One-Sided Error QMA with Shared EPR Pairs—A Simpler Proof

Extended Abstract

Attila Pereszlényi*

16th June, 2013

Abstract—We give a simpler proof of one of the results of Kobayashi, Le Gall, and Nishimura [10], which shows that any QMA protocol can be converted to a one-sided error protocol, in which Arthur and Merlin initially share a constant number of EPR pairs and then Merlin sends his proof to Arthur. Our protocol is similar but somewhat simpler than the original. Our main contribution is a simpler and more direct analysis of the soundness property that uses well-known results in quantum information such as properties of the trace distance and the fidelity, and the quantum de Finetti theorem.

1 Introduction

The class MA was defined by Babai [3] as the natural probabilistic extension of the class NP. In the definition of MA, the prover (Merlin) gives a polynomial length 'proof' to the verifier (Arthur), who then performs a polynomial-time randomized computation and has to decide if an input x is in a language L or not. The verifier is allowed to make some small error in his decision, but he must satisfy two conditions. If $x \in L$ then he has to accept a valid proof with high probability. The probability that he rejects such proof is called the *completeness* error. If $x \notin L$ then no matter what proof the verifier receives, he must reject with high probability. The probability that he accepts an invalid proof is called the *soundness* error.

One of the first questions one may ask is whether it is possible to get rid of one or both types of error. It is easy to see that forcing the soundness error to zero collapses MA to NP. So we can't eliminate the soundness error completely, but it is known that we can make it to be at most an inverse-exponential function of the input length, without reducing the expressive power of MA. On the other hand, it was shown by Zachos and Fürer [15] that having *perfect completeness*, also called as *one-sided error*, doesn't change the power of MA.[1]

Quantum Merlin-Arthur proof systems (and the class QMA) were introduced by Knill [9], Kitaev [8], and also by Watrous [14] as a natural extension of MA and NP to the quantum computational setting. We know from the early results that it can be made to have exponentially small two-sided error [8, 2, 11]. It also has natural complete problems, such as the 'k-local Hamiltonian' problem [8, 2], for $k \geq 2$ [7], which can be thought of as a quantum analogue of k-SAT.

Interestingly, we don't know if $\mathsf{QMA} \stackrel{?}{=} \mathsf{QMA}_1$, i.e., whether QMA can be made to have perfect completeness. It is a long-standing open problem which was already mentioned in an early survey by Aharonov and Naveh [2]. Besides its inherent importance, giving a positive answer to it would immediately imply that the QMA_1-complete problems are also complete for QMA. Most notable of these is the 'Quantum k-SAT' problem of Bravyi [4], for $k \geq 3$ [5], which is considered as a more natural quantum generalization of k-SAT than the k-local Hamiltonian problem. Unfortunately, all previous techniques used to show one-sided error properties of quantum interactive proof systems require adding extra messages to the protocol, so they can't be used directly in QMA. Aaronson [1] gave an evidence that shows that proving $\mathsf{QMA} = \mathsf{QMA}_1$ may be difficult. He proved that there exists a quantum oracle relative to which $\mathsf{QMA} \neq \mathsf{QMA}_1$. Another difficulty with QMA, compared to MA, is that in a QMA proof system the acceptance probability can be an arbitrary irrational number. However, if certain assumptions are made about the maximum acceptance probability then QMA can be made to have one-sided error [12]. Recently, Jordan et al. [6] showed that if Merlin's proof is classical then perfect completeness is achievable. In another variant of QMA, where we have multiple unentangled provers and exponentially

*Centre for Quantum Technologies, National University of Singapore, e-mail: attila.pereszlenyi@gmail.com.

[1] Similar properties also hold for interactive proof systems and quantum interactive proof systems.

or double-exponentially small gap, we also know that perfect completeness is achievable [13]. The most recent and strongest result towards proving the original QMA versus QMA_1 question is by Kobayashi et al. [10]. They showed that we can convert a QMA proof system to have one-sided error, if we allow the prover and the verifier of the resulting QMA_1 protocol to share a constant number of EPR pairs before the prover sends the proof to the verifier. The corresponding class is denoted by $\mathsf{QMA}_1^{\text{const-EPR}}$. With this notation, their result can be formalized as the following theorem.

Theorem 1 ([10])**.** $\mathsf{QMA} \subseteq \mathsf{QMA}_1^{\text{const-EPR}}$.

Since sharing an EPR pair can be done by the verifier preparing it and sending half of it to the prover, the above result implies that QMA is contained in the class of languages provable by one-sided error, two-message quantum interactive proof systems. This is a nontrivial upper bound.

1.1 Our Contribution The contribution of this paper is a conceptually simpler and more direct proof of Theorem 1, compared to the original one by Kobayashi et al. [10]. The algorithm of our verifier is also simpler, but the main difference is in the proof of its soundness. We believe that our proof helps to understand the result better and we think that it may be simplified further. We describe the main ideas behind our proof in the next section. We also point out the similarities and the differences between our proof and the original proof.

2 The Idea Behind Our Proof

The basic idea to achieve perfect completeness is very similar to Ref. [10]. For any input x, let us define $\mathbf{M}_x \stackrel{\text{def}}{=} \Pi_{\text{init}} \mathbf{V}_x^* \Pi_{\text{acc}} \mathbf{V}_x \Pi_{\text{init}}$, where Π_{init} is the projector that corresponds to projecting the private space of the verifier to the all zero vector, Π_{acc} is the projector that corresponds to acceptance, and $\mathbf{V}_x$ is the circuit of the verifier. Note that $0 \leq \mathbf{M}_x \leq \mathbb{1}$. As was observed in [11], the maximum acceptance probability of $\mathbf{V}_x$ is $\|\mathbf{M}_x\|_\infty$, or in other words, the maximum eigenvalue of $\mathbf{M}_x$. The completeness property implies that if $x \in L$ then $\|\mathbf{M}_x\|_\infty \geq 1/2$. Our first objective is to modify $\mathbf{M}_x$ such that its maximum eigenvalue is exactly $1/2$. We do this by using an auxiliary qubit (stored in register S) and defining

$$\mathbf{M}'_x \stackrel{\text{def}}{=} \mathbf{M}_x \otimes \left(|0\rangle\langle 0|_{\mathsf{S}} \, \mathbf{W}_q^* \, |1\rangle\langle 1|_{\mathsf{S}} \, \mathbf{W}_q \, |0\rangle\langle 0|_{\mathsf{S}} \right)$$

where $\mathbf{W}_q$ is a rotation about the $\hat{x}$ axes in the Bloch sphere by an angle of $2\arcsin\left(\sqrt{q}\right)$ and $q \stackrel{\text{def}}{=} \frac{1}{2p} \in \left[\frac{1}{2}, 1\right]$. It is easy to see that $\|\mathbf{M}'_x\|_\infty = 1/2$ and we can write $\mathbf{M}'_x$ as $\mathbf{M}'_x = \Delta\Pi\Delta$, where projectors Δ and Π are defined as $\Delta \stackrel{\text{def}}{=} \Pi_{\text{init}} \otimes |0\rangle\langle 0|$ and $\Pi \stackrel{\text{def}}{=} \mathbf{V}_x^* \Pi_{\text{acc}} \mathbf{V}_x \otimes \mathbf{W}_q^* \, |1\rangle\langle 1| \, \mathbf{W}_q$. Now, we construct a test that accepts with probability 1. Let the principal eigenvector of $\mathbf{M}'_x$ (that corresponds to eigenvalue $1/2$) be denoted by $|\omega\rangle \otimes \left|\bar{0}\right\rangle$. The test receives this eigenstate as the input, applies the unitary operator $\mathbb{1} - 2\Pi$, and performs a measurement defined by operators $\{\Delta, \mathbb{1} - \Delta\}$. If the state is projected to Δ the test rejects and otherwise it accepts. It is easy to see that with this input we never project to Δ.

However, a polynomial-time verifier may not be able to perform this test, because it is possible that $\mathbf{W}_q$ can't be expressed by a polynomial-size quantum circuit and the verifier may not even know the exact value of q. To overcome this difficulty, the verifier expects the prover to give several copies of the normalized Choi-Jamiołkowski representations of $\mathbf{W}_q^*$, besides $|\omega\rangle$. These can be used to perform $\mathbf{W}_q$ and $\mathbf{W}_q^*$. Since $\mathbf{W}_q$ is applied to $|0\rangle$, we can produce $\mathbf{W}_q \, |0\rangle$ by applying a suitable unitary on the Choi-Jamiołkowski representation. To perform $\mathbf{W}_q^*$ we use a procedure that is similar to teleportation, which we call post-selection. Unfortunately, post-selection fails with probability $1/2$, even with the honest prover, in which case we have to accept in order to maintain perfect completeness. This is the main idea to prove perfect completeness, and it is basically the same as in [10].

The harder part is to prove the soundness and this is where our proof differs from the one in [10]. Let us first give a high-level overview of the soundness proof of Kobayashi et al. [10]. The main idea in their proof is to perform a sequence of tests (i.e., quantum algorithms with measurements at the end), which together ensure that the registers that are supposed to contain the Choi-Jamiołkowski representations

of the desired operator, actually contain the Choi-Jamiołkowski representations of *some* operator. Then they show that doing the so-called 'Reflection Simulation Test', the one just described above, with these states in the registers, will cause rejection with some constant probability. The tests they use to ensure that the states are close to Choi-Jamiołkowski representations are the 'Distillation Procedure' (which is used to remove the entanglement between the register of the original proof and the registers of the Choi-Jamiołkowski representations), the 'Space Restriction Test' (which tests that the states are in a certain subspace), and the SWAP Test. In their analysis they also use the de Finetti theorem. We don't describe these tests here, as the interested reader can find them in [10]. We just list them in order to compare them to the tools we use.

Our main idea behind the soundness proof is conceptually different. We don't argue that the states are close to Choi-Jamiołkowski representations, but we analyze our version of the Reflection Simulation Test directly. As we described this test above, there are two measurements in it. The first measurement is in the post-selection and the second is given by $\{\Delta, \mathbb{1} - \Delta\}$. So, roughly speaking, we have to prove two things. First, we have to show that post-selection can't always fail, as otherwise we would end up always accepting without reaching the end of the procedure. In order to prove this, we only need two assumptions. The first assumption is that the state being measured in the post-selection is separable, which is guaranteed by the de Finetti theorem. The second assumption is that the state of some registers is close to being completely mixed, which is obviously true because these registers hold parts of EPR pairs.

The second part of the soundness proof is to show that conditioned on the post-selection being successful, we get a state that projects to Δ with constant probability. We first argue that the private space of the verifier projects to $|\bar{0}\rangle\langle\bar{0}|$. This follows from simple properties of the trace distance. We then show that the state of register S projects to $|0\rangle\langle 0|$. To prove this, we use the SWAP Test on the registers that are supposed to contain the Choi-Jamiołkowski representations. This ensures that the state of these registers are close to the same pure state. We also use a simplified version of the Space Restriction Test, which is not really a test but an application of a super-operator on the above mentioned registers. We can think of it as performing a projective measurement that corresponds to the Space Restriction Test and forgetting the outcome. Using the above tools, it will follow by direct calculation that the state of S projects to $|0\rangle\langle 0|$.

Note that we don't use the Distillation Procedure of [10] and we use a simpler form of the Space Restriction Test. Besides that, it's worth mentioning that the tools we use can be grouped into two sets based on whether we use them in the analysis of the first or the second measurement. For the analysis of the first measurement, we need that some state is close to being maximally mixed, while in the analysis of the second, we use the SWAP Test and the above mentioned super-operator. One exception is the de Finetti theorem, as we need that the states are separable in both parts. This property of the proof may be useful for simplifying it further, because for example, to omit the SWAP Test, one would only need to re-prove that the state of S projects to $|0\rangle\langle 0|$ in the last measurement.

References

[1] S. Aaronson. On perfect completeness for QMA. *Quantum Information and Computation*, 9(1):81–89, Jan. 2009.

[2] D. Aharonov and T. Naveh. Quantum NP - a survey. Oct. 2002.

[3] L. Babai. Trading group theory for randomness. In *Proceedings of the 17th annual ACM Symposium on Theory of Computing*, STOC '85, pages 421–429, 1985.

[4] S. Bravyi. Efficient algorithm for a quantum analogue of 2-SAT. Feb. 2006.

[5] D. Gosset and D. Nagaj. Quantum 3-SAT is QMA_1-complete. Feb. 2013.

[6] S. P. Jordan, H. Kobayashi, D. Nagaj, and H. Nishimura. Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. *Quantum Information and Computation*, 12(5–6):461–471, May 2012.

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

[8] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, 2002.

[9] E. Knill. Quantum randomness and nondeterminism. Oct. 1996.

[10] 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*, ITCS '13, pages 329–352, New York, NY, USA, 2013. ACM.

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

[12] D. Nagaj, P. Wocjan, and Y. Zhang. Fast amplification of QMA. *Quantum Information and Computation*, 9(11):1053–1068, Nov. 2009.

[13] A. Pereszlényi. Multi-prover quantum Merlin-Arthur proof systems with small gap. May 2012.

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

[15] S. Zachos and M. Fürer. Probabalistic quantifiers vs. distrustful adversaries. In *Proceedings of the Seventh Conference on Foundations of Software Technology and Theoretical Computer Science*, volume 287 of *Lecture Notes in Computer Science*, pages 443–455, London, UK, 1987. Springer-Verlag.