Quantum Information and Computation, Vol. 12, No. 5&6 (2012) 0461–0471

ACHIEVING PERFECT COMPLETENESS IN CLASSICAL-WITNESS QUANTUM MERLIN-ARTHUR PROOF SYSTEMS

STEPHEN P. JORDAN[a]
Applied and Computational Mathematics Division
National Institute of Standards and Technology, Gaithersburg, MD, USA.

HIROTADA KOBAYASHI
Principles of Informatics Research Division
National Institute of Informatics, Tokyo, Japan.

DANIEL NAGAJ
Research Center for Quantum Information
Institute of Physics, Slovak Academy of Sciences, Bratislava, Slovakia.

HARUMICHI NISHIMURA
Department of Mathematics and Information Sciences
Graduate School of Science, Osaka Prefecture University, Sakai, Osaka, Japan.

Received November 23, 2011
Revised February 3, 2012

This paper proves that classical-witness quantum Merlin-Arthur proof systems can achieve perfect completeness. That is, QCMA = 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 is quantumly nonrelativizing, and uses a simple but novel quantum technique that *additively* adjusts the success probability, which may be of independent interest.

Keywords: quantum Merlin-Arthur proof systems, perfect completeness
Communicated by: R Jozsa & M Mosca

1 Introduction

QCMA (also called MQA [1, 2]) was first formally[b] defined by Aharonov and Naveh [4] 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 w (the purported witness) is provided by a computationally unbounded but untrustworthy prover (Merlin) to a verifier with only polynomial resources (Arthur). The verification procedure of the verifier is a polynomial time *quantum* computation while the witness w is a *classical* bit string. If the verifier is a polynomial-time classical computer, then the resulting class is called MA [5, 6]. If the

[a]Part of this work was done while at the Institute for Quantum Information, California Institute of Technology, Pasadena, CA.
[b]The general notion of nondeterminism in quantum computation originates much earlier due to Knill [3].

verifier and witness are both quantum, that is, w is an arbitrary quantum state, the resulting complexity class is called QMA [7] (originally called BQNP [8, 9]).

The standard way of defining these complexity classes allows two-sided bounded error: Arthur may wrongly reject each yes-instance with small probability (completeness error), and may also wrongly accept each no-instance with small probability (soundness error). If Arthur never wrongly rejects yes-instances, the system is said to have *perfect completeness*. The versions of QMA, QCMA, and MA with perfect completeness are denoted QMA_1, QCMA_1, and MA_1, respectively.

One of the important open problems in quantum Merlin-Arthur proofs (both in the QCMA case and in the QMA case) is whether the class defined with two-sided error equals that with perfect completeness. A proof that $\mathrm{QMA} = \mathrm{QMA}_1$ would be particularly interesting, as the problem of deciding whether a Hamiltonian is frustrated is QMA_1-complete [10]. Classically, it is known that $\mathrm{MA} = \mathrm{MA}_1$ due to Zachos and Fürer [11] (Goldreich and Zuckerman [12] provided an alternative proof of this). More generally, it is known that perfect completeness is achievable in various models of quantum and classical interactive proof systems [11, 13, 14, 15, 16, 17, 18]. In contrast, Aaronson [19] presented a *quantum* oracle relative to which QMA_1 is a proper subclass of QMA. This implies that any proof of $\mathrm{QMA} = \mathrm{QMA}_1$ must be quantumly nonrelativizing. Aaronson's oracle also separates QCMA from QCMA_1 since in fact he showed a quantum oracle relative to which BQP is not contained in the exponential-time analogue of QMA_1. He suggested that the result (and the proof) in Ref. [19] implies that any proof of $\mathrm{QMA} = \mathrm{QMA}_1$ (and also $\mathrm{QCMA} = \mathrm{QCMA}_1$) requires some technique of explicitly representing (probability) amplitudes that appear in quantum states or evolutions.

This paper shows that demanding perfect completeness does *not* weaken the power of QCMA proof systems under a reasonable assumption on the gate set. Specifically, assuming that Hadamard transformations and all classical reversible transformations can be exactly implemented, $\mathrm{QCMA} = \mathrm{QCMA}_1$. To the best of our knowledge, 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. [19]). Our proof of $\mathrm{QCMA} = \mathrm{QCMA}_1$ is nonrelativizing since our technique also utilizes an explicit representation of amplitudes. This suggests that the oracle separation of Ref. [19] may not be an insurmountable barrier to proving $\mathrm{QMA} = \mathrm{QMA}_1$. We hope that 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 [20] can be verified with perfect completeness.

Our basic strategy to prove $\mathrm{QCMA} = \mathrm{QCMA}_1$ 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 [21, 22] or Watrous's quantum rewinding [23]. 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 [24, 25]. 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 Watrous's 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 [18]. 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 of our knowledge, no such "additive" method of amplitude adjustment has appeared in the literature previously, and we believe it may have other applications in quantum complexity theory.

2 Preliminaries

We assume the reader is familiar with the quantum formalism, in particular the quantum circuit model (see Refs. [26, 9], for instance). Throughout this paper, let $\mathbb{N}$ and $\mathbb{Z}^+$ denote the sets of positive and nonnegative integers, respectively. A function $f\colon \mathbb{Z}^+ \to \mathbb{N}$ is *polynomially bounded* if there exists a polynomial-time deterministic Turing machine that outputs $1^{f(n)}$ on input 1^n. A function $f\colon \mathbb{Z}^+ \to [0,1]$ is *negligible* if, for every polynomially bounded function $g\colon \mathbb{Z}^+ \to \mathbb{N}$, it holds that $f(n) < 1/g(n)$ for all but finitely many values of n.

For a quantum register R, let $|0\rangle_{\mathsf{R}}$ denote the state in which all the qubits in R are in state $|0\rangle$. In this paper, all Hilbert spaces have dimension a power of two.

Polynomial-Time Uniformly Generated Families of Quantum Circuits Following conventions, we define quantum Merlin-Arthur proof systems in terms of quantum circuits. In particular, we use the following notion of polynomial-time uniformly generated families of quantum circuits.

A family $\{Q_x\}$ of quantum circuits is *polynomial-time uniformly generated* if there exists a deterministic procedure that, on every input x, outputs a description of Q_x and runs in time polynomial in $|x|$. It is assumed that the circuits in such a family are composed of gates in some reasonable, universal, finite set of quantum gates. Furthermore, it is assumed that the number of gates in any circuit is not more than the length of the description of that circuit. Therefore Q_x must have size polynomial in $|x|$. For convenience, we may identify a circuit Q_x with the unitary operator it induces.

Throughout this paper, we assume a gate set with which the Hadamard and any classical reversible transformations can be exactly implemented. Note that this assumption is satisfied by many standard gate sets such as the Shor basis [27] consisting of the Hadamard, controlled-i-phase-shift, and Toffoli gates, and the one consisting of the Hadamard and Toffoli gates [24, 25]. Hence we believe that our condition is reasonable and not restrictive. For concreteness, we may assume the specific gate set {Hadamard, Toffoli, NOT} for both the original QCMA verifer and our corresponding QCMA_1 verifier. Note that, although {Hadamard, Toffoli} is computationally universal [24, 25] given a supply of both $|0\rangle$ and $|1\rangle$ ancilla qubits, we include the NOT gate because we assume the verifier receives all qubits initialized to $|0\rangle$. The witness string w is hardcoded into the verifier circuit $V_{x,w}$ by initial NOT gates acting on each witness bit whose value should be 1.

Since non-unitary and unitary quantum circuits are equivalent in computational power [28], it is sufficient to treat only unitary quantum circuits, which justifies the above definition. However, we describe our verification procedure using intermediate projective measurements in the computational basis and unitary operations conditioned on the outcome of the measurements. If we wished, we could defer all of the measurements of the verification procedure to the end of the computation, along the lines described on page 186 of Ref. [26].

More specifically, one sees from Figure 1 in the next section that our verification procedure involves Boolean-outcome measurements at Steps 1, 3.1, and 3.5. Let b_1, $b_{3.1}$, and $b_{3.5}$ denote the outcomes of these measurements. Final acceptance occurs if

$$\neg b_1 \wedge (b_{3.1} \vee b_{3.5}) \tag{1}$$

evaluates to true. This can be determined unitarily using Toffoli gates, as they can perform universal classical computation. One may worry that exact unitary implementation of the conditional operations would require the addition of conditional-Hadamard to our gate set. However, the operations in Steps 2 and 3 which, for conceptual clarity, we describe as being performed only under certain measurement outcomes, can in fact be performed unconditionally without affecting final acceptance. By construction, the formula (1) simply ignores the outcomes of these steps in the cases that they are irrelevant.

Classical-Witness Quantum Merlin-Arthur Proof Systems This paper discusses the power of quantum Merlin-Arthur proof systems where Merlin sends a classical witness to Arthur, which we call *QCMA proof systems*.

Formally, the class $\mathrm{QCMA}(c,s)$ of problems having such systems with completeness c and soundness s is defined as follows. For generality, we use promise problems [29] rather than languages when defining complexity classes.

Definition 1 *Given functions $c,s\colon \mathbb{Z}^+ \to [0,1]$, a promise problem $A=(A_{\mathrm{yes}},A_{\mathrm{no}})$ is in $\mathrm{QCMA}(c,s)$ iff there exist a polynomially bounded function $m\colon \mathbb{Z}^+ \to \mathbb{N}$ and a polynomial-time quantum verifier V, who is a polynomial-time uniformly generated family of quantum circuits $\{V_{x,w}\}_{x\in\{0,1\}^*, w\in\{0,1\}^{m(|x|)}}$, such that, for every input x:*

(Completeness) *if $x \in A_{\mathrm{yes}}$, there exists a witness $w \in \{0,1\}^{m(|x|)}$ with which V accepts x (i.e., the measurement on the output qubit of $V_{x,w}$ results in $|1\rangle$) with probability at least $c(|x|)$,*

(Soundness) *if $x \in A_{\mathrm{no}}$, for any witness $w' \in \{0,1\}^{m(|x|)}$ given, V accepts x with probability at most $s(|x|)$.*

The complexity class QCMA is defined as follows.

Definition 2 *A promise problem $A=(A_{\mathrm{yes}},A_{\mathrm{no}})$ is in* QCMA *iff A is in* $\mathrm{QCMA}(1-\varepsilon,\varepsilon)$ *for some negligible function $\varepsilon\colon \mathbb{Z}^+ \to [0,1]$.*

Similarly, the class QCMA_1 is defined as follows.

Definition 3 *A promise problem $A=(A_{\mathrm{yes}},A_{\mathrm{no}})$ is in* QCMA_1 *iff A is in* $\mathrm{QCMA}(1,\varepsilon)$ *for some negligible function $\varepsilon\colon \mathbb{Z}^+ \to [0,1]$.*

Note that $\mathrm{QCMA} = \mathrm{QCMA}(2/3,1/3)$ and $\mathrm{QCMA}_1 = \mathrm{QCMA}(1,1/2)$, since the gap between completeness and soundness can be amplified exponentially by repeating the verification procedure.

3 Result

Now we show that any QCMA proof system with two-sided error can be converted into another QCMA proof system with perfect completeness.

Theorem 1 $\mathrm{QCMA} = \mathrm{QCMA}_1$.

In fact, we show a more general theorem stated below. Theorem 1 is an immediate corollary.

Theorem 2 *For any polynomial-time computable function $c\colon \mathbb{Z}^+ \to [0,1]$ and any function $s\colon \mathbb{Z}^+ \to [0,1]$ satisfying $c-s \geq 1/q$ for some polynomially bounded[c] function $q\colon \mathbb{Z}^+ \to \mathbb{N}$,*

$$\mathrm{QCMA}(c,s) \subseteq \mathrm{QCMA}(1,s'),$$

where $s' = \frac{1}{2}\bigl(1-(c-s)\bigr)\bigl(1+(1+c-s)^2\bigr) < 1$.

By taking $c=2/3$ and $s=1/3$, Theorem 2 implies $\mathrm{QCMA}(2/3,1/3) \subseteq \mathrm{QCMA}(1,25/27)$, which is sufficient to obtain Theorem 1.

The rest of this section is devoted to the proof of Theorem 2.

Proof of Theorem 2: Let $A=(A_{\mathrm{yes}},A_{\mathrm{no}})$ be in $\mathrm{QCMA}(c,s)$ and let V be the verifier of the corresponding QCMA system. Consider the quantum circuit $V_{x,w}$ of V when the input is x and the received witness is w of $m(|x|)$ bits, for some polynomially bounded function $m\colon \mathbb{Z}^+ \to \mathbb{N}$.

[c] Actually, it is sufficient for our proof that $c-s \geq 1/2^q$ for some polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$.

Without loss of generality, by Refs. [25, 24], one can assume that $V_{x,w}$ consists of only the Hadamard, Toffoli, and NOT gates, and the output is obtained by measuring the designated output qubit in the computational basis. Therefore, the acceptance probability of $V_{x,w}$ is exactly expressible as $k_{x,w}/2^{l(|x|)}$ for some integer $k_{x,w}$ in $\{0,1,\ldots,2^{l(|x|)}\}$, where $l\colon \mathbb{Z}^+ \to \mathbb{N}$ is a polynomially bounded function such that $l(|x|)$ denotes the size of the circuit $V_{x,w}$.

We construct a new verifier W assuring that A is in QCMA$(1,s')$. Let R be the quantum register consisting of all the qubits used by $V_{w,x}$. The verifier W uses three more quantum registers B, O, and S in addition to R, where B and O are single-qubit registers, and S is a quantum register of $l(|x|)$ qubits. All the qubits in these four registers are initialized to $|0\rangle$. The qubit in O is designated as the output qubit in the constructed system. As a witness, W receives binary strings w and k, where w is expected to be the witness V would receive in the original system, and k is an $l(|x|)$-bit string that identifies a positive integer in $\{1,\ldots,2^{l(|x|)}\}$ that is expected to be $k_{x,w}$. Here notice that we are considering a natural one-to-one correspondence between $l(|x|)$-bit strings and integers from 1 to $2^{l(|x|)}$ (rather than from 0 to $2^{l(|x|)}-1$), for $k_{x,w}$ cannot be zero but can be $2^{l(|x|)}$ in the yes-instance case. W immediately rejects if k viewed as an integer is less than $c(|x|)\cdot 2^{l(|x|)}$.

Then W applies the Hadamard transformations over all qubits in registers B and S, and applies the original verification circuit $V_{x,w}$ over the qubits in R. W accepts either when B contains 0 and the content of R would result in acceptance in the original system, or when B contains 1 and the content of S viewed as an integer expressed by an $l(|x|)$-bit string is greater than k (the qubit in O, which is the output qubit of the constructed system, is flipped to $|1\rangle$ in these two cases). Otherwise W continues by performing the quantum rewinding procedure. The precise description of the protocol of W is given in Figure 1. It is easy to see that this protocol is exactly implementable using only the Hadamard and classical reversible transformations (the protocol includes intermediate measurement, which can be postponed until the very end of the protocol via a standard technique that only uses classical reversible transformations).

Now we analyze the protocol. Our analysis is similar to the proof of Lemma 3.3 in Ref. [18] (which is based on the ideas in Refs. [17, 23]).

Let Π_{init} be the projection onto the all-zero state (i.e., the state in which all the qubits in $(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})$ are in state $|0\rangle$, which is denoted by $|0\rangle_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})}$) and let Π_{acc} be the projection onto states in which the qubit in O is in state $|1\rangle$. Let Q be the unitary transformation induced by the actions in Step 2. Conditioned on W *not* rejecting in Step 1, the probability of being accepted in Step 3.1 can be written as $p_{x,w,k} = \left\|\Pi_{\mathrm{acc}} Q|0\rangle_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})}\right\|^2$. This implies that the matrix $M = \Pi_{\mathrm{init}} Q^\dagger \Pi_{\mathrm{acc}} Q \Pi_{\mathrm{init}}$ is expressed as

$$M = \Pi_{\mathrm{init}} Q^\dagger \Pi_{\mathrm{acc}} Q \Pi_{\mathrm{init}} = p_{x,w,k}|0\rangle\langle 0|_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})} = p_{x,w,k}\Pi_{\mathrm{init}},$$

since

$$\begin{aligned}\Pi_{\mathrm{init}} Q^\dagger \Pi_{\mathrm{acc}} Q \Pi_{\mathrm{init}} &= |0\rangle_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})}\big(\langle 0|_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})} Q^\dagger \Pi_{\mathrm{acc}} Q|0\rangle_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})}\big)\langle 0|_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})}\\ &= \left\|\Pi_{\mathrm{acc}} Q|0\rangle_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})}\right\|^2 |0\rangle\langle 0|_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})}.\end{aligned}$$

Define the unnormalized states $|\phi_0\rangle$, $|\phi_1\rangle$, $|\psi_0\rangle$, and $|\psi_1\rangle$ by

$$|\phi_0\rangle = \Pi_{\mathrm{acc}} Q|0\rangle_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})},\quad |\phi_1\rangle = \Pi_{\mathrm{rej}} Q|0\rangle_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})},\quad |\psi_0\rangle = \Pi_{\mathrm{init}} Q^\dagger|\phi_0\rangle,\quad |\psi_1\rangle = \Pi_{\mathrm{illegal}} Q^\dagger|\phi_0\rangle,$$

Verifier's Protocol for Achieving Perfect Completeness

1. Receive an $m(|x|)$-bit string w and an integer k in $\{1, \dots, 2^{l(|x|)}\}$ expressed by an $l(|x|)$-bit string as witness. Reject if $k/2^{l(|x|)} < c(|x|)$.
2. Perform the following unitary transformation Q over the qubits in $(\mathsf{B}, \mathsf{O}, \mathsf{R}, \mathsf{S})$.
   - 2.1 Apply the Hadamard transformations to all the qubits in B and S, and apply $V_{x,w}$ to the qubits in R.
   - 2.2 Apply the bit-flip to the qubit in O either when B contains 0 and the content of R would result in acceptance in the original system, or when B contains 1 and the content of S viewed as an integer in $\{1, \dots, 2^{l(|x|)}\}$ is greater than k.
3. Do the following steps (quantum rewinding):
   - 3.1 Accept if O contains 1, and continue otherwise.
   - 3.2 Invert Step 2. That is, apply $Q^\dagger$ to $(\mathsf{B}, \mathsf{O}, \mathsf{R}, \mathsf{S})$.
   - 3.3 Perform the phase-flip (i.e., multiply -1 in phase) if all the qubits in $(\mathsf{B}, \mathsf{O}, \mathsf{R}, \mathsf{S})$ are in state $|0\rangle$.
   - 3.4 Perform the same operations as in Step 2. That is, apply Q to $(\mathsf{B}, \mathsf{O}, \mathsf{R}, \mathsf{S})$.
   - 3.5 Accept if O contains 1, and reject otherwise.

Fig. 1. Verifier's protocol for achieving perfect completeness. Note that the conditional phase flip can be exactly achieved using {Hadmard, Toffoli, NOT} by preparing an ancilla qubit $|0\rangle$ into the state $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ by the application of a NOT followed by a Hadamard, and then performing a conditional NOT on that qubit.

where Π_{illegal} is the projection onto states orthogonal to $|0\rangle_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})}$ and Π_{rej} is that onto states in which the qubit in O is in state $|0\rangle$.

First, we analyze the acceptance probability of W when the claimed k satisfies $k \geq c(|x|) \cdot 2^{l(|x|)}$ (i.e., when W does not reject in Step 1). Clearly, W accepts in Step 3.1 with probability $p_{x,w,k}$. We analyze the probability of being accepted in Step 3.5. For this purpose, it suffices to follow the changes of the unnormalized state $|\phi_1\rangle = \Pi_{\mathrm{rej}} Q |0\rangle_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})}$ during the protocol when W continues in Step 3.1. Since

$$\begin{aligned}
|\psi_0\rangle &= \Pi_{\mathrm{init}} Q^\dagger \Pi_{\mathrm{acc}} Q |0\rangle_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})} \\
&= \Pi_{\mathrm{init}} Q^\dagger \Pi_{\mathrm{acc}} Q \Pi_{\mathrm{init}} |0\rangle_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})} = M|0\rangle_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})} = p_{x,w,k}|0\rangle_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})},
\end{aligned}$$

the state[d] just after Step 3.2 is

$$\begin{aligned}
Q^\dagger \Pi_{\mathrm{rej}} Q |0\rangle_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})} &= |0\rangle_{(\mathsf{B},\mathsf{O},\mathsf{R},\mathsf{S})} - Q^\dagger |\phi_0\rangle \\
&= \frac{1}{p_{x,w,k}} |\psi_0\rangle - \big(|\psi_0\rangle + |\psi_1\rangle\big) \\
&= \frac{1 - p_{x,w,k}}{p_{x,w,k}} |\psi_0\rangle - |\psi_1\rangle.
\end{aligned}$$

[d]The norm of this state is $\sqrt{1 - p_{x,w,k}}$. Alternatively, one could carry out the analysis with a conventional normalized state, in which case one would obtain the *conditional* probability of accepting in Step 3.5 given that Step 3.1 does not accept. This conditional probability is one in the case where $p_{x,w,k} = 1/2$.

As $\Pi_{\mathrm{init}}|\psi_0\rangle = |\psi_0\rangle$ and $\Pi_{\mathrm{init}}|\psi_1\rangle = 0$, the controlled phase-flip in Step 3.3 changes the state to

$$-\frac{1-p_{x,w,k}}{p_{x,w,k}}|\psi_0\rangle - |\psi_1\rangle = -\frac{1-2p_{x,w,k}}{p_{x,w,k}}|\psi_0\rangle - \big(|\psi_0\rangle + |\psi_1\rangle\big)$$
$$= -(1-2p_{x,w,k})|0\rangle_{(\mathsf{B,O,R,S})} - Q^\dagger|\phi_0\rangle.$$

Using $Q|0\rangle_{(\mathsf{B,O,R,S})} = |\phi_0\rangle + |\phi_1\rangle$, one can see that the state just after Step 3.4 is

$$-(1-2p_{x,w,k})Q|0\rangle_{(\mathsf{B,O,R,S})} - |\phi_0\rangle = -(2-2p_{x,w,k})|\phi_0\rangle - (1-2p_{x,w,k})|\phi_1\rangle.$$

Thus, the probability of being accepted in Step 3.5 is

$$(2-2p_{x,w,k})^2\big\||\phi_0\rangle\big\|^2 = 4p_{x,w,k}(1-p_{x,w,k})^2.$$

Hence, the acceptance probability p_{acc} of W when the claimed k satisfies $k \geq c(|x|)\cdot 2^{l(|x|)}$ is given by

$$p_{\mathrm{acc}} = p_{x,w,k} + 4p_{x,w,k}(1-p_{x,w,k})^2.$$

Now we calculate $p_{x,w,k} = \big\|\Pi_{\mathrm{acc}}Q|0\rangle_{(\mathsf{B,O,R,S})}\big\|^2$. Notice that

$$\begin{aligned} Q|0\rangle_{(\mathsf{B,O,R,S})} = \frac{1}{\sqrt{2^{l(|x|)+1}}}\Big(&|0\rangle_{\mathsf{B}}|0\rangle_{\mathsf{O}}\big(|0\rangle|\chi_0\rangle\big)_{\mathsf{R}}\sum_{z\in\{1,\dots,2^{l(|x|)}\}}|z\rangle_{\mathsf{S}} \\ &+|0\rangle_{\mathsf{B}}|1\rangle_{\mathsf{O}}\big(|1\rangle|\chi_1\rangle\big)_{\mathsf{R}}\sum_{z\in\{1,\dots,2^{l(|x|)}\}}|z\rangle_{\mathsf{S}} \\ &+|1\rangle_{\mathsf{B}}|0\rangle_{\mathsf{O}}\big(|0\rangle|\chi_0\rangle+|1\rangle|\chi_1\rangle\big)_{\mathsf{R}}\sum_{z\in\{1,\dots,k\}}|z\rangle_{\mathsf{S}} \\ &+|1\rangle_{\mathsf{B}}|1\rangle_{\mathsf{O}}\big(|0\rangle|\chi_0\rangle+|1\rangle|\chi_1\rangle\big)_{\mathsf{R}}\sum_{z\in\{k+1,\dots,2^{l(|x|)}\}}|z\rangle_{\mathsf{S}}\Big), \end{aligned}$$

where we denote the state $V_{x,w}|0\rangle_{\mathsf{R}}$ just before the final measurement in the original system by $|0\rangle|\chi_0\rangle + |1\rangle|\chi_1\rangle$, assuming that the first qubit in R was the output qubit in the original system. Since $\big\||\chi_1\rangle\big\|^2 = k_{x,w}/2^{l(|x|)}$, one can see that

$$p_{x,w,k} = \frac{1}{2}\cdot\frac{k_{x,w}}{2^{l(|x|)}} + \frac{1}{2}\cdot\frac{2^{l(|x|)}-k}{2^{l(|x|)}} = \frac{1}{2} - \frac{1}{2^{l(|x|)+1}}(k-k_{x,w}).$$

Now we are ready to verify the completeness and soundness of the constructed protocol.

For the completeness, one can take w to be any string that achieves $k_{x,w}/2^{l(|x|)} \geq c(|x|)$ (recall that the acceptance probability of $V_{x,w}$ is $k_{x,w}/2^{l(|x|)}$), and k to be $k_{x,w}$ for the chosen w. Then clearly W does not reject in Step 3.1 and we have $p_{x,w,k} = 1/2$, which implies $p_{\mathrm{acc}} = 1$. Thus, W accepts x with certainty.

For the soundness, note that one has only to consider the case where $k/2^{l(|x|)} \geq c(|x|)$, as otherwise W rejects with certainty in Step 3.1. Since for any w the acceptance probability $k_{x,w}/2^{l(|x|)}$ of $V_{x,w}$ is at most $s(|x|)$,

$$p_{x,w,k} \leq \frac{1}{2} - \frac{1}{2^{l(|x|)+1}}\big(c(|x|)\cdot 2^{l(|x|)} - s(|x|)\cdot 2^{l(|x|)}\big) = \frac{1}{2} - \frac{c(|x|)-s(|x|)}{2}.$$

Noting that the function $f(p) = p + 4p(1-p)^2$ is monotone increasing over $[0, 1/2]$ and $f(1/2) = 1$, one can see that p_{acc} is at most

$$\begin{aligned} & f\left(\frac{1}{2} - \frac{c(|x|) - s(|x|)}{2}\right) \\ & \quad = \frac{1}{2} - \frac{c(|x|) - s(|x|)}{2} + 4\left(\frac{1}{2} - \frac{c(|x|) - s(|x|)}{2}\right)\left(\frac{1}{2} + \frac{c(|x|) - s(|x|)}{2}\right)^2 \\ & \quad = \frac{1}{2}\Big(1 - \big(c(|x|) - s(|x|)\big)\Big)\Big(1 + \big(1 + c(|x|) - s(|x|)\big)^2\Big), \end{aligned}$$

which is smaller than $f(1/2) = 1$. Thus the soundness follows, which completes the proof. □

4 Concluding Remarks

This paper has proved that $\mathrm{QCMA} = \mathrm{QCMA}_1$ holds under any gate set with which the Hadamard and arbitrary classical reversible transformations can be exactly implemented. As already mentioned, this result is not quantumly relativizing. It should be noted, however, that it is classically relativizing (i.e., $\mathrm{QCMA}^A = \mathrm{QCMA}_1^A$ for any classical oracle A). Here we assume the standard model of classical oracles in computational complexity theory, in particular that the answer of A for any query is deterministic. This fact can be easily seen: for any specific choice of A, the acceptance probability of the verifier can still be represented in the form of $k/2^{l(|x|)}$ since A is deterministic.

A natural question to ask is whether one can extend our argument to the QMA case to show that $\mathrm{QMA} = \mathrm{QMA}_1$. There seem to be at least two obstacles for this. First, the maximum acceptance probability of the verifier (even in the honest Merlin case) cannot be expressed with a polynomial number of bits in general. This is because the maximum acceptance probability in the QMA system corresponds to the largest eigenvalue of a certain appropriate matrix, which might only be describable as a zero of some polynomial with exponentially many terms. Second, even if one knew its probability as an algebraic number, it is not easy to boost the probability to one via amplitude amplification or quantum rewinding – without an explicit description of the initial state we do not see a way to perform a perfect reflection about the initial state, which seems to be necessary (see, *e.g.*, Ref. [30]).

Acknowledgements

The authors thank Jake Taylor, Michele Mosca, and Pawel Wocjan for useful discussions, and an anonymous reviewer for helpful comments on the earlier version of this paper. Part 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. HK is partially supported by 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, from the project APVV-0646-10, and European project Q-ESSENCE. HN is partially supported by the Grant-in-Aid 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

1. John Watrous. Quantum computational complexity. In Robert A. Meyers, editor, *Encyclopedia of Complexity and Systems Science*, pages 7174–7201. Springer-Verlag, 2009. arXiv:0804.3401[quant-ph].
2. Sevag Gharibian, Jamie Sikora, and Sarvagya Upadhyay. QMA variants with polynomially many provers. arXiv:1108.0617[quant-ph], 2011.
3. Emanuel Knill. Quantum randomness and nondeterminism. Technical Report LAUR-96-2186, Los Alamos National Laboratory, 1996. arXiv:quant-ph/9610012.
4. Dorit Aharonov and Tomer Naveh. Quantum NP - A survey. arXiv:quant-ph/0210077, 2002.
5. László Babai. Trading group theory for randomness. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, pages 421–429, 1985.
6. László Babai and Shlomo Moran. Arthur-Merlin games: A randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36(2):254–276, 1988.
7. John Watrous. Succinct quantum proofs for properties of finite groups. In *41st Annual Symposium on Foundations of Computer Science*, pages 537–546, 2000. arXiv:cs/0009002[cs.CC].
8. Alexei Yu. Kitaev. Quantum NP. Talk at the 2nd Workshop on Algorithms in Quantum Information Processing, DePaul University, Chicago, January 1999.
9. 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.
10. Sergey Bravyi. Efficient algorithm for a quantum analogue of 2-SAT. arXiv:quant-ph/0602108, 2006.
11. Stathis Zachos and Martin Fürer. Probabalistic 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.
12. Oded Goldreich and David Zuckerman. Another proof that BPP $\subseteq$ 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.
13. Oded Goldreich, Yishay Mansour, and Michael Sipser. Interactive proof systems: Provers that never fail and random selection (extended abstract). In *28th Annual Symposium on Foundations of Computer Science*, pages 449–461, 1987.
14. Martin Fürer, Oded Goldreich, Yishay Mansour, Michael Sipser, and Stathis Zachos. On completeness and soundness in interactive proof systems. In Silvio Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, pages 429–442. JAI Press, 1989.
15. Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, pages 113–131, 1988.
16. 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.
17. Chris Marriott and John Watrous. Quantum Arthur-Merlin games. *Computational Complexity*, 14(2):122–152, 2005. arXiv:cs/0506068[cs.CC].
18. Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, and Thomas Vidick. Using entanglement in quantum multi-prover interactive proofs. *Computational Complexity*, 18(2):273–307, 2009. arXiv:0711.3715[quant-ph].
19. Scott Aaronson. On perfect completeness for QMA. *Quantum Information and Computation*, 9(1–2):0081–0089, 2009. arXiv:0806.0450[quant-ph].
20. Pawel Wocjan, Dominik Janzing, and Thomas Beth. Two QCMA-complete problems. *Quantum Information and Computation*, 3(6):635–643, 2003. arXiv:quant-ph/0305090.
21. 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. arXiv:quant-ph/0005055.

22. 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. arXiv:quant-ph/9708005.
23. John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009. arXiv:quant-ph/0511020.
24. Yaoyun Shi. Both Toffoli and Controlled-NOT need little help to do universal quantum computing. *Quantum Information and Computation*, 3(1):084–092, 2002. arXiv:quant-ph/0205115.
25. Dorit Aharonov. A simple proof that Toffoli and Hadamard are quantum universal. arXiv:quant-ph/0301040, 2003.
26. Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
27. Peter W. Shor. Fault-tolerant quantum computation. In *37th Annual Symposium on Foundations of Computer Science*, pages 56–65, 1996. arXiv:quant-ph/9605011.
28. Dorit Aharonov, Alexei Kitaev, and Noam Nisan. Quantum circuits with mixed states. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, pages 20–30, 1998. arXiv:quant-ph/9806029.
29. Shimon Even, Alan L. Selman, and Yacov Yacobi. The complexity of promise problems with applications to public-key cryptography. *Information and Control*, 61(2):159–173, 1984.
30. Daniel Nagaj, Pawel Wocjan, and Yong Zhang. Fast amplification of QMA. *Quantum Information and Computation*, 9(11–12):1053–1068, 2009. arXiv:0904.1549[quant-ph].