Quantum interactive proofs with weak error bounds

Tsuyoshi Ito* Hirotada Kobayashi† John Watrous*

A full version is available as arXiv.org e-Print 1012.4427 [quant-ph].
http://arxiv.org/abs/1012.4427

Abstract

We prove that the computational power of quantum interactive proof systems with a double-exponentially small gap in acceptance probability between the completeness case and the soundness case is precisely characterized by EXP, the class of problems solvable in exponential time by deterministic Turing machines. This fact, and our proof of it, has implications concerning quantum and classical interactive proof systems in the setting of unbounded error that include the following:

- Quantum interactive proof systems are strictly more powerful than their classical counterparts in the unbounded-error setting unless $\mathrm{PSPACE} = \mathrm{EXP}$, as even unbounded error classical interactive proof systems can be simulated in PSPACE.
- The recent proof of Jain, Ji, Upadhyay and Watrous (STOC 2010) establishing $\mathrm{QIP} = \mathrm{PSPACE}$ relies heavily on the fact that the quantum interactive proof systems defining the class QIP have bounded error. Our result implies that some nontrivial assumption on the error bounds for quantum interactive proofs is unavoidable to establish this result (unless $\mathrm{PSPACE} = \mathrm{EXP}$).
- To prove our result we give a quantum interactive proof system for EXP with perfect completeness and soundness error $1 - 2^{-2^{poly}}$, for which the soundness error bound is provably tight. This establishes another respect in which quantum and classical interactive proof systems differ, because such a bound cannot hold for any classical interactive proof system: distinct acceptance probabilities for classical interactive proof systems must be separated by a gap that is at least (single-)exponentially small.

We also study the computational power of a few other related unbounded-error complexity classes.

Interactive proof systems [Bab85, GMR89] are a central notion in complexity theory. It is well-known that IP, the class of problems having single-prover classical interactive proof systems with polynomially-bounded verifiers, coincides with PSPACE [Fel86, LFKN92, Sha92], and it was recently proved that the same characterization holds when the prover and verifier have quantum computers [JJUW10]. More succinctly, it holds that

$$\mathrm{IP} = \mathrm{PSPACE} = \mathrm{QIP}. \tag{1}$$

The two equalities in (1) are, in some sense, intertwined: it is only through the trivial relationship $\mathrm{IP} \subseteq \mathrm{QIP}$, together with the landmark result $\mathrm{PSPACE} \subseteq \mathrm{IP}$, that we know $\mathrm{PSPACE} \subseteq \mathrm{QIP}$. While there exist classical refinements [She92, Mei10] of the original method of Lund, Fortnow, Karloff and Nisan [LFKN92] and Shamir [Sha92] used to prove $\mathrm{PSPACE} \subseteq \mathrm{IP}$, there is no "short-cut" known that proves $\mathrm{PSPACE} \subseteq \mathrm{QIP}$ through the use of quantum computation.

*Institute for Quantum Computing and School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada.
†Principles of Informatics Research Division, National Institute of Informatics, Tokyo, Japan.

The opposite containments required to prove the two equalities in the above equation (1) are IP $\subseteq$ PSPACE and QIP $\subseteq$ PSPACE, respectively. The first containment is usually attributed to Feldman [Fel86], and can fairly be described as being straightforward to prove. The standard proof, in fact, gives a polynomial-space algorithm that computes the optimal acceptance probability for a prover in a classical interactive proof system *exactly*, with this optimal probability expressible as some integer divided by 2^k, where k is the maximum number of coin-flips used by the verifier. The proof of the containment QIP $\subseteq$ PSPACE given in [JJUW10], on the other hand, is much more complicated: it uses known properties of QIP [KW00, MW05] to derive a semidefinite programming formulation of it, which is then approximated in PSPACE through the use of an algorithm based on the *matrix multiplicative weights update* method [AK07, WK06]. Unlike the standard proof of IP $\subseteq$ PSPACE, this proof relies heavily on the bounded-error property of the quantum interactive proof systems that define QIP.

There must, of course, be alternate ways to prove QIP $\subseteq$ PSPACE, and we note that Wu [Wu10] and Gutoski and Wu [GW10] have made noteworthy advances in both simplifying and extending the proof method of [JJUW10]. The main question that motivates the work we present here is whether the assumption of bounded-error is *required* to prove QIP $\subseteq$ PSPACE, or could be bypassed. Our results demonstrate that indeed *some* assumption on the gap between completeness and soundness probabilities must be in place to prove QIP $\subseteq$ PSPACE unless PSPACE $=$ EXP.

To explain our results in greater detail it will be helpful to introduce the following notation. Given any choice of functions $m : \mathbb{N} \rightarrow \mathbb{N}$ and $a, b : \mathbb{N} \rightarrow [0,1]$, where we take $\mathbb{N} = \{0,1,2,\ldots\}$, we write $\mathrm{QIP}(m,a,b)$ to denote the class of promise problems $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ having a quantum interactive proof system[1] with $m(|x|)$ messages, completeness probability at least $a(|x|)$ and soundness error at most $b(|x|)$ on all input strings $x \in A_{\mathrm{yes}} \cup A_{\mathrm{no}}$. When sets of functions are taken in place of m, a or b, it is to be understood that a union is implied. For example,

$$\mathrm{QIP}(\mathit{poly}, 1, 1 - 2^{-\mathit{poly}}) = \bigcup_{m,p \in \mathit{poly}} \mathrm{QIP}\left(m, 1, 1 - 2^{-p}\right),$$

where *poly* denotes the set of all functions of the form $p : \mathbb{N} \rightarrow \mathbb{N}$ for which there exists a polynomial-time deterministic Turing machine that outputs $1^{p(n)}$ on input 1^n for all $n \in \mathbb{N}$. We will also frequently refer to functions of the form $f\colon \mathbb{N} \rightarrow [0,1]$ that are polynomial-time computable, and by this it is meant that a polynomial-time deterministic Turing machine exists that, on input 1^n, outputs a rational number $f(n)$ in the range $[0,1]$, represented by a ratio of integers expressed in binary notation. Our main result may now be stated more precisely as follows.

Theorem 1. *It holds that*

$$\bigcup_a \mathrm{QIP}\left(\mathit{poly}, a, a - 2^{-2^{\mathit{poly}}}\right) = \mathrm{QIP}\left(3, 1, 1 - 2^{-2^{\mathit{poly}}}\right) = \mathrm{EXP},$$

where the union is taken over all polynomial-time computable functions $a\colon \mathbb{N} \rightarrow (0,1]$.

Actually the only new relation in the statement of Theorem 1 is

$$\mathrm{EXP} \subseteq \mathrm{QIP}\left(\mathit{poly}, 1, 1 - 2^{-2^{\mathit{poly}}}\right); \tag{2}$$

we have expressed the theorem in the above form only for the sake of clarity. In particular, the containment

$$\mathrm{QIP}\left(\mathit{poly}, 1, 1 - 2^{-2^{\mathit{poly}}}\right) \subseteq \mathrm{QIP}\left(3, 1, 1 - 2^{-2^{\mathit{poly}}}\right)$$

[1] The definitions of quantum computational models based on quantum circuits, including quantum interactive proof systems, is particularly sensitive to the choice of a gate set in the unbounded error setting. For our main result we take the standard Toffoli, Hadamard, $\pi/2$-phase-shift gate set, but relax this choice for a couple of our secondary results.

follows from the fact that

$$\mathrm{QIP}(m,1,1-\varepsilon) \subseteq \mathrm{QIP}\left(3,1,1-\frac{\varepsilon}{(m-1)^2}\right)$$

for all $m \in \mathit{poly}$ and any function $\varepsilon : \mathbb{N} \to [0,1]$, as was proved in [KKMV09] (or an earlier result of [KW00] with a slightly weaker parameter). The containment

$$\mathrm{QIP}\left(3,1,1-2^{-2^{\mathit{poly}}}\right) \subseteq \bigcup_a \mathrm{QIP}\left(\mathit{poly},a,a-2^{-2^{\mathit{poly}}}\right)$$

is trivial. The containment

$$\bigcup_a \mathrm{QIP}\left(\mathit{poly},a,a-2^{-2^{\mathit{poly}}}\right) \subseteq \mathrm{EXP}$$

follows from the results of Gutoski and Watrous [GW07], as a semidefinite program representing the optimal acceptance probability of a given quantum interactive proof system[2] can be solved to an exponential number of bits of accuracy using an exponential-time algorithm [Kha79, GLS88, NN94].

The new containment (2), which represents the main contribution of this work, is proved in two steps. The first step constructs a classical two-prover one-round interactive proof system with one-sided error double-exponentially close to 1 for the EXP-complete SUCCINCT CIRCUIT VALUE problem. It will be proved that in this proof system, provers cannot make the verifier accept no-input strings with probability more than double-exponentially close to 1 even if they are allowed to use a *no-signaling strategy*, i.e., a strategy that cannot be used for communication between them. The second step converts this classical two-prover one-round interactive proof system to a quantum single-prover interactive proof system without ruining its soundness properties.

Theorem 1 and its proof have the following three consequences.

- Unbounded-error classical interactive proof systems recognize exactly PSPACE. Therefore, Theorem 1 implies that unbounded-error quantum interactive proof systems are strictly more powerful than their classical counterparts unless $\mathrm{PSPACE} = \mathrm{EXP}$.

- The dependence on the error bound in the proof in [JJUW10] is not an artifact of the proof techniques, but is a necessity unless $\mathrm{PSPACE} = \mathrm{EXP}$. To be more precise, even though a double-exponential gap is sufficient to obtain the EXP upper bound by applying a polynomial-time algorithm for semidefinite programming, Theorem 1 implies that a double-exponential gap is not sufficient for the PSPACE upper bound unless $\mathrm{PSPACE} = \mathrm{EXP}$.

- Our proof of Theorem 1 shows that a quantum interactive proof system can have a completeness-soundness gap smaller than singly exponential, which cannot happen in classical interactive proof systems. In our quantum interactive proof system for EXP, the gap is double-exponentially small, and this is tight in the sense that a dishonest prover can make the verifier accept with probability double-exponentially close to 1.

We do not know if the double-exponentially small gap in Theorem 1 can be improved to one that is single-exponentially small by constructing a different proof system.

Some additional results concerning unbounded-error quantum interactive proof systems are also discussed.

[2]The results of Gutoski and Watrous [GW07] are actually more general and give the EXP upper bound on the corresponding class with two competing quantum provers. In addition, only mild assumptions on the gate set are needed to obtain this containment. Namely, the containment holds if the gate set consists of finitely many gates and the Choi-Jamiołkowski representation of each gate is a matrix made of rational complex numbers.

References

[AK07] Sanjeev Arora and Satyen Kale. A combinatorial, primal-dual approach to semidefinite programs. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, pages 227–236, June 2007.

[Bab85] László Babai. Trading group theory for randomness. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, pages 496–505, May 1985.

[Fel86] Paul Feldman. The optimum prover lives in PSPACE. Manuscript, 1986.

[GLS88] Martin Grötschel, Lászlá Lovász, and Alexander Schrijver. *Geometric Algorithms and Combinatorial Optimization*, volume 2 of *Algorithms and Combinatorics*. Springer, 1988.

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal on Computing*, 18(1):186–208, February 1989.

[GW07] Gus Gutoski and John Watrous. Toward a general theory of quantum games. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*, pages 565–574, June 2007.

[GW10] Gus Gutoski and Xiaodi Wu. Short quantum games characterize PSPACE, November 2010. Available as arXiv.org e-Print 1011.2787v1 [quant-ph].

[JJUW10] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. $\mathrm{QIP} = \mathrm{PSPACE}$. In *Proceedings of the Forty-Second Annual ACM Symposium on Theory of Computing*, pages 573–582, June 2010.

[Kha79] Leonid G. Khachiyan. A polynomial algorithm in linear programming. *Soviet Mathematics Doklady*, 20(1):191–194, 1979.

[KKMV09] Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, and Thomas Vidick. Using entanglement in quantum multi-prover interactive proofs. *Computational Complexity*, 18(2):273–307, June 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, May 2000.

[LFKN92] Carsten Lund, Lance Fortnow, Howard J. Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, October 1992.

[Mei10] Or Meir. $\mathrm{IP} = \mathrm{PSPACE}$ using error correcting codes. Technical Report TR10-137, revision #5, Electronic Colloquium on Computational Complexity, October 2010.

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

[NN94] Yurii Nesterov and Arkadii Nemirovskii. *Interior-Point Polynomial Algorithms in Convex Programming*, volume 13 of *SIAM Studies in Applied Mathematics*. SIAM, 1994.

[Sha92] Adi Shamir. $\mathrm{IP} = \mathrm{PSPACE}$. *Journal of the ACM*, 39(4):869–877, October 1992.

[She92] Alexander Shen. $\mathrm{IP} = \mathrm{PSPACE}$: Simplified proof. *Journal of the ACM*, 39(4):878–880, October 1992.

[WK06] Manfred K. Warmuth and Dima Kuzmin. Online variance minimization. In *Proceedings of the Nineteenth Annual Conference on Learning Theory*, volume 4005 of *Lecture Notes in Computer Science*, pages 514–528. Springer, June 2006.

[Wu10] Xiaodi Wu. Equilibrium value method for the proof of $\mathrm{QIP} = \mathrm{PSPACE}$. Available as arXiv.org e-Print 1004.0264v3 [quant-ph], September 2010.