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

Attila Pereszlényi[1] †

[1] *Centre for Quantum Technologies, National University of Singapore*

Abstract. We give a simpler proof of one of the results of Kobayashi, Le Gall, and Nishimura [8], 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.

Keywords: computational complexity, quantum Merlin-Arthur proof systems, one-sided error

1 Introduction

The class MA was defined by Babai [2] as the natural probabilistic extension of 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 and otherwise he has to reject with high probability. The probability that he rejects a valid proof is called the *completeness* error and 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. On the other hand, it is known that having *perfect completeness*, also called as *one-sided error*, doesn't change the power of MA [11].

Quantum Merlin-Arthur proof systems (and the class QMA) were introduced by Kitaev [7] as the natural quantum extension of MA and NP. QMA has natural complete problems, such as the 'k-local Hamiltonian' problem [7], for $k \geq 2$ [6], which can be thought of as a quantum analogue of k-SAT. Interestingly, we don't know if $\mathsf{QMA} \stackrel{?}{=} \mathsf{QMA}_1$ and it is a long-standing open problem. Besides its inherent importance, giving a positive answer to it would imply that the QMA_1-complete problems are also complete for QMA. Most notable of these is the 'Quantum k-SAT' problem [3], for $k \geq 3$ [4], 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. Moreover, Aaronson [1] proved that there exists a quantum oracle relative to which $\mathsf{QMA} \neq \mathsf{QMA}_1$. Another difficulty with QMA is that 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 [9]. There are other variants of QMA where we also know that perfect completeness is achievable [5, 10]. The most recent and strongest result towards proving the QMA vs. QMA_1 question is by Kobayashi et al. [8]. 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 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 ([8]) $\mathsf{QMA} \subseteq \mathsf{QMA}_1^{\text{const-EPR}}$.

The above result implies that $\mathsf{QMA} \subseteq \mathsf{QIP}_1(2)$.

Our contribution is a conceptually simpler and more direct proof of Theorem 1, compared to the original one in Ref. [8]. 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.

2 The Idea Behind Our Proof

The basic idea to achieve perfect completeness is very similar to Ref. [8]. 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 $0 \leq \mathbf{M}_x \leq \mathbb{1}$. It is easy to see that the maximum acceptance probability of $\mathbf{V}_x$ is $\|\mathbf{M}_x\|_\infty$. The completeness property implies that if $x \in L$ then $\|\mathbf{M}_x\|_\infty \geq 1/2$. First, we 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 $\mathbf{M}'_x \stackrel{\text{def}}{=} \mathbf{M}_x \otimes \left(|0\rangle\langle 0|_{\mathcal{S}} \mathbf{W}_q^* |1\rangle\langle 1|_{\mathcal{S}} \mathbf{W}_q |0\rangle\langle 0|_{\mathcal{S}} \right)$, 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 $\mathbf{M}'_x$ be denoted by

*Extended abstract. The full version is available at arXiv:1306.5406.

† attila.pereszlenyi@gmail.com

$|\omega\rangle \otimes |\bar{0}\rangle$. 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 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, 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 C.-J. 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, with the honest prover, in which case we accept in order to maintain perfect completeness. This is the main idea to prove completeness and it is basically the same as in [8].

The harder part is to prove the soundness and this is where our proof differs from the one in [8]. Let us first give a high-level overview of the soundness proof of Kobayashi et al. [8]. 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 C.-J. representations of the desired operator, actually contain the C.-J. 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 C.-J. representations are the 'Distillation Procedure' (which is used to remove the entanglement between the register of the original proof and the registers of the C.-J. 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 [8]. 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 C.-J. 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 Π_{init}. 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 C.-J. 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 follows by direct calculation that the state of S projects to $|0\rangle\langle 0|$.

Note that we don't use the Distillation Procedure of [8] 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. 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 Info. Comput.*, 9(1):81–89, 2009, arXiv:0806.0450.

[2] L. Babai. Trading group theory for randomness. In *Proc. 17th ACM STOC*, pages 421–429, 1985.

[3] S. Bravyi. Efficient algorithm for a quantum analogue of 2-SAT. 2006, arXiv:quant-ph/0602108.

[4] D. Gosset and D. Nagaj. Quantum 3-SAT is QMA_1-complete. 2013, arXiv:1302.0290.

[5] S. P. Jordan, H. Kobayashi, D. Nagaj, and H. Nishimura. Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. *Quantum Info. Comput.*, 12(5–6):461–471, 2012, arXiv:1111.5306.

[6] J. Kempe, A. Kitaev, and O. Regev. The complexity of the local hamiltonian problem. *SIAM J. Comput.*, 35(5):1070–1097, 2006, arXiv:quant-ph/0406180.

[7] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation.* AMS, 2002.

[8] H. Kobayashi, F. Le Gall, and H. Nishimura. Stronger methods of making quantum interactive proofs perfectly complete. In *Proc. 4th ITCS*, pages 329–352. ACM, 2013, arXiv:1210.1290.

[9] D. Nagaj, P. Wocjan, and Y. Zhang. Fast amplification of QMA. *Quantum Info. Comput.*, 9(11):1053–1068, 2009, arXiv:0904.1549.

[10] A. Pereszlényi. Multi-prover quantum Merlin-Arthur proof systems with small gap. 2012, arXiv:1205.2761.

[11] S. Zachos and M. Fürer. Probabalistic quantifiers vs. distrustful adversaries. In *Proc. 7th FSTTCS*, volume 287 of *LNCS*, pages 443–455, 1987.