity Theory Conference*, pages 156–161, 1988.

[65] T. Fritz. Tsirelson's problem and Kirchberg's conjecture. *Reviews in Mathematical Physics*, 24(05):1250012, 2012.

[66] S. Gharibian. Strong NP-hardness of the quantum separability problem. *Quantum Information & Computation*, 10(3):343–360, 2010.

[67] S. Gharibian and J. Kempe. Hardness of approximation for quantum problems. In *Automata, Languages, and Programming*, volume 7391 of *Lecture Notes in Computer Science*, pages 387–398. Springer, 2012.

[68] S. Gharibian and J. Sikora. Ground state connectivity of local Hamiltonians. Available as arXiv.org e-Print 1409.3182, 2014.

[69] O. Goldreich. Zero-knowledge twenty years after its invention. Electronic Colloquium on Computational Complexity Report 2002/186, 2002.

[70] O. Goldreich, A. Sahai, and S. Vadhan. Honest verifier statistical zero knowledge equals general statistical zero knowledge. In *Proceedings of the 30th Annual ACM Symposium on Theory of Computing*, pages 23–26, 1998.

[71] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. In *Proceedings of the 17th Annual ACM Symposium on Theory of Computing*, pages 291–304, 1985.

[72] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, 1989.

[73] S. Goldwasser and M. Sipser. Private coins versus public coins in interactive proof systems. In S. Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, pages 73–90. Greenwich: JAI Press, 1989.

[74] D. Gosset and D. Nagaj. Quantum 3-SAT is QMA1-complete. In *Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science*, pages 756–765, 2013.

[75] D. Gottesman and S. Irani. The quantum and classical complexity of translationally invariant tiling and Hamiltonian problems. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 95–104, 2009.

[76] A. Grilo, I. Kerenidis, and J. Sikora. Quantum NP - a survey. Available as arXiv.org e-Print quant-ph/0210077, 2002.

[77] A. Grilo, I. Kerenidis, and J. Sikora. QMA with subset state witnesses. Available as arXiv.org e-Print 1410.2882, 2014.

[78] L. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, pages 212–219, 1996.

[79] L. Gurvits. Classical deterministic complexity of Edmonds' problem and quantum entanglement. In *Proceedings of the 35th Annual ACM Symposium on Theory of Computing*, pages 1–19, 2003.

[80] G. Gutoski. Upper bounds for quantum interactive proofs with competing provers. In *Proceedings of the 20th Conference on Computational Complexity*, pages 334–343, 2005.

[81] G. Gutoski. *Quantum Strategies and Local Operations*. PhD thesis, University of Waterloo, 2009.

[82] G. Gutoski, P. Hayden, K. Milner, and M. Wilde. Quantum interactive proofs and the complexity of separability testing. *Theory of Computing*, 11(3):59–103, 2015.

[83] G. Gutoski and J. Watrous. Quantum interactive proofs with competing provers. In *Proceedings of the 22nd Symposium on Theoretical Aspects of Computer Science*, volume 3404 of *Lecture Notes in Computer Science*, pages 605–616. Springer, 2005.

[84] G. Gutoski and J. Watrous. Toward a general theory of quantum games. In *Proceedings of the 39th Annual ACM Symposium on Theory of Computing*, pages 565–574, 2007.

[85] G. Gutoski and X. Wu. Parallel approximation of min-max problems. *Computational Complexity*, 22(2):385–428, 2013.

[86] S. Hallgren, A. Kolla, P. Sen, and S. Zhang. Making classical honest verifier zero knowledge protocols secure against quantum attacks. In *Proceedings of the 35th International Colloquium on Automata, Languages and Programming*, volume 5126 of *Lecture Notes in Computer Science*, pages 592–603. Springer, 2008.

[87] S. Hallgren, A. Smith, and F. Song. Classical cryptographic protocols in a quantum world. In *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *Lecture Notes in Computer Science*, pages 411–428. Springer, 2011.

[88] A. Harrow and A. Montanaro. Testing product states, quantum Merlin–Arthur games and tensor optimization. *Journal of the ACM*, 60(1):3, 2013.

[89] J. Håstad. Some optimal inapproximability results. *Journal of the ACM*, 48:798–859, 2001.

[90] P. Hayden, K. Milner, and M. Wilde. Two-message quantum interactive proofs and the quantum separability problem. *Quantum Information & Computation*, 14(5&6):384–416, 2014.

[91] T. Holenstein. Parallel repetition: Simplifications and the no-signaling case. *Theory of Computing*, 5:141–172, 2009.

[92] T. Ito. Parallelization of entanglement-resistant multi-prover interactive proofs. *Information Processing Letters*, 114(10):579–583, 2014.

[93] T. Ito, H. Kobayashi, and K. Matsumoto. Oracularization and two-prover one-round interactive proofs against nonlocal strategies. In *Proceedings of the 24th Conference on Computational Complexity*, pages 217–228, 2009.

[94] T. Ito, H. Kobayashi, and J. Watrous. Quantum interactive proofs with weak error bounds. In *Proceedings of the 3rd Conference on Innovations in Theoretical Computer Science*, pages 266–275, 2012.

[95] T. Ito and T. Vidick. A multi-prover interactive proof for NEXP sound against entangled provers. *Proceedings of the 53rd IEEE Symposium on Foundations of Computer Science*, pages 243–252, 2012.

[96] R. Jain, Z. Ji, S. Upadhyay, and J. Watrous. QIP = PSPACE. *Journal of the ACM*, 58(6):30, 2011.

[97] R. Jain, I. Kerenidis, G. Kuperberg, M. Santha, O. Sattath, and S. Zhang. On the power of a unique quantum witness. *Theory of Computing*, 8(17):375–400, 2012.

[98] R. Jain, A. Pereszlényi, and P. Yao. A parallel repetition theorem for entangled two-player one-round games under product distributions. In *Proceedings of the 29th Conference on Computational Complexity*, pages 209–216, 2014.

[99] R. Jain, S. Upadhyay, and J. Watrous. Two-message quantum interactive proofs are in PSPACE. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 534–543, 2009.

[100] R. Jain and J. Watrous. Parallel approximation of non-interactive zero-sum quantum games. In *Proceedings of the 24th Conference on Computational Complexity*, pages 243–253, 2009.

[101] D. Janzing, P. Wocjan, and T. Beth. “Non-identity-check” is QMA-complete. *International Journal of Quantum Information*, 3(3):463–473, 2005.

[102] Z. Ji. Classical verification of quantum proofs. Available as arXiv.org e-Print 1505.07432, 2015.

[103] M. Junge, M. Navascues, C. Palazuelos, D. Perez-Garcia, V. Scholz, and R. Werner. Connes’ embedding problem and Tsirelson’s problem. *Journal of Mathematical Physics*, 52(1):012102, 2011.

[104] S. Kale. *Efficient Algorithms Using the Multiplicative Weights Update Method*. PhD thesis, Princeton University, 2007.

[105] R. Karp. Reducibility among combinatorial problems. In R. Miller and J. Thatcher, editors, *Complexity of Computer Computations*, pages 85–103. Plenum Press, New York, 1972.

[106] P. Kaye, R. Laflamme, and M. Mosca. *An Introduction to Quantum Computing*. Oxford University Press, 2007.

[107] J. Kempe, A. Kitaev, and O. Regev. The complexity of the local Hamiltonian problem. *SIAM Journal on Computing*, 35(5):1070–1097, 2006.

[108] J. Kempe, H. Kobayashi, K. Matsumoto, B. Toner, and T. Vidick. Entangled games are hard to approximate. *SIAM Journal on Computing*, 40(3):848–877, 2011.

[109] J. Kempe, H. Kobayashi, K. Matsumoto, and T. Vidick. Using entanglement in quantum multi-prover interactive proofs. *Computational Complexity*, 18:273–307, 2009.

[110] J. Kempe and O. Regev. 3-local Hamitonian is QMA-complete. *Quantum Information & Computation*, 3(3):258–264, 2003.

[111] J. Kempe and T. Vidick. Parallel repetition of entangled games. In *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing*, pages 353–362, 2011.

[112] E. Kirchberg. On non-semisplit extensions, tensor products and exactness of group C^*-algebras. *Inventiones Mathematicae*, 112(1):449–489, 1993.

[113] A. Kitaev, A. Shen, and M. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

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

[115] E. Knill. Quantum randomness and nondeterminism. Technical Report LAUR-96-2186, Los Alamos National Laboratory, 1996. Available as arXiv.org e-Print quant-ph/9610012.

[116] H. Kobayashi. Non-interactive quantum perfect and statistical zero-knowledge. In *Proceedings of the 14th International Symposium on Algorithms and Computation*, volume 2906 of *Lecture Notes in Computer Science*, pages 178–188. Springer, 2003.

[117] H. Kobayashi. General properties of quantum zero-knowledge proofs. In *Proceedings of the 5th IACR Theory of Cryptography Conference*, volume 4948 of *Lecture Notes in Computer Science*, pages 107–124. Springer, 2008.

[118] H. Kobayashi, F. Le Gall, and H. Nishimura. Stronger methods of making quantum interactive proofs perfectly complete. In *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science*, pages 329–352, 2013.

[119] H. Kobayashi and K. Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *Journal of Computer and System Sciences*, 66(3):429–450, 2003.

[120] H. Kobayashi, K. Matsumoto, and T. Yamakami. Quantum Merlin–Arthur proof systems: Are multiple Merlins more helpful to Arthur? In *Algorithms and Computation*, volume 2906 of *Lecture Notes in Computer Science*, pages 189–198. Springer, 2003.

[121] D. Leung, B. Toner, and J. Watrous. Coherent state exchange in multi-prover quantum interactive proof systems. *Chicago Journal of Theoretical Computer Science*, 2013:11, 2013.

[122] L. Levin. Universal sequential search problems (English translation). *Problems of Information Transmission*, 9(3):265–266, 1973.

[123] Y.-K. Liu. Consistency of local density matrices is QMA-complete. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, volume 4110 of *Lecture Notes in Computer Science*, pages 438–449. Springer, 2006.

[124] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, 1992.

[125] C. Marriott and J. Watrous. Quantum Arthur–Merlin games. *Computational Complexity*, 14(2):122–152, 2005.

[126] M. McKague, T. Yang, and V. Scarani. Robust self-testing of the singlet. *Journal of Physics A: Mathematical and Theoretical*, 45(45):455304, 2012.

[127] D. Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, 65(27):3373–3376, 1990.

[128] R. Mittal and M. Szegedy. Product rules in semidefinite programming. In *Fundamentals in Computation Theory*, volume 4639 of *Lecture Notes in Computer Science*, pages 435–445. Springer, 2007.

[129] M. Navascués, S. Pironio, and A. Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, 2008.

[130] C. Neff. Specified precision polynomial root isolation is in NC. *Journal of Computer and System Sciences*, 48(3):429–463, 1994.

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

[132] H. Nishimura and T. Yamakami. Polynomial time quantum computation with advice. *Information Processing Letters*, 90(4):195–204, 2004.

[133] R. O'Donnell. A history of the PCP theorem, 2005. Available at `http://courses.cs.washington.edu/courses/cse533/05au/pcp-history.pdf`.

[134] T. Okamoto. On relationships between statistical zero-knowledge proofs. *Journal of Computer and System Sciences*, 60(1):47–108, 2000.

[135] R. Oliveira and B. Terhal. The complexity of quantum spin systems on a two-dimensional square lattice. *Quantum Information & Computation*, 8(10):900–924, 2008.

[136] N. Ozawa. About the QWEP conjecture. *International Journal of Mathematics*, 15(05):501–530, 2004.

[137] N. Ozawa. About the Connes embedding conjecture. *Japanese Journal of Mathematics*, 8(1):147–183, 2013.

[138] C. Papadimitriou and M. Yannakakis. The complexity of facets (and some facets of complexity). *Journal of Computer and System Sciences*, 28(2):244–259, 1984.

[139] A. Peres. Incompatible results of quantum measurements. *Physics Letters A*, 151(3–4):107–108, 1990.

[140] R. Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27(3):763–803, 1998.

[141] O. Regev and T. Vidick. Quantum XOR games. In *Proceedings of the 28th Conference on Computational Complexity*, pages 144–155, 2013.

[142] B. Reichardt, F. Unger, and U. Vazirani. A classical leash for a quantum system: Command of quantum systems via rigidity of CHSH games. Available as arXiv.org e-Print 1209.0448, 2012.

[143] B. Reichardt, F. Unger, and U. Vazirani. Classical command of quantum systemes. *Nature*, 496(7446):456–460, 2013.

[144] B. Rosgen. Additivity and distinguishability of random unitary channels. *Journal of Mathematical Physics*, 49(10):102107, 2008.

[145] B. Rosgen. Distinguishing short quantum computations. In *Proceedings of the 25th International Symposium on Theoretical Aspects of Computer Science*, pages 597–608, 2008.

[146] B. Rosgen. *Computational Distinguishability of Quantum Channels*. PhD thesis, University of Waterloo, 2009.

[147] B. Rosgen and J. Watrous. On the hardness of distinguishing mixed-state quantum computations. In *Proceedings of the 20th Conference on Computational Complexity*, pages 344–354, 2005.

[148] A. Sahai and S. Vadhan. A complete promise problem for statistical zero-knowledge. *Journal of the ACM*, 50(2):196–249, 2003.

[149] V. Scholz and R. Werner. Tsirelson's problem. Available as arXiv.org e-Print 0812.4305.

[150] A. Shamir. IP = PSPACE. *Journal of the ACM*, 39(4):869–877, 1992.

[151] P. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[152] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[153] W. Slofstra. Lower bounds on the entanglement needed to play XOR non-local games. *Journal of Mathematical Physics*, 52(10):102202, 2011.

[154] R. Spekkens and T. Rudolph. Degrees of concealment and bindingness in quantum bit-commitment protocols. *Physical Review A*, 65(1):123410, 2001.

[155] B. Terhal. Is entanglement monogamous? *IBM Journal of Research and Development*, 48:71–78, 2004.

[156] B. Toner. Monogamy of non-local quantum correlations. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, volume 465, pages 59–69, 2009.

[157] B. Tsirelson. Bell inequalities and operator algebras. Available at `http://www.tau.ac.il/~tsirel/download/bellopalg.pdf`.

[158] B. Tsirel'son. Quantum analogues of the Bell inequalities: The case of two spatially separated domains. *Journal of Soviet Mathematics*, 36:557–570, 1987.

[159] D. Unruh. Quantum proofs of knowledge. In *Advances in Cryptology – Eurocrypt 2012*, volume 7237 of *Lecture Notes in Computer Science*, pages 135–152. Springer, 2012.

[160] L. Valiant and V. Vazirani. NP is as easy as detecting unique solutions. *Theoretical Computer Science*, 47:85–93, 1986.

[161] W. van Dam and P. Hayden. Universal entanglement transformations without communication. *Physical Review A*, 67(6):060302, 2003.

[162] J. van de Graaf. *Towards a Formal Definition of Security for Quantum Protocols*. PhD thesis, Université de Montréal, 1997.

[163] T. Vértesi and K. Pál. Bounding the dimension of bipartite quantum systems. *Physical Review A*, 79:042106, 2009.

[164] M. Warmuth and D. Kuzmin. Online variance minimization. In *Proceedings of the 19th Annual Conference on Learning Theory*, volume 4005 of *Lecture Notes in Computer Science*, pages 514–528. Springer, 2006.

[165] J. Watrous. PSPACE has constant-round quantum interactive proof systems. In *Proceedings of the 40th Annual IEEE Symposium on Foundations of Computer Science*, pages 112–119, 1999.

[166] J. Watrous. Succinct quantum proofs for properties of finite groups. In *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science*, pages 537–546, 2000.

[167] J. Watrous. Limits on the power of quantum statistical zero-knowledge. In *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science*, pages 459–468, 2002.

[168] J. Watrous. PSPACE has constant-round quantum interactive proof systems. *Theoretical Computer Science*, 292(3):575–588, 2003.

[169] J. Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009.

[170] S. Wehner. Entanglement in interactive proof systems with binary answers. In *Proceedings of the 23rd Annual Symposium on Theoretical Aspects of Computer Science*, volume 3884 of *Lecture Notes in Computer Science*, pages 162–171, 2006.

[171] X. Wu. Equilibrium value method for the proof of QIP=PSPACE. Available as arXiv.org e-Print 1004.0264, 2010.

[172] X. Wu, K.-M. Chung, and H. Yuen. Parallel repetition for entangled k-player games via fast quantum search. In *Proceedings of the 30th Conference on Computational Complexity*, volume 33 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 512–536. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2015.