Towards Perfect Completeness in QMA

Stephen P. Jordan[*]
NIST
Gaithersburg, MD, USA

Hirotada Kobayashi
NII
Tokyo, Japan

François Le Gall
The University of Tokyo
Tokyo, Japan

Daniel Nagaj[*]
University of Vienna
Vienna, Austria

Harumichi Nishimura[*]
Nagoya University
Nagoya, Japan

Abstract

This talk presents two results, both of which are quantumly nonrelativizing, and arguably step towards affirmatively settling the QMA versus QMA_1 problem (i.e., the problem of whether quantum Merlin-Arthur proof systems with one-sided bounded error of perfect completeness have verification power equivalent to general quantum Merlin-Arthur proof systems with two-sided bounded error).

First, it is proved that classical-witness quantum Merlin-Arthur proof systems can achieve perfect completeness. That is, $\mathrm{QCMA} = \mathrm{QCMA}_1$. This holds under any gate set with which the Hadamard and arbitrary classical reversible transformations can be exactly implemented, *e.g.*, {Hadamard, Toffoli, NOT}. The proof uses a simple but novel quantum technique that *additively* adjusts the success probability, which may be of independent interest.

Second, it is proved that any problem in QMA has a two-message quantum interactive proof system of perfect completeness with constant soundness error, where the verifier has only to send a constant number of halves of EPR pairs. This in particular implies that the class QMA is necessarily included by the class $\mathrm{QIP}_1(2)$ of problems having two-message quantum interactive proofs of perfect completeness, which gives the first nontrivial upper bound for QMA in terms of quantum interactive proofs.

This talk is based on the following two papers:

- Stephen P. Jordan, Hirotada Kobayashi, Daniel Nagaj, and Harumichi Nishimura. Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. *Quantum Information and Computation*, 12(5–6):0461–0471, 2012. arXiv:1111.5306v2 [quant-ph].
- Hirotada Kobayashi, François Le Gall, and Harumichi Nishimura. Stronger methods of making quantum interactive proofs perfectly complete. In *Proceedings of the 4th Innovations in Theoretical Computer Science Conference*, 2013. To appear. arXiv:1210.1290 [quant-ph].

[*] Part of this work was done while SJ was at the Institute for Quantum Information, California Institute of Technology, Pasadena, CA, USA, DN was at the Research Center for Quantum Information, Institute of Physics, Slovak Academy of Sciences, Bratislava, Slovakia, and HN was at the Department of Mathematics and Information Sciences, Graduate School of Science, Osaka Prefecture University, Sakai, Osaka, Japan.

1 Background and Motivation

The classical complexity class MA of problems having Merlin-Arthur (MA) proof systems, first introduced by Babai [Bab85], is a natural probabilistic generalization of the class NP. Informally, in a Merlin-Arthur proof system, Arthur, a probabilistic polynomial-time verifier, first receives a message (a witness) from Merlin, an all-powerful but untrustworthy prover, and then checks with high probability the validity of Merlin's claim that the common input is a yes-instance of the problem.

Quantum Merlin-Arthur (QMA) proof systems are a generalization of the Merlin-Arthur proof systems to the quantum setting, whose notion was already discussed at an early stage of quantum computing research in a technical report by Knill [Kni96]. In this setting, Arthur now receives a quantum witness from Merlin and performs polynomial-time quantum computation to check with high probability whether the input is a yes-instance or not. The resulting complexity class is called QMA [Wat00] (originally called BQNP [Kit99, KSV02]), and has been central to the development of quantum complexity theory in that it plays a role similar to that NP plays in classical computation.

The standard way of defining MA and QMA allows two-sided bounded error: each yes-instance may be wrongly rejected with small probability (completeness error), while each no-instance may also be wrongly accepted with small probability (soundness error). If completeness error is zero, that is, yes-instances are never wrongly rejected, the corresponding system is said to have *perfect completeness*. The versions of MA and QMA with perfect completeness are denoted by MA_1 and QMA_1, respectively.

Classically, it is known that any Merlin-Arthur proof system that may have two-sided bounded error can always be modified into another Merlin-Arthur proof system with one-sided bounded error of perfect completeness, i.e., $\mathrm{MA} = \mathrm{MA}_1$ holds [ZF87, GZ11]. A natural question to ask is whether the same property holds for quantum Merlin-Arthur proof systems as well, i.e., whether $\mathrm{QMA} = \mathrm{QMA}_1$. This question still remains unsolved after many years of investigation. Besides its theoretical interest, answering this question by the affirmative would lead to many consequences. In particular, any computational problem complete for the class QMA_1, such as QUANTUM SATISFIABILITY (QSAT) [Bra06], would immediately become complete for the class QMA as well. Furthermore, for several years, researchers have been trying to prove a quantum analogue [AALV09, AALV11, AE11] of the celebrated PCP theorem [AS98, ALM$^+$98]. A proof that $\mathrm{QMA} = \mathrm{QMA}_1$ could aid in this goal, because one-sided error verifications are much easier to treat, and also because the QSAT problems are more direct quantum analogues of the SAT problems than the LOCAL HAMILTONIAN problems. Thus, one could draw a closer parallel to the classical PCP theorem, which can be viewed as proving the NP-completeness of a special case of the 3SAT problem in which, for every no-instance, at most a constant fraction of clauses are simultaneously satisfiable.

As a barrier to affirmatively answering the QMA versus QMA_1 question, Aaronson [Aar09] constructed a quantum oracle relative to which QMA_1 is a proper subclass of QMA, which means that a "black-box" proof of $\mathrm{QMA} = \mathrm{QMA}_1$ cannot exist. Nevertheless, no classical oracle is known that separates QMA_1 from QMA, and Nagaj, Wocjan, and Zhang [NWZ09] made a step towards an affirmative answer to the question by showing that perfect completeness is achievable for a special case of quantum Merlin-Arthur proof systems in which some real number related to the maximum acceptance probability of a given system can be exactly expressed with a bit string of polynomial length.

Quantum Merlin-Arthur proof systems may be viewed as a special case of more general quantum interactive proof systems, where the verifier and the prover may exchange messages using many rounds of communications. In their seminal paper, Kitaev and Watrous [KW00] showed that perfect completeness is achievable in quantum interactive proof systems. More precisely, with two additional messages, any quantum interactive proof system that may involve two-sided bounded error can be transformed into another quantum interactive proof system that has one-sided bounded error of perfect completeness. This in particular implies that $\mathrm{QMA} \subseteq \mathrm{QIP}_1(3)$, where $\mathrm{QIP}_1(3)$ is the class of problems having three-message quantum interactive proof systems of perfect completeness. Unfortunately, $\mathrm{QIP}_1(3)$ is already so powerful that it includes PSPACE [Wat03] (actually, $\mathrm{QIP}_1(3) = \mathrm{QIP} = \mathrm{PSPACE}$ [KW00, JJUW11], where QIP denotes the class of problems having general quantum interactive proofs). Accordingly, this only gives a weaker result for the upper bound of QMA, as QMA is known to be inside PP [KW00, Wat00, MW05] (in fact, a slightly stronger bound $\mathrm{QMA} \subseteq \mathrm{A_0PP} = \mathrm{SBQP}$ is known [Vya03, Kup09]).

2 Our Results and Their Meaning

Achieving Perfect Completeness in Classical-Witness Quantum Merlin-Arthur Proof Systems. First, it is proved that perfect completeness is indeed achievable in quantum Merlin-Arthur proof systems *of classical witness*, under a reasonable assumption on the gate set that Hadamard transformations and all classical reversible transformations can be exactly implemented.

Theorem 1. $\mathrm{QCMA} = \mathrm{QCMA}_1$ *(or* $\mathrm{MQA} = \mathrm{MQA}_1$ *in a recently-proposed terminology [Wat09a, GSU11]).*

Here QCMA (or MQA) is the class of problems having quantum Merlin-Arthur proof systems with two-sided bounded error in which Arthur, the verifier, can receive only a classical witness from Merlin, the prover, and QCMA_1 (or MQA_1) is the one-sided bounded error version of this complexity class with perfect completeness. Note that the quantum oracle of Aaronson [Aar09] also separates QCMA_1 from QCMA, and our proof of $\mathrm{QCMA} = \mathrm{QCMA}_1$ is quantumly nonrelativizing, for it makes use of an explicit representation of amplitudes. To the best knowledge of the authors, this is the first "nontrivial" example that overcomes a quantum oracle separation (except quantumly nonrelativizing "trivial" containments such as $\mathrm{BQP} \subseteq \mathrm{ZQEXP}$ as found in Ref. [Aar09]). This suggests that the oracle separation of Ref. [Aar09] may not be an insurmountable barrier to proving $\mathrm{QMA} = \mathrm{QMA}_1$, and our proof may provide guidance on approaching the longstanding QMA versus QMA_1 problem, and on developing quantumly nonrelativizing techniques in general. It is also interesting to note that, as a corollary of our result, the solutions to the known QCMA-complete problems [WJB03] can be verified with perfect completeness.

The basic strategy to prove Theorem 1 is very simple: Given any QCMA proof system with two-sided error, one considers letting Arthur receive a description of the acceptance probability in addition to the original classical witness. This allows Arthur to adjust the acceptance probability by standard exact amplitude amplification [BHMT02, CK98] or Watrous's quantum rewinding [Wat09b, KKMV09]. One obvious problem in this approach is that the original acceptance probability might not be expressible exactly with polynomially many bits. This can be overcome by making use of the robustness of the two-sided error complexity class QCMA against the choice of gate set. Specifically, one can assume without loss of generality that the verification procedure of the original two-sided error QCMA system is implemented only with Hadamard, Toffoli, and NOT gates [Shi02, Aha03]. This ensures that any possible acceptance probability on input x in this system is exactly equal to $k/2^{l(|x|)}$ for some integer k and some polynomially bounded, integer-valued function l.

Another problem, which is more difficult to overcome, is that Arthur may not be able to appropriately adjust the acceptance probability without error, even if he knows the original acceptance probability. The standard way to adjust success probability in exact amplitude amplification is a "multiplicative" method that applies some suitable rotation operator. This rotation depends on the input length, and cannot be exactly implemented with a fixed finite gate set in general. We overcome this difficulty by introducing a simple but novel "additive" method of adjusting the acceptance probability. The goal is to have a base procedure whose initial acceptance probability is exactly $1/2$, which leads to a protocol with perfect completeness via quantum rewinding (the choice of quantum rewinding rather than exact amplitude amplification is just for ease of analysis, and is not essential).

On input x, Arthur receives as a witness a string w and an integer k, written using $l(|x|)$ bits, where w is expected to be the witness he would receive in the original system, and k is expected such that $k/2^{l(|x|)}$ equals the acceptance probability $p_{x,w}$ on input x and witness w in the original system. If the claimed k is too small relative to the value computed from the original completeness condition, Arthur rejects. Otherwise Arthur performs with equal amplitude the original verification test and an additional second test, where Arthur generates a uniform superposition of values from 1 to $2^{l(|x|)}$ and simply accepts if this value is more than k. Notice that this second test is exactly implementable only with the Hadamard and classical reversible transformations. Clearly, the honest Merlin can prepare some suitable pair (w, k) with which Arthur accepts with probability $p_{x,w}$ in the original verification test and with probability $1 - k/2^{l(|x|)} = 1 - p_{x,w}$ in the second test. Hence, this base procedure has its initial success probability exactly $1/2$ for yes-instances, and one can construct a system of perfect completeness via quantum rewinding, similar to the case of quantum multi-prover interactive proofs [KKMV09]. For a dishonest Merlin, any possible w must have a small $p_{x,w}$ value while k must be such that the value $k/2^{l(|x|)}$ is large, and thus, whichever pair (w, k) is prepared, the initial success probability of the base procedure must be less than $1/2$, which ensures soundness. To the best knowledge of the authors, no such "additive" method of amplitude adjustment has appeared in the literature previously, and the authors believe it may have other applications in quantum complexity theory.

The full version of this part can be found in Ref. [JKNN12].

Stronger Methods of Making Quantum Interactive Proofs Perfectly Complete. This talk further presents new general techniques to transform quantum interactive proof systems into those of perfect completeness, which increase the number of messages by just one. In particular, it is proved that any problem in QMA has a two-message quantum interactive proof of perfect completeness.

Theorem 2. $\mathrm{QMA} \subseteq \mathrm{QIP}_1(2)$.

Here $\mathrm{QIP}_1(2)$ is the class of problems having two-message quantum interactive proof systems of perfect completeness (with negligible soundness error). This gives the first nontrivial upper bound of QMA in terms of quantum interactive proofs, which has no relation known to the existing upper bound $\mathrm{A_0PP} = \mathrm{SBQP} \subseteq \mathrm{PP}$. Note that the inclusion $\mathrm{QMA} \subseteq \mathrm{QIP}(2)$ is indeed trivial for the two-sided error class $\mathrm{QIP}(2)$ of two-message quantum interactive proofs, but the inclusion here is by the one-sided error class $\mathrm{QIP}_1(2)$ and is nontrivial to prove.

In fact, we prove a much stronger result, which arguably steps towards settling the QMA versus QMA_1 question. Namely, we show that, to achieve perfect completeness with constant soundness error, the verifier in the two-message quantum interactive proof system has only to send a constant number of halves of EPR pairs to the prover. Or in other words, any problem in QMA has a quantum Merlin-Arthur proof system of perfect completeness with constant soundness error, in which Arthur and Merlin share a constant number of EPR pairs *a priori*. More formally, let $\mathrm{QMA}^{k\text{-EPR}}(c, s)$ denote the class of problems having quantum Merlin-Arthur proof systems with completeness c and soundness s, where Arthur and Merlin initially share k EPR pairs. Then we have the following containment.

Theorem 3. *For any constant* $s \in (0, 1]$, *there exists a constant* $k \in \mathbb{N}$ *such that* $\mathrm{QMA} \subseteq \mathrm{QMA}^{k\text{-EPR}}(1, s)$.

Theorem 2 is an immediate consequence of Theorem 3, as one may view quantum Merlin-Arthur proof systems with shared EPR pairs as a special case of two-message quantum interactive proofs where the verifier first generates the EPR pairs and sends halves of them to the prover (and the parallel repetition of two-message quantum interactive proofs works perfectly [KW00]). Theorem 3 nevertheless appears to be much stronger than Theorem 2 since it shows that perfect completeness is achievable with just one additional message of a very restricted form (a constant number of halves of EPR pairs). To see this, let $\mathrm{QMA}^{\text{const-EPR}}$ be the class of problems having quantum Merlin-Arthur proof systems with a constant number of prior shared EPR pairs that may involve two-sided bounded error, and let $\mathrm{QMA}_1^{\text{const-EPR}}$ be that of perfect completeness. Then, indeed, the equality $\mathrm{QMA}^{\text{const-EPR}} = \mathrm{QMA}$ immediately follows from the result by Beigi, Shor, and Watrous [BSW11], as any quantum Merlin-Arthur proof system with a constant number of prior shared EPR pairs is a special case of two-message quantum interactive proofs *with short questions* (i.e., two-message quantum interactive proofs with the first message consisting of at most logarithmically many qubits). Therefore, we obtain the following characterization of QMA.

Corollary 4. $\mathrm{QMA}_1^{\text{const-EPR}} = \mathrm{QMA}^{\text{const-EPR}} = \mathrm{QMA}$.

This in particular implies that perfect completeness is achievable for the model of quantum Merlin-Arthur proof systems with a constant number of prior shared EPR pairs, a model that has computational power equivalent to QMA. Similar arguments further imply that perfect completeness is achievable even with the models of quantum Merlin-Arthur proof systems with a logarithmic number of prior shared EPR pairs and "short-question" two-message quantum interactive proof systems, as both of these have computational power equivalent to QMA.

The methodology developed in this work essentially shows that, in order to obtain the inclusion $\mathrm{QMA} \subseteq \mathrm{QMA}_1$ (and thus immediately the equality $\mathrm{QMA} = \mathrm{QMA}_1$), it is sufficient to find a way of eliminating the need for the constant number of shared EPR pairs in our proof system. In fact, as will be clear from our proof structure, the constant number of shared EPR pairs are necessary only for the purpose of forcing a dishonest prover to send a witness that is close to some maximally entangled state of constant dimensions. Hence, some suitable procedure that tests if a given state of constant dimensions is sufficiently entangled or not may replace the shared EPR pairs to affirmatively answer the QMA versus QMA_1 question (if two-sided error is allowed, such a test is possible with quantum state tomography). Moreover, our construction gives another example of quantumly non-relativizing techniques for quantum interactive proofs, which again indicates that Aaronson's quantum oracle separation [Aar09] may not be an insurmountable barrier when proving that $\mathrm{QMA} = \mathrm{QMA}_1$ or its related results.

For general quantum interactive proof systems, we further present a method that makes any quantum interactive proof system perfectly complete by increasing the number of messages by just one. This improves the previous result due to Kitaev and Watrous [KW00], whose construction increases the number of messages by two, if not using their parallelization result.

The proof idea of Theorem 3 is as follows. Let p_x denote the maximum acceptance probability on input x, over all possible witnesses, of the verification procedure. From the definition of the class QMA we can assume that, for every yes-instance x we have $p_x \geq 1/2$, and for every no-instance x we have $p_x \leq 1/3$. The basic idea of our protocol is to simulate a procedure that we call REFLECTION PROCEDURE. Roughly speaking, this procedure is viewed as performing a part of amplitude amplification [Gro96] on the original verification procedure, and is quite similar to the so-called quantum rewinding technique [Wat09b], the underlying idea of which dates back to the strong amplification method for QMA due to Marriott and Watrous [MW05].

The first problem with this idea is that the verifier does not know in general the probability p_x, and is then not able to apply the desired amplification procedure. Informally, our basic idea to overcome this difficulty consists in asking the prover to send the verifier, along with the witness of the original proof system, a "rotational" adjustment on a qubit (depending on p_x) so that the verifier can apply REFLECTION PROCEDURE with initial success probability being independent of x (precisely speaking, in our actual proof, we do not use rotation operators but instead use reflection operators for adjustment, which slightly simplifies the analysis). In fact, this is done by asking the prover to send two copies of the *Choi-Jamiołkowski state* associated with the adjustment. If the prover is honest, by using the two copies the verifier can simulate REFLECTION PROCEDURE probabilistically with one-sided error, which makes the protocol perfectly complete.

The biggest hurdle in the no-instance case is, of course, that a dishonest prover may not send the prescribed states. In particular, one of the main difficulties is that a dishonest prover may illegally use entanglement among the supposed witness state and copies of the Choi-Jamiołkowski state. Even if a dishonest prover does not use entanglement, there remains another problem that he/she may prepare states different from the supposed copies of the Choi-Jamiołkowski state. In order to force the prover not to use entanglement much, we make use of quantum tools such as the swap test and the quantum de Finetti theorem [KR05, CKMR07]. To further force the prover to send a state close to some desired copies of a Choi-Jamiołkowski state, we also device a test that restricts the Hilbert space in which the verifier expects to receive the copies of the Choi-Jamiołkowski state. The assumption of a constant number of prior-shared EPR pairs is then tactically used with this space-restriction test to finally ensure that the entire witness sent from the prover must be close to some legal state of the prescribed form.

The full version of this part can be found in Ref. [KLGN13].

Acknowledgements

The authors are grateful to Richard Cleve, Michele Mosca, Jake Taylor, and Pawel Wocjan for useful discussions, and to anonymous reviewers for helpful comments on the earlier versions of the papers which this talk is based on. SJ gratefully acknowledges support from the Sherman Fairchild Foundation and NSF grant PHY-0803371 and thanks the Slovak Academy of Sciences for hospitality. HK, FLG, and HN are supported by the Grant-in-Aid for Scientific Research (A) No. 24240001 of the Japan Society for the Promotion of Science and the Grant-in-Aid for Scientific Research on Innovative Areas No. 24106009 of the Ministry of Education, Culture, Sports, Science and Technology in Japan. HK also acknowledges support from the Grant-in-Aid for Scientific Research (B) No. 21300002 of the Japan Society for the Promotion of Science. DN gratefully acknowledges support from the Slovak Research and Development Agency under the contract No. LPP-0430-09, the project APVV-0646-10, and European project Q-ESSENCE. HN also acknowledges support from the Grant-in-Aids for Scientific Research (A) Nos. 21244007 and 23246071 of the Japan Society for the Promotion of Science and the Grant-in-Aid for Young Scientists (B) No. 22700014 of the Ministry of Education, Culture, Sports, Science and Technology in Japan.

References

[AALV09] Dorit Aharonov, Itai Arad, Zeph Landau, and Umesh Vazirani. The detectability lemma and quantum gap amplification [extended abstract]. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing*, pages 417–426, 2009.

[AALV11] Dorit Aharonov, Itai Arad, Zeph Landau, and Umesh Vazirani. The 1D area law and the complexity of quantum states: A combinatorial approach. In *2011 52nd Annual IEEE Symposium on Foundations of Computer Science*, pages 324–333, 2011.

[Aar09] Scott Aaronson. On perfect completeness for QMA. *Quantum Information and Computation*, 9(1–2):0081–0089, 2009.

[AE11] Dorit Aharonov and Lior Eldar. On the complexity of commuting local Hamiltonians, and tight conditions for topological order in such systems. In *2011 52nd Annual IEEE Symposium on Foundations of Computer Science*, pages 334–343, 2011.

[Aha03] Dorit Aharonov. A simple proof that Toffoli and Hadamard are quantum universal. arXiv.org e-Print archive, arXiv:quant-ph/0301040, 2003.

[ALM$^+$98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM*, 45(3):501–555, 1998.

[AS98] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: A new characterization of NP. *Journal of the ACM*, 45(1):70–122, 1998.

[Bab85] László Babai. Trading group theory for randomness. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, pages 421–429, 1985.

[BHMT02] Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. In Samuel Lomonaco, Jr. and Howard E. Brandt, editors, *Quantum Computation and Information*, volume 305 of *Contemporary Mathematics*, pages 53–74. American Mathematical Society, 2002.

[Bra06] Sergey Bravyi. Efficient algorithm for a quantum analogue of 2-SAT. arXiv.org e-Print archive, arXiv:quant-ph/0602108, 2006.

[BSW11] Salman Beigi, Peter Shor, and John Watrous. Quantum interactive proofs with short messages. *Theory of Computing*, 7:101–117 (Article 7), 2011.

[CK98] Dong Pyo Chi and Jinsoo Kim. Quantum database search by a single query. In *Quantum Computing and Quantum Communications, First NASA International Conference, QCQC'98*, volume 1509 of *Lecture Notes in Computer Science*, pages 148–151, 1998.

[CKMR07] Matthias Christandl, Robert König, Graeme Mitchison, and Renato Renner. One-and-a-half quantum de Finetti theorems. *Communications in Mathematical Physics*, 273(2):473–498, 2007.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing*, pages 212–219, 1996.

[GSU11] Sevag Gharibian, Jamie Sikora, and Sarvagya Upadhyay. QMA variants with polynomially many provers. arXiv.org e-Print archive, arXiv:1108.0617 [quant-ph], 2011.

[GZ11] Oded Goldreich and David Zuckerman. Another proof that $\mathrm{BPP} \subseteq \mathrm{PH}$ (and more). In Oded Goldreich, editor, *Studies in Complexity and Cryptography, Miscellanea on the Interplay between Randomness and Computation*, volume 6650 of *Lecture Notes in Computer Science*, pages 40–53. Springer-Verlag, 2011. Electronic Colloquium on Computational Complexity, Report TR97-045, 1997.

[JJUW11] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. $\mathrm{QIP} = \mathrm{PSPACE}$. *Journal of the ACM*, 58(6):Article 30, 2011.

[JKNN12] Stephen P. Jordan, Hirotada Kobayashi, Daniel Nagaj, and Harumichi Nishimura. Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. *Quantum Information and Computation*, 12(5–6):0461–0471, 2012. arXiv:1111.5306v2 [quant-ph].

[Kit99] Alexei Yu. Kitaev. Quantum NP. Talk at the 2nd Workshop on Algorithms in Quantum Information Processing, DePaul University, Chicago, January 1999.

[KKMV09] Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, and Thomas Vidick. Using entanglement in quantum multi-prover interactive proofs. *Computational Complexity*, 18(2):273–307, 2009.

[KLGN13] Hirotada Kobayashi, François Le Gall, and Harumichi Nishimura. Stronger methods of making quantum interactive proofs perfectly complete. In *Proceedings of the 4th Innovations in Theoretical Computer Science Conference*, 2013. To appear. arXiv:1210.1290 [quant-ph].

[Kni96] Emanuel Knill. Quantum randomness and nondeterminism. Technical Report LAUR-96-2186, Los Alamos National Laboratory, 1996. arXiv:quant-ph/9610012.

[KR05] Robert König and Renato Renner. A de Finetti representation for finite symmetric quantum states. *Journal of Mathematical Physics*, 46(12):122108, 2005.

[KSV02] Alexei Yu. Kitaev, Alexander H. Shen, and Mikhail N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, 2002.

[Kup09] Greg Kuperberg. How hard is it to approximate the Jones polynomial? arXiv.org e-print archive, arXiv:0908.0512 [quant-ph], 2009.

[KW00] Alexei Kitaev and John Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof systems. In *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*, pages 608–617, 2000.

[MW05] Chris Marriott and John Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005.

[NWZ09] Daniel Nagaj, Pawel Wocjan, and Yong Zhang. Fast amplification of QMA. *Quantum Information and Computation*, 9(11–12):1053–1068, 2009.

[Shi02] Yaoyun Shi. Both Toffoli and Controlled-NOT need little help to do universal quantum computing. *Quantum Information and Computation*, 3(1):084–092, 2002.

[Vya03] Mikhail N. Vyalyi. $\mathrm{QMA} = \mathrm{PP}$ implies that PP contains PH. Electronic Colloquium on Computational Complexity, Report TR03-021, 2003.

[Wat00] John Watrous. Succinct quantum proofs for properties of finite groups. In *41st Annual Symposium on Foundations of Computer Science*, pages 537–546, 2000.

[Wat03] John Watrous. PSPACE has constant-round quantum interactive proof systems. *Theoretical Computer Science*, 292(3):575–588, 2003.

[Wat09a] John Watrous. Quantum computational complexity. In Robert A. Meyers, editor, *Encyclopedia of Complexity and Systems Science*, pages 7174–7201. Springer-Verlag, 2009.

[Wat09b] John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009.

[WJB03] Pawel Wocjan, Dominik Janzing, and Thomas Beth. Two QCMA-complete problems. *Quantum Information and Computation*, 3(6):635–643, 2003.

[ZF87] Stathis Zachos and Martin Fürer. Probabilistic quantifiers vs. distrustful adversaries. In *Foundations of Software Technology and Theoretical Computer Science, Seventh Conference*, volume 287 of *Lecture Notes in Computer Science*, pages 443–455, 1987.