QCMA with one-sided error equals QCMA with two-sided error

Stephen P. Jordan*† and Daniel Nagaj ‡

Abstract

QCMA is the set of decision problems such that if the answer is yes, there exists a classical bit string, or proof, that can be efficiently verified by a quantum computer. The verifier is allowed a small probability of rejecting a valid proof or accepting invalid proofs. We show that for all problems in QCMA, the acceptance probability for valid proofs can be amplified to one, thus QCMA with one-sided error is equal to QCMA. This is a quantum analog to the result of Zachos and Fürer, that the classical complexity class MA with one sided error is the same as MA with two-sided error. Because a quantum oracle separating QCMA and QCMA with one sided error is known [1], our result provides an example of a quantumly non-relativizing proof.

1 Introduction

QCMA was first defined in [3] as the class of decision problems whose solutions (given as classical bit strings) can be efficiently verified by a quantum computer. The letters MA stand for Merlin-Arthur, as the complexity class is motivated by the following protocol. A bit string s (the purported proof) is provided by an computationally unbounded but untrustworthy prover (Merlin) to a verifier with only polynomial resources (Arthur). The Q indicates that Arthur's verification procedure is polynomial time quantum computation, and the C indicates that the proof s is a *classical* bit string. If the verifier is a classical polynomial-time computer, then the resulting class is called MA [5]. If the verifier and proof are both quantum, that is, s is an arbitrary quantum state, the resulting complexity class is called QMA [11]. We give a more precise definition of QCMA as follows, where $|x|$ denotes the length of bit string x.

Definition 1 (QCMA) *A language $L \subseteq \{0,1\}^*$ is in QCMA if there is an efficient quantum verifier (a quantum computer of* $\mathrm{poly}(|x|)$ *time and space resources), and a fixed polynomial m such that*

1. *if $x \in L$ then $\exists s \in \{0,1\}^{m(|x|)}$ such that the verifier accepts s with probability at least 2/3*
2. *if $x \notin L$ then $\forall s \in \{0,1\}^{m(|x|)}$ the verifier accepts s with probability at most 1/3.*

The constants 2/3 and 1/3 appearing in the definitions of QCMA and QMA are called the completeness and soundness probabilities, respectively. The completeness probability can be replaced by any constant strictly between 1/2 and 1 without changing the resulting complexity class. Arthur can amplify the completeness probability in QCMA by testing s several times and taking the majority vote among the outputs of the verifier circuit. Amplifying the completeness probability in QMA is more nontrivial, but protocols to do so have been discovered [11, 12, 13]. QMA and QCMA arise widely in complexity theory. In particular, each has natural complete problems [9, 15].

*National Institute of Standards and Technology, Gaithersburg, MD, USA. stephen.jordan@nist.gov

†Much of this work was done while SJ was at the Institute for Quantum Information at Caltech.

‡Research Center for Quantum Information, Slovak Academy of Sciences, Dúbravská cesta 9, 842 15 Bratislava, Slovakia. daniel.nagaj@savba.sk

Whether the completeness probabilities in QCMA and QMA can be replaced by one without changing these complexity classes is an open question. Bravyi first defined QMA with perfect completeness in [7] and named it QMA_1. In the same paper, Bravyi showed that deciding whether a Hamiltonian is frustration free is QMA_1-complete. In [1], Aaronson constructed a simple quantum oracle relative to which $\mathsf{QMA}_1 \neq \mathsf{QMA}$. Thus, if a proof of $\mathsf{QMA}_1 = \mathsf{QMA}$ exists it will have to be quantumly nonrelativizing, and this eliminates many standard proof techniques.

We here define QCMA_1 as follows.

Definition 2 (QCMA_1) *A language $L \subseteq \{0,1\}^*$ is in QCMA_1 if there is an efficient quantum verifier (a quantum computer of $\mathrm{poly}(|x|)$ time and space resources), and a fixed polynomial m such that*

1. *if $x \in L$, $\exists s \in \{0,1\}^{m(|x|)}$ such that the verifier accepts s with probability 1*
2. *if $x \notin L$ then $\forall s \in \{0,1\}^{m(|x|)}$, the verifier accepts s with probability at most 1/3.*

We further specify that the quantum verifier use only gates in which each matrix element is an algebraic number of bounded degree specifiable with polynomially many bits.

Our main result is

Theorem 1 *$\mathsf{QCMA} = \mathsf{QCMA}_1$.*

This is a quantum analog to the result of Zachos and Fürer, showing that MA is equal to MA with one-sided error[16]. The quantum oracle used in [1] to separate QMA_1 from QMA also separates QCMA_1 from QCMA. Our proof of theorem 1 is quantumly nonrelativizing and thereby evades this obstacle. To our knowledge, this is the first example of a quantumly nonrelativizing proof. We hope it may provide guidance on approaching the longstanding QMA vs. QMA_1 problem.

Note that our definition of QCMA_1 specifies a gate set, whereas the definition of QCMA does not. In the definition of QCMA it is implicit that the quantum circuits are constructed using a universal gate set, that is, a set of local unitaries that generate a dense subgroup of the full unitary group (modulo phase). The Solovay-Kitaev theorem guarantees that any universal gate set can efficiently approximate any other [10]. Thus, the complexity class QCMA is independent of which particular universal gate set is chosen. However, as it refers to approximability, the Solovay-Kitaev theorem does imply gate-set independence for zero or one-sided error complexity classes such as QCMA_1. It does not seem reasonable to define QCMA_1 using entirely arbitrary 1- and 2-qubit gates, as these could require infinitely many bits to specify. Instead, we follow [7] and allow all gates with algebraic matrix elements of bounded degree specifiable with polynomially many bits.

2 Proof Overview

To prove theorem 1, it suffices to show that $\mathsf{QCMA} \subseteq \mathsf{QCMA}_1$, since $\mathsf{QCMA}_1 \subseteq \mathsf{QCMA}$ is immediate. Given a verifier for a language $L \in \mathsf{QCMA}$ with proof size m we explicitly construct a modified verifier with proof size $m' = \mathrm{poly}(m)$ satisfying conditions 1 and 2 of definition 2.

In the case of 'yes' instances, the accepted proof s' consists of the original proof s concatenated with the original acceptance probability $p_{\mathrm{acc}} \in [2/3, 1)$ encoded as a bit string. Given p_{acc}, the QCMA_1 verifier can amplify acceptance probability to one using amplitude amplification, which is a generalization of Grover's search algorithm [8]. (In [6] a similar boosting of BQP to zero error was previously discussed. Note however that our presentation is self-contained; we do not assume familiarity with [6].)

The above scheme requires that the acceptance probability of the original QCMA verifier be exactly specifiable using polynomially many bits. We show that it can be, by constructing a universal gate set $\mathcal{G}$ in which all the matrix elements have common denominator five. In this case, the acceptance probability can be specified with polynomially many digits in base five. Since the complexity class QCMA is independent of which universal gate set is used by the verifier, we may assume without loss of generality that the original QCMA verifier uses gates from $\mathcal{G}$. The QCMA_1 verifier that we construct uses a different gate set. Specifically,

let $\mathcal{A}(d,b)$ be the set of one-qubit and two-qubit gates in which every matrix element is an algebraic number of degree at most d specifiable with at most b bits. The QCMA_1 verifier that we construct uses gates from $\mathcal{A}(2,6T)$, where T is the number of $\mathcal{G}$-gates used by the original QCMA verifier.

3 Universal Gates with Rational Amplitudes

Let

$$\mathcal{G} = \left\{ A = \begin{bmatrix} \frac{4}{5} & -\frac{3}{5} \\ \frac{3}{5} & \frac{4}{5} \end{bmatrix},\ B = \begin{bmatrix} \frac{4}{5} & i\frac{3}{5} \\ i\frac{3}{5} & \frac{4}{5} \end{bmatrix},\ \text{CNOT} \right\}. \tag{1}$$

In this section we show that $\mathcal{G}$ is a universal gate set. To do this, we first show that the single qubit gates $\{A, B\}$ generate a dense subgroup of $SU(2)$ modulo phase. Thus, by [10], for any $U \in SU(2)$, one can efficiently find a product $\tilde{U}$ of polylog(ϵ) A gates and B gates such that $\|\tilde{U} - e^{i\theta}U\| \leq \epsilon$ for some $\theta \in [0, 2\pi)$. The gate set $\mathcal{G}$ is thus universal, because the CNOT gate together with the set of all single-qubit gates is universal in the sense that any unitary on n qubits can be constructed as a product of gates from this set [14]. We use techniques from [2], which showed that quantum Turing machines using only rational transition amplitudes can perform universal quantum computation.

To show that the gate set $\{A, B\}$ generates a dense subgroup of $SU(2)$, modulo phase, we use the well known surjective homomorphism $\phi : SU(2) \to SO(3)$ whose kernel is $\{\pm\mathbb{1}\}$ (*cf.* [4]). A general element of $SU(2)$ can be written as

$$\cos\left(\frac{\theta}{2}\right)\mathbb{1} + i\sin\left(\frac{\theta}{2}\right)\left[v_x\hat{\sigma}_x + v_y\hat{\sigma}_y + v_z\hat{\sigma}_z\right], \tag{2}$$

where $\hat{\sigma}_x, \hat{\sigma}_y, \hat{\sigma}_z$ are the Pauli matrices and v_x, v_y, v_z are real numbers satisfying $v_x^2 + v_y^2 + v_z^2 = 1$. The homomorphism ϕ maps this element to the rotation by angle θ about the axis $\vec{v} = (v_x, v_y, v_z)$. Thus $\phi(A)$ is a rotation by angle $\theta = 2\cos^{-1}\left(\frac{4}{5}\right)$ about the y axis, while $\phi(B)$ is a rotation by the same angle θ about the x axis. As discussed in [2], the only complex roots of unity with rational real and imaginary parts are ± 1 and $\pm i$. We have $e^{i\theta} = \frac{14}{5} + i\frac{48}{5}$, meaning that θ must be an irrational multiple of π. Therefore, any rotation around the x axis can be approximated to any precision by a sufficiently high power of B, and any rotation around the y axis can be approximated to any precision by a sufficiently high power of A. By the usual Euler angle construction, any element of $SO(3)$ can thus be approximated to any precision by some product of $\phi(A)$ and $\phi(B)$. That is, $\phi(A)$ and $\phi(B)$ generate a dense subgroup of $SO(3)$. Therefore, modulo phase, A and B generate a dense subgroup of $SU(2)$, and the gate set $\mathcal{G}$, which has only rational entries, is universal for quantum computation.

4 Perfect Completeness

The QCMA verifier's circuit V takes input $|s0\ldots0\rangle$, where $s \in \{0,1\}^m$ is the purported proof, and $0\ldots0$ are r ancilla qubits, the last of which is declared to be the output qubit. Here r and m are polynomial in $|x|$. If the output qubit is found in the state $|1\rangle$ at the end of the computation, the verifier declares acceptance. The acceptance probability for $|s\rangle$ is then[1]

$$p_{\text{acc}} = \sum_{g\in\{0,1\}^{r-1}} \left|\langle sg1|\, V\, |s0\ldots0\rangle\right|^2. \tag{3}$$

Using the gate set $\mathcal{G}$ ensures that each amplitude $\langle sg1|\, V\, |s0\ldots0\rangle$ is a rational number whose expansion in base five has at most T digits, where T is the number of gates in V. Hence, p_{acc} is a rational number whose expansion in base 5 has at most $2T$ digits. Each base five digit can be specified using three bits. We correspondingly define s' to be the concatenation of s with the string of $6T$ bits encoding p_{acc}.

[1] We follow a standard quantum computation convention, in which the input is left untouched, and the "garbage" string g is stored only in the ancilla register. It is always straightforward put a quantum circuit into this form [14].

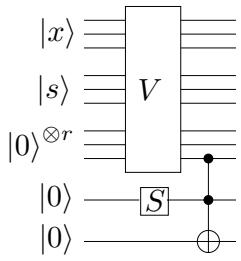

Figure 1: With the S gate defined as in (4), this modification brings acceptance probability to exactly 1/4.

Given s', a polynomial time classical computer Arthur can construct a quantum circuit V_1 which accepts s with probability one, as follows. If p_{acc} were 1/4 then a single iteration of Grover's algorithm would amplify the acceptance probability to exactly one. However, what Arthur receives from Merlin is a proof whose acceptance probability is a rational number $1 \leq p_{\text{acc}} \leq \frac{2}{3}$. To bring it down to $\frac{1}{4}$, we construct a modifier operation. Consider the rotation

$$S = \begin{bmatrix} \sqrt{1-p_s} & \sqrt{p_s} \\ -\sqrt{p_s} & \sqrt{1-p_s} \end{bmatrix} \tag{4}$$

with

$$p_s = \frac{1}{4p_{\text{acc}}}. \tag{5}$$

Note that $S \in \mathcal{A}(2, 6T)$.

Let us now modify our circuit V as depicted in Figure 1. We first add an extra ancilla qubit and rotate it with S. This qubit should then be in the state $\sqrt{1-p_s}\,|0\rangle + \sqrt{p_s}\,|1\rangle$. Second, we add one more ancilla, and flip it only if both the output of V and the rotated qubit are in the state $|1\rangle$. The value of this last qubit now decides the acceptance for the modified circuit V'. Thus, if V accepts with probability p_{acc} then V' accepts with probability exactly $p_{\text{acc}}p_s = 1/4$.

Following [6], we now use Grover's algorithm to amplify the acceptance probability in the following way. Let $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$ be projectors acting on the acceptance qubit (that is, the last ancilla qubit). Let R_0 be the reflection about the rejected subspace.

$$R_0 = \mathbb{1} - 2P_1 \tag{6}$$

R_0 can be constructed as a very simple quantum circuit, namely a σ_z gate on the output qubit. Similarly, let R_1 be the reflection about the input state.

$$R_1 = 2\,|s0\ldots0\rangle\langle s0\ldots0| - \mathbb{1} \tag{7}$$

R_1 may be constructed efficiently from Toffoli and σ_z gates using standard techniques of reversible computation[14]. Let

$$R_\varphi = V' R_1 (V')^\dagger. \tag{8}$$

One sees that $R_\varphi = 2\,|\varphi\rangle\langle\varphi| - \mathbb{1}$ where $|\varphi\rangle = V'\,|s0\ldots0\rangle$. An efficient circuit for R_φ may be constructed by concatenating the circuit for $(V')^\dagger$, followed by the circuit for R_1, followed by the circuit for V'. The circuit for $(V')^\dagger$ consists of the adjoints of the gates of the circuit for V' in reverse order.

The angle between $|\varphi\rangle$ and the unnormalized state $P_1\,|\varphi\rangle$ is $\pi/6$ since $\langle\varphi|\,P_1\,|\varphi\rangle = \frac{1}{4}$. Hence, as shown in Figure 2, the product of the two reflections $R_\varphi R_0$ acts on the span of $P_1\,|\varphi\rangle$ and $P_0\,|\varphi\rangle$ as a rotation by $\frac{\pi}{3}$, exactly the angle separating the state $|\varphi\rangle$ from the perfectly accepted state $P_1\,|\varphi\rangle$. Hence, when Arthur obtains a valid proof s' consisting of s and its acceptance probability p_{acc} for the circuit V, he applies the quantum circuit $V_1 = R_\varphi R_0 V'$ to the state $|s0\ldots0\rangle$ (with $r+2$ ancilla qubits) and obtain a state in which

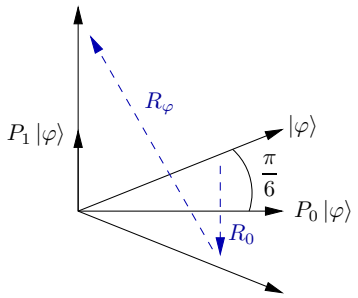

Figure 2: A single iteration of Grover's algorithm on a state $|\varphi\rangle$ that has overlap $\frac{1}{2}$ with the desired state results in obtaining the desired state exactly.

the acceptance qubit is $|1\rangle$ with probability exactly one. Thus, Merlin can make the verifier accept valid proofs with certainty. All that remains is to show that invalid proofs are accepted with probability no more than $1/3$, which we do in the following section.

Not that in constructing R_1 and V' we have used Toffoli (*i.e.* doubly-controlled-NOT) gates, which act on three qubits. We could of course include these in the gate set used to define QCMA_1. However, this is unnecessary because, as illustrated in Figure 4.8 of [14], the Toffoli gate may be constructed exactly as a product of five two-qubit gates with algebraic matrix elements of degree at most two.

5 Soundness

If $x \in L$, Merlin can cause Arthur to accept with probability one by transmitting polynomially many classical bits, as shown in the previous section. By definition, if $x \notin L$ instance, there is no proof s which causes the verifier circuit to accept with probability more than $\frac{1}{3}$. The procedure described in the previous section, while boosting the acceptance probability to one for $x \in L$, also boosts the acceptance probability for $x \notin L$. We now show that this boosting is sufficiently small that by simply performing the test five times and accepting only if acceptance bit was measured to be in the $|1\rangle$ state every time, Arthur can bring the acceptance probability of all claimed proofs for $x \notin L$ back below $\frac{1}{3}$.

Let p_{claim} be the acceptance probability claimed by Merlin. Examination of the procedure in the preceding section shows that the QCMA_1 verifier accepts with probability

$$p'_{\text{acc}} = \sin^2\left(3\sin^{-1}\left(\sqrt{\frac{p_{\text{acc}}}{4p_{\text{claim}}}}\right)\right). \tag{9}$$

For $x \notin L$, $0 \leq p_{\text{acc}} \leq 1/3$. Furthermore, Arthur always rejects unless $2/3 \leq p_{\text{claim}} \leq 1$. These restrictions imply that $0 \leq \sqrt{\frac{p_{\text{acc}}}{4p_{\text{claim}}}} \leq \frac{1}{\sqrt{8}}$. Within this range, the function $\sin^2\left(3\sin^{-1}\theta\right)$ is monotonically increasing. Thus for $x \notin L$, $p'_{\text{acc}} \leq \sin^2\left(3\sin^{-1}\left(1/\sqrt{8}\right)\right) \simeq 0.78$. By demanding five successive acceptances by the quantum circuit, Arthur ensures that he accepts false proofs with probability at most $\sin^{10}\left(3\sin^{-1}\theta\right)$, which is less than $1/3$.

6 Acknowledgements

We thank Jake Taylor, Michele Mosca, and Pawel Wocjan for useful discussions. DN gratefully acknowledges support from the Slovak Research and Development Agency under the contract No. LPP-0430-09, from the project meta-QUTE ITMS 26240120022 and European project Q-ESSENCE. Much of this work was performed while SJ was at the Institute for Quantum Computation at Caltech. He gratefully acknowledges

the support he received from the Sherman Fairchild Foundation and NSF grant PHY-0803371 and thanks the Slovak Academy of Sciences for hospitality.

References

[1] Scott Aaronson. On perfect completeness for QMA. *Quantum Information and Computation*, 9:81–89, 2009. arXiv:0806.0450.

[2] Leonard M. Adleman, Jonathan Demarrais, and Ming-Deh A. Huang. Quantum computability. *SIAM Journal on Computing*, 26(5):1524–1540, 1997.

[3] Dorit Aharonov and Tomer Naveh. Quantum NP - a survey. *arXiv:quant-ph/0210077*, 2002.

[4] Michael Artin. *Algebra*, chapter 8, page 276. Prentice Hall, 1991.

[5] László Babai. Trading group theory for randomness. In *Proceedings of the seventeenth annual ACM symposium on theory of computing (STOC)*, pages 421–429, 1985.

[6] Gilles Brassard, Peter Høyer, Michele Mosca, and Alain Tapp. Quantum amplitude amplification and estimation. In Samuel J. Lomonaco Jr. and Howard E. Brandt, editors, *Quantum Computation and Quantum Information: A Millennium Volume*, volume 305 of *AMS Contemporary Mathematics Series*. American Mathematical Society, 2002.

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

[8] Lov K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 79(2):325–328, 1997. arXiv:quant-ph/9605043.

[9] Julia Kempe, Alexei Kitaev, and Oded Regev. The complexity of the local Hamiltonian problem. *SIAM Journal of Computing*, 35(5):1070–1097, 2006. arXiv:quant-ph/0406180.

[10] A. Y. Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, 1997.

[11] A. Yu. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002.

[12] Chris Marriott and John Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005. arXiv:cs/0506068.

[13] Daniel Nagaj, Pawel Wocjan, and Yong Zhang. Fast amplification of QMA. *Quantum Information and Computation*, 9(11/12):1053–1068, 2009. arXiv:0904.1549.

[14] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 2000.

[15] Pawel Wocjan, Dominic Janzing, and Thomas Beth. Two QCMA-complete problems. *Quantum Information and Computation*, 3(6):635–643, 2003. arXiv:quant-ph/0305090.

[16] S. Zachos and M. Fürer. Probabilistic quantifiers vs. distrustful adversaries. In *Proceedings of FST-TCS*, volume 287 of *Lecture Notes in Computer Science*, pages 443–455. Springer-Verlag, 1987.