Generalized Quantum Arthur-Merlin Games

Hirotada Kobayashi[1], François Le Gall[2], and Harumichi Nishimura[3]

1 **Principles of Informatics Research Division**
National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda, Tokyo 101-8430, Japan
hirotada@nii.ac.jp

2 **Department of Computer Science**
Graduate School of Information Science and Technology
The University of Tokyo
7-3-1 Hongo, Bunkyo, Tokyo 113-0033, Japan
legall@is.s.u-tokyo.ac.jp

3 **Department of Computer Science and Mathematical Informatics**
Graduate School of Information Science
Nagoya University
Furo-cho, Chikusa, Nagoya, Aichi 464-8601, Japan
hnishimura@is.nagoya-u.ac.jp

Abstract

This paper investigates the role of interaction and coins in *quantum Arthur-Merlin games* (also called *public-coin quantum interactive proof systems*). While the existing model restricts the messages from the verifier to be classical even in the quantum setting, the present work introduces a generalized version of quantum Arthur-Merlin games where the messages from the verifier can be quantum as well: the verifier can send not only random bits, but also halves of EPR pairs. This generalization turns out to provide several novel characterizations of quantum interactive proof systems with a constant number of turns. First, it is proved that the complexity class corresponding to two-turn quantum Arthur-Merlin games where both of the two messages are quantum, denoted qq-QAM in this paper, does not change by adding a constant number of turns of classical interaction prior to the communications of qq-QAM proof systems. This can be viewed as a quantum analogue of the celebrated collapse theorem for AM due to Babai. To prove this collapse theorem, this paper presents a natural complete problem for qq-QAM: deciding whether the output of a given quantum circuit is close to a totally mixed state. This complete problem is on the very line of the previous studies investigating the hardness of checking properties related to quantum circuits, and thus, qq-QAM may provide a good measure in computational complexity theory. It is further proved that the class qq-QAM_1, the perfect-completeness variant of qq-QAM, gives new bounds for standard well-studied classes of two-turn quantum interactive proof systems. Finally, the collapse theorem above is extended to comprehensively classify the role of classical and quantum interactions in quantum Arthur-Merlin games: it is proved that, for any constant $m \geq 2$, the class of problems having m-turn quantum Arthur-Merlin proof systems is either equal to PSPACE or equal to the class of problems having two-turn quantum Arthur-Merlin proof systems of a specific type, which provides a complete set of quantum analogues of Babai's collapse theorem.

1998 ACM Subject Classification F.1.2 Modes of Computation, F.1.3 Complexity Measures and Classes

Keywords and phrases interactive proof systems, Arthur-Merlin games, quantum computing, complete problems, entanglement

Digital Object Identifier 10.4230/LIPIcs.CCC.2015.488

30th Conference on Computational Complexity (CCC'15).
Editor: David Zuckerman; pp. 488–511

Leibniz International Proceedings in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

1 Introduction

Background and motivation. Interactive proof systems [9, 4] play a central role in computational complexity and have many applications such as probabilistically checkable proofs and zero-knowledge proofs. The aim of such a system is the verification of an assertion (e.g., verifying if an input is in a language) by a party implementing a polynomial-time probabilistic computation, called the verifier, interacting with another party with unlimited power, called the prover, in polynomially many turns. Two definitions are given on the secrecy of the coin which the verifier can flip: Goldwasser, Micali, and Rackoff [9] defined private-coin proof systems, where the prover cannot see the outcomes of coin flips, while Babai [4] defined public-coin proof systems, where the prover can see all the outcomes of coin flips. Public-coin interactive proof systems are often called Arthur-Merlin games or Arthur-Merlin proof systems, since the verifier was called Arthur and the prover was called Merlin in Ref. [4].

It is natural to expect that the power of interactive proof systems depends on the number of turns of interaction. Babai [4] showed, however, that as long as the number of turns is a constant at least two, the number of turns does not affect the power of Arthur-Merlin proof systems, i.e., $\mathrm{AM}(m) = \mathrm{AM}(2)$ for any constant $m \geq 2$ (the *collapse theorem*), where $\mathrm{AM}(m)$ is the class of problems having m-turn Arthur-Merlin proof systems. Goldwasser and Sipser [10] then showed that a private-coin interactive proof system can be simulated by an Arthur-Merlin proof system by adding two turns, and thus, these two types of interactive proof systems are computationally equivalent. By the above results, the class of problems having interactive proof systems of a constant number of turns is equal to $\mathrm{AM}(2)$ (regardless of definitions with public coins or private coins), and this class is nowadays called AM. The class AM is believed to be much smaller than PSPACE, as it is contained in Π_2^{P} in the second level of the polynomial-time hierarchy [22, 4]. On the contrary, the class of problems having more general interactive proof systems of polynomially many turns, called IP, does coincide with PSPACE [26, 23, 28] (again regardless of definitions with public coins or private coins [10, 29]).

Quantum interactive proof systems were introduced by Watrous [34], and the class of problems having quantum interactive proof systems is called QIP. In the quantum world, the importance of the number of turns in interactive proof systems is drastically changed. The first paper on quantum interactive proofs [34] already proved the surprising power of quantum interactive proof systems with a constant number of turns, by showing that any problem in PSPACE has a three-turn quantum interactive proof system. Kitaev and Watrous [16] then proved that any quantum interactive proof system can be simulated by a three-turn quantum interactive proof system, namely, $\mathrm{QIP} = \mathrm{QIP}(3)$, where $\mathrm{QIP}(m)$ denotes the class of problems having m-turn quantum interactive proof systems. Finally, the recent result $\mathrm{QIP} = \mathrm{PSPACE}$ by Jain, Ji, Upadhyay, and Watrous [13] completely characterized the computational power of quantum interactive proof systems with three turns or more. In contrast, despite a number of intensive studies [33, 36, 14, 12], still very little is known on the class $\mathrm{QIP}(2)$ corresponding to *two-turn* quantum interactive proof systems, and characterizing the computational power of two-turn quantum interactive proof systems is one of the main open problems in this field.

A public-coin version of quantum interactive proof systems was first introduced by Marriott and Watrous [24], named quantum Arthur-Merlin proof systems, where the messages from the verifier are restricted to classical strings consisting only of outcomes of polynomially many attempts of a fair coin flip. They then showed that three-turn quantum Arthur-Merlin proof systems can simulate three-turn standard quantum interactive proof systems, and

hence the corresponding class, denoted QMAM, coincides with QIP = PSPACE. They also investigated the case of two-turn quantum Arthur-Merlin proof systems and showed that the corresponding class, denoted QAM, is included in BP · PP, a subclass of PSPACE obtained by applying the BP operator to the class PP, which is still the only nontrivial upper bound known for QAM.

Results and their meanings. This paper introduces a "fully quantum" version of quantum Arthur-Merlin proof systems, which generalizes the existing quantum Arthur-Merlin proof systems in Ref. [24]. In this generalized model, the verifier can send quantum messages, but these messages can be used only for sharing EPR pairs with the prover, i.e., the verifier at his/her turn first generates polynomially many EPR pairs and then sends one half of each of them to the prover. Recall that classical public-coin messages can be interpreted as messages for sharing uniform randomness between the verifier and the prover. In this context, sharing EPR pairs would be the most natural quantum analogue of sharing randomness, and thus, the model introduced above may be viewed as a natural full-quantum version of quantum Arthur-Merlin proof systems.

The main interest in this model is again on the two-turn case, as allowing three or more turns in this model obviously hits the PSPACE ceiling. Let qq-QAM be the class of problems having two-turn "fully quantum" Arthur-Merlin proof systems, i.e., two-turn quantum interactive proof systems in which the first message from the verifier consists only of polynomially many halves of EPR pairs. Note that the only difference from the existing class QAM lies in the type of the message from the verifier: uniform random classical bits are replaced by halves of EPR pairs. The main goal of this paper is to investigate the computational power of this class qq-QAM in order to figure out the advantages offered by sharing EPR pairs rather than classical randomness, and more generally, to make a step forward in the understanding of two-turn quantum interactive proof systems.

While the class qq-QAM is the main target of investigation, this paper further studies the power of various models of quantum Arthur-Merlin proofs with quantum/classical messages. For any constant $m \geq 1$ and any message-types $t_1, \ldots, t_m$ in $\{\mathrm{c}, \mathrm{q}\}$, let $t_m \cdots t_1$-QAM(m) be the class of problems having m-turn quantum interactive proof systems with the following restrictions:

- For any odd j, $1 \leq j \leq m$, the $(m-j+1)$st message (or the jth message counting from the last), which is the message from the prover sent at the $(m-j+1)$st turn, is a quantum message if $t_j = \mathrm{q}$, and is restricted to a classical message if $t_j = \mathrm{c}$.
- For any even j, $1 \leq j \leq m$, at the $(m-j+1)$st turn, which is a turn for the verifier, the verifier first generates polynomially many EPR pairs and then sends halves of them if $t_j = \mathrm{q}$, while the verifier first flips a fair coin polynomially many times and then sends their outcomes if $t_j = \mathrm{c}$.

The class $t_m \cdots t_1$-QAM(m) may be simply written as $t_m \cdots t_1$-QAM when there is no ambiguity in the number of turns: for instance, qq-QAM(2) may be abbreviated to qq-QAM. Note that the classes QAM and QMAM defined in Ref. [24] are exactly the classes cq-QAM and qcq-QAM, respectively. The class cc-QAM corresponds to two-turn public-coin quantum interactive proofs with classical communications: the verifier sends a question consisting only of outcomes of polynomially many attempts of a fair coin flip, then the prover responds with polynomially many classical bits, and the final verification is done by the verifier via polynomial-time quantum computation. By definition, AM $\subseteq$ cc-QAM $\subseteq$ cq-QAM $\subseteq$ qq-QAM $\subseteq$ QIP(2).

As mentioned above, the main target in this paper is the class qq-QAM. First, it is proved that the power of qq-QAM proof systems does not change by adding a constant number of turns of classical interaction prior to the communications of qq-QAM proof systems.

▶ **Theorem 1.1.** *For any constant* $m \geq 2$, $\mathrm{c}\cdots\mathrm{cqq\text{-}QAM}(m) = \mathrm{qq\text{-}QAM}$.

In stark contrast to this, as mentioned before and will be stated clearly in Theorem 1.7, adding one turn of prior quantum interaction gives qq-QAM proof systems the full power of quantum interactive proof systems (i.e., the resulting class is PSPACE). Hence, Theorem 1.1 may be viewed as a quantum analogue of Babai's collapse theorem [4] for the class qq-QAM.

The proof of Theorem 1.1 comes in three parts: The first part proves that, for any constant $m \geq 4$, $\mathrm{c}\cdots\mathrm{cqq\text{-}QAM}(m)$ is necessarily included in ccqq-QAM. The second part proves that cqq-QAM is included in qq-QAM. Finally, the third part proves that ccqq-QAM is included in qq-QAM, by using the containment proved in the second part.

The first part is proved by carefully extending the argument in Babai's collapse theorem. The core idea of Babai's proof is that, by a probabilistic argument applied to a parallel repetition of the original proof system, the order of the verifier and the prover in the first three turns of the original system can be switched, which results in another proof system that has fewer number of turns. When proving the first part, the messages of the first three turns of the original m-turn quantum Arthur-Merlin proof system are classical, and thus, the argument in Babai's collapse theorem still works.

The proof of the second part is one of the highlights of this paper. The main difficulty in proving this part (and the third part) is that the argument used in Babai's collapse theorem fails when any of the first three turns is quantum in the starting proof system.

To overcome this difficulty, this paper first provides a natural complete promise problem for qq-QAM, namely, the Close Image to Totally Mixed (CITM) problem, which asks to check if the image of a given quantum circuit can be close to a totally mixed state, formally defined as follows.

Close Image to Totally Mixed Problem: $\mathrm{CITM}(a, b)$

Input: A description of a quantum circuit Q acting on q_{all} qubits that has q_{in} specified input qubits and q_{out} specified output qubits.

Yes Instances: There exists a q_{in}-qubit state ρ such that $D\big(Q(\rho), (I/2)^{\otimes q_{\mathrm{out}}}\big) \leq a$.

No Instances: For any q_{in}-qubit state ρ, $D\big(Q(\rho), (I/2)^{\otimes q_{\mathrm{out}}}\big) \geq b$.

Here, $D(\cdot,\cdot)$ denotes the trace distance, $Q(\rho)$ is the q_{out}-qubit output state of Q when the input state was ρ (i.e., the reduced state obtained by tracing out the space corresponding to the $(q_{\mathrm{all}} - q_{\mathrm{out}})$ non-output qubits after applying Q to $\rho \otimes (|0\rangle\langle 0|)^{\otimes(q_{\mathrm{all}} - q_{\mathrm{in}})}$), and I is the identity operator of dimension two (and thus, $(I/2)^{\otimes q_{\mathrm{out}}}$ corresponds to the totally mixed state of q_{out} qubits). The following completeness result is proved.

▶ **Theorem 1.2.** *For any constants* a *and* b *in* $(0,1)$ *such that* $(1-a)^2 > 1-b^2$, $\mathrm{CITM}(a,b)$ *is* qq-QAM*-complete under polynomial-time many-one reduction.*

Then the core idea for proving the second part is to use the structure of this complete problem that yes-instances are witnessed by the existence of a quantum state (i.e., the $\exists$ quantifier appears in the first place), while no such witness quantum state exists for no-instances (i.e., the $\forall$ quantifier appears in the first place). This makes it possible to incorporate the first turn of the cqq-QAM system into the input quantum state of the complete problem CITM (as the quantifier derived from the first turn of the cqq-QAM system matches the quantifier derived from the complete problem CITM), and thus, any problem in cqq-QAM

can be reduced in polynomial time to the CITM problem with appropriate parameters, which is in qq-QAM.

Actually, for the proof, whether the image of a constructed quantum circuit can be close to a totally mixed state is partly evaluated by using the maximum output entropy of quantum channels, which shows implicitly the qq-QAM-completeness of another problem that asks to check whether the maximum output entropy of a quantum channel is larger than a given value or not. More formally, the following Maximum Output Quantum Entropy Approximation (MaxOutQEA) problem is also qq-QAM-complete.

Maximum Output Quantum Entropy Approximation Problem: MaxOutQEA

Input: A description of a quantum circuit that specifies a quantum channel Φ, and a positive integer t.

Yes Instances: $S_{\max}(\Phi) \geq t + 1$.

No Instances: $S_{\max}(\Phi) \leq t - 1$.

Here, $S_{\max}(\cdot)$ denotes the maximum output von Neumann entropy. Namely, for any quantum channel Φ, $S_{\max}(\Phi) = \max_{\rho} S(\Phi(\rho))$, where $S(\cdot)$ denotes the von Neumann entropy and $\Phi(\rho)$ is the output quantum state of Φ when the input quantum state to it was ρ.

▶ **Theorem 1.3.** MaxOutQEA *is* qq-QAM*-complete under polynomial-time many-one reduction.*

Finally, the third part of the proof of Theorem 1.1 is obtained by first providing a randomized reduction from a problem in ccqq-QAM to a problem in cqq-QAM, and then using the containment proved in the second part for the resulting problem in cqq-QAM.

Besides its usefulness in proving Theorem 1.1, the complete problem CITM is of independent interest in the following sense. Recall that problems with formulations similar to CITM have already been studied, and were crucial to understand and characterize several complexity classes related to quantum interactive proof systems: testing closeness between the images of two given quantum circuits is QIP-complete [27] (and hence PSPACE-complete), testing closeness between the state produced by a given circuit and the image of another quantum circuit is QIP(2)-complete [32] (see also Ref. [12]), testing closeness between the two states produced by two given quantum circuits is QSZK-complete [33, 35], and testing closeness between the state produced by a quantum circuit and the totally mixed state is NIQSZK-complete [18, 8]. Theorem 1.2 shows that the class qq-QAM, besides its theoretical interest in the context of interactive proofs, is a very natural one that actually corresponds to a concrete computational problem that is on this line of studies investigating the hardness of checking properties related to quantum circuits. Since CITM corresponds to the remaining pattern (image versus totally mixed state), Theorem 1.2 provides the last piece for characterizing the hardness of these kinds of computational problems.

The complete problem MaxOutQEA is also on the very line of the previous studies. Indeed, it is known that the following problems characterize the power of various models of quantum interactive proofs: deciding which of the two states produced by two given quantum circuits has higher entropy is QSZK-complete [6], and checking whether the entropy of the state produced by a given quantum circuit is larger than a given value or not is NIQSZK-complete [6, 8]. Along this line, MaxOutQEA is the first entropy-related problem

that characterizes the power of quantum interactive proofs without zero-knowledge property, which may be worthy of note.

It is further proved that the class cq-QAM (i.e., the standard QAM) is necessarily contained in the one-sided bounded error version of qq-QAM of perfect completeness, denoted by qq-QAM_1 (throughout this paper, the perfect completeness version of each complexity class is indicated by adding the subscript "1").

▶ **Theorem 1.4.** cq-QAM $\subseteq$ qq-QAM_1.

One useful property when proving this theorem is that the proof of Theorem 1.1 does not harm the perfect completeness property, i.e., the equality $\mathrm{c}\cdots\mathrm{cqq\text{-}QAM}_1(m) = \mathrm{qq\text{-}QAM}_1$ also holds for any constant $m \geq 2$. Especially, the class ccqq-QAM_1 is included in the class qq-QAM_1, and thus, one has only to prove that cq-QAM is included in ccqq-QAM_1. This can be proved by combining the classical technique due to Cai [7] for proving $\mathrm{AM} = \mathrm{AM}_1$ (which itself originates in the proof of $\mathrm{BPP} \subseteq \Sigma_2^{\mathrm{P}}$ due to Lautemann [22]), and the recent result that any problem in QMA has a one-sided bounded error quantum Merlin-Arthur proof system of perfect completeness in which Arthur and Merlin initially share a constant number of EPR pairs [20] (which in particular implies that QMA is included in qq-QAM_1). Now the point is that, using two classical turns, the classical technique in Ref. [7] can be used to generate polynomially many instances of a (promise) QMA problem, all of which are QMA yes-instances if the input was a yes-instance, while at least one of which is a QMA no-instance with high probability if the input was a no-instance. Hence, by making use of the proof system in Ref. [20] for each QMA instance, which essentially runs polynomially many attempts of a protocol of qq-QAM type in parallel to check that none of them results in rejection, one obtains a proof system of ccqq-QAM type with perfect completeness.

An immediate corollary of this theorem is the first nontrivial upper bound for QAM in terms of quantum interactive proofs.

▶ **Corollary 1.5.** $\mathrm{QAM} \subseteq \mathrm{QIP}_1(2)$.

Here, $\mathrm{QIP}_1(2)$ denotes the class of problems having two-turn quantum interactive proof systems of perfect completeness. This also improves the best known lower bound of $\mathrm{QIP}_1(2)$ (from QMA shown in Ref. [20] to QAM). By using the fact $\mathrm{MQA} = \mathrm{MQA}_1$ (a.k.a., $\mathrm{QCMA} = \mathrm{QCMA}_1$) stating that classical-witness QMA systems can be made perfectly complete [15], a technique similar to the proof of Theorem 1.4 proves that perfect completeness is achievable in cc-QAM.

▶ **Theorem 1.6.** cc-QAM = cc-QAM_1.

Finally, results similar to Theorem 1.1 can be derived for other complexity classes related to generalized quantum Arthur-Merlin proof systems. Namely, the following complete characterization is proved on the power of generalized quantum Arthur-Merlin proofs involving a constant number of turns, which can be viewed as the complete set of quantum analogues of Babai's collapse theorem.

▶ **Theorem 1.7.** *The following four properties hold:*

(i) *For any constant $m \geq 3$ and any message-types $t_1, \ldots, t_m$ in $\{\mathrm{c}, \mathrm{q}\}$, if there exists an index $j \geq 3$ such that $t_j = \mathrm{q}$, then $t_m \cdots t_1$-$\mathrm{QAM}(m) = \mathrm{PSPACE}$.*

(ii) *For any constant $m \geq 2$ and any message-type t in $\{\mathrm{c}, \mathrm{q}\}$, $\mathrm{c}\cdots\mathrm{cq}t\text{-}\mathrm{QAM}(m) = \mathrm{qq\text{-}QAM}$.*

(iii) *For any constant $m \geq 2$, $\mathrm{c}\cdots\mathrm{cq\text{-}QAM}(m) = \mathrm{cq\text{-}QAM}$ $(= \mathrm{QAM})$.*

(iv) *For any constant $m \geq 2$, $\mathrm{c}\cdots\mathrm{c\text{-}QAM}(m) = \mathrm{cc\text{-}QAM}$.*

Further related work. There are several studies in which relevant subclasses of qq-QAM were treated. The class $\mathrm{QMA}^{\text{const-EPR}}$ was introduced in Ref. [20] to give an upper bound of QMA by its one-sided bounded error subclass $\mathrm{QMA}_1^{\text{const-EPR}}$ with perfect completeness. This $\mathrm{QMA}^{\text{const-EPR}}$ is an obvious subclass of qq-QAM with a restriction that the first message from the verifier consists of not polynomially many but a constant number of halves of EPR pairs. The class qq-QAM may be called $\mathrm{QMA}^{\text{poly-EPR}}$, following the notation in Ref. [20]. Another subclass of qq-QAM is the class NIQSZK studied in Refs. [18, 8] that corresponds to non-interactive quantum statistical zero-knowledge proof systems, where the zero-knowledge property must also be satisfied.

Organization of the paper. Section 2 summarizes the notions and properties that are used throughout this paper. Section 3 presents formal definitions of generalized quantum Arthur-Merlin proof systems. Section 4 provides a sketch of a proof of the qq-QAM-completeness of the CITM problem. Section 5 then proves Theorem 1.1, the collapse theorem for qq-QAM. This essentially shows the qq-QAM-hardness of the MaxOutQEA problem also. Section 6 treats the inclusion of the standard QAM in qq-QAM_1 (Theorem 1.4). Section 7 proves Theorem 1.7, the complete classification of the complexity classes derived from generalized quantum Arthur-Merlin proof systems. Finally, Section 8 concludes the paper with some open problems. A proof of the MaxOutQEA problem being in qq-QAM is provided in the appendix, which completes the proof of the qq-QAM-completeness of MaxOutQEA (Theorem 1.3). Some of the technical proofs are relegated to the full version [19] of this paper.

2 Preliminaries

Throughout this paper, let $\mathbb{N}$ and $\mathbb{Z}^+$ denote the sets of positive and nonnegative integers, respectively, and let $\Sigma = \{0,1\}$ denote the binary alphabet set. 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 any polynomially bounded function $g\colon \mathbb{Z}^+ \to \mathbb{N}$, the inequality $f(n) < 1/g(n)$ holds for all but finitely many values of n.

Quantum fundamentals. We assume the reader is familiar with the quantum formalism, including pure and mixed quantum states, density operators, and measurements, as well as the quantum circuit model (see Refs. [25, 17, 37], for instance). Some notations and properties are summarized here for later use.

For each k in $\mathbb{N}$, let $\mathbb{C}(\Sigma^k)$ denote the 2^k-dimensional complex Hilbert space whose standard basis vectors are indexed by the elements in Σ^k. In this paper, all Hilbert spaces are complex and have dimension a power of two. For a Hilbert space $\mathcal{H}$, let $\mathbf{L}(\mathcal{H})$ denote the set of linear operators over $\mathcal{H}$ (i.e., the set of linear mappings from $\mathcal{H}$ to itself), and let $\mathbf{D}(\mathcal{H})$ denote the set of density operators over $\mathcal{H}$. For Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, let $\mathbf{C}(\mathcal{H},\mathcal{K})$ denote the set of quantum channels from $\mathbf{D}(\mathcal{H})$ to $\mathbf{D}(\mathcal{K})$ (i.e., the set of linear mappings from $\mathbf{L}(\mathcal{H})$ to $\mathbf{L}(\mathcal{K})$ that are completely positive and trace-preserving). As usual, let

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

denote the two-qubit state in $\mathbb{C}(\Sigma^2)$ that forms an EPR pair, and let

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

denote the Pauli operators. For convenience, we may identify a unitary operator with the unitary transformation it induces. In particular, for a unitary operator U, the induced unitary transformation is also denoted by U.

For a linear operator A, the *trace norm* of A is defined by

$$\|A\|_{\mathrm{tr}} = \mathrm{tr}\sqrt{A^\dagger A}.$$

For a Hilbert space $\mathcal{H}$ and two quantum states ρ and σ in $\mathbf{D}(\mathcal{H})$, the *trace distance* between ρ and σ is defined by

$$D(\rho,\sigma) = \frac{1}{2}\|\rho-\sigma\|_{\mathrm{tr}}.$$

For Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$ and two quantum channels Φ and Ψ in $\mathbf{C}(\mathcal{H},\mathcal{K})$, the *minimum output trace distance* between Φ and Ψ is defined by

$$D_{\min}(\Phi,\Psi) = \min\left\{D(\Phi(\rho),\Psi(\sigma))\colon \rho,\sigma\in\mathbf{D}(\mathcal{H})\right\}.$$

The minimum output trace distance satisfies the following property. The proof is found in the full version [19] of this paper.

▶ **Lemma 2.1.** *For any Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$, any quantum channels Φ and Ψ in $\mathbf{C}(\mathcal{H},\mathcal{K})$, and any k in $\mathbb{N}$,*

$$1-\left[1-(D_{\min}(\Phi,\Psi))^2\right]^{\frac{k}{2}} \le D_{\min}\left(\Phi^{\otimes k},\Psi^{\otimes k}\right) \le k\, D_{\min}(\Phi,\Psi).$$

For any quantum state ρ, the *von Neumann entropy* of ρ is defined by

$$S(\rho) = -\,\mathrm{tr}(\rho\log\rho).$$

A special case of the von Neumann entropy is the *Shannon entropy* of a probability distribution μ, which is defined by

$$H(\mu) = S(\mu)$$

by viewing probability distributions as special cases of quantum states with diagonal density operators.

For Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$ and a quantum channel Φ in $\mathbf{C}(\mathcal{H},\mathcal{K})$, the *maximum output von Neumann entropy* of Φ is defined by

$$S_{\max}(\Phi) = \max\left\{S(\Phi(\rho))\colon \rho\in\mathbf{D}(\mathcal{H})\right\}.$$

This paper uses the following two properties on von Neumann entropy.

The first lemma provides an upper bound on the von Neumann entropy of a mixture of quantum states [25, Theorem 11.10].

▶ **Lemma 2.2.** *For any Hilbert space $\mathcal{H}$ and any quantum state ρ in $\mathbf{D}(\mathcal{H})$ such that $\rho=\sum_j \mu_j\rho_j$ for some probability distribution $\mu=\{\mu_j\}$ and quantum states ρ_j in $\mathbf{D}(\mathcal{H})$,*

$$S(\rho) \le H(\mu) + \sum_j \mu_j\, S(\rho_j).$$

The second lemma describes relations between the von Neumann entropy of a quantum state and the trace distance between the state and the totally mixed state (a similar statement appeared in the full version of Ref. [8] without a proof). The proof of the statement described here is found in the full version [19] of this paper.

▶ **Lemma 2.3.** *For any quantum state ρ of n qubits, it holds that*

$$\left(1-D\left(\rho,(I/2)^{\otimes n}\right)-2^{-n}\right)n \le S(\rho) \le n - \log\frac{1}{1-D(\rho,(I/2)^{\otimes n})} + 2.$$

Quantum circuits. Following conventions, this paper defines quantum Arthur-Merlin proof systems in terms of quantum circuits. In particular, this paper uses the following notion of polynomial-time uniformly generated families of quantum circuits.

A *quantum circuit* is specified by a series of quantum gates, each of which is applied to some designated set of qubits. It is assumed that any quantum circuit is composed of gates in some reasonable, universal, finite set of quantum gates. A *description* of a quantum circuit is a string in Σ^* that encodes the specification of the quantum circuit. The encoding must be a "natural" one, i.e., the number of gates in a circuit encoded is not more than the length of the description of that circuit, and each gate of the circuit is specifiable by a deterministic procedure in time polynomial with respect to the length of the description.

A family $\{Q_x\}_{x\in\Sigma^*}$ of quantum circuits is *polynomial-time uniformly generated* if there exists a polynomial-time deterministic procedure that, on input x in Σ^*, outputs a description of Q_x. For convenience, we may identify a circuit Q_x with the unitary operator it induces.

For the results in which perfect completeness is concerned, this paper assumes 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 [31] consisting of the Hadamard, i-phase-shift, and Toffoli gates, and the gate set consisting of the Hadamard, Toffoli, and NOT gates [30, 2]. Moreover, as the Hadamard transformation in a sense can be viewed as a quantum analogue of the classical operation of flipping a fair coin, our assumption would be the most natural quantum correspondence to the tacit classical assumption in randomized complexity theory that fair coins and perfect logical gates are available. Hence, the authors believe that the condition above is very reasonable and not restrictive.

Since non-unitary and unitary quantum circuits are equivalent in computational power [3], it is sufficient to treat only unitary quantum circuits, as defined above. Nevertheless, for readability, most procedures in this paper will be described using intermediate projective measurements and unitary operations conditioned on the outcome of the measurements. All of these intermediate measurements can be deferred to the end of the procedure by a standard technique so that the procedure becomes implementable with a unitary circuit.

3 Generalized quantum Arthur-Merlin proof systems

A generalized quantum Arthur-Merlin proof system consists of a polynomial-time quantum verifier and an all-powerful quantum prover. For any constant $m \geq 1$ and any message-type t_j in $\{\mathrm{c}, \mathrm{q}\}$ for each j in $\{1, \ldots, m\}$, a generalized quantum Arthur-Merlin proof system is of $t_m \cdots t_1$-*QAM type* if the message at the $(m-j+1)$st turn is quantum (resp. is restricted to classical) for each j such that $t_j = \mathrm{q}$ (resp. $t_j = \mathrm{c}$).

Formally, an m-turn quantum verifier V for generalized quantum Arthur-Merlin proof systems is a polynomial-time computable mapping of the form $V\colon \Sigma^* \to \Sigma^*$. For each x in Σ^*, $V(x)$ is interpreted as a description of a quantum circuit acting on $(q_{\mathsf{V}}(|x|) + m\, q_{\mathsf{M}}(|x|))$ qubits with a specification of a $q_{\mathsf{V}}(|x|)$-qubit quantum register V and each $q_{\mathsf{M}}(|x|)$-qubit quantum register M_j for j in $\{1, \ldots, m\}$, for some polynomially bounded functions $q_{\mathsf{V}}, q_{\mathsf{M}}\colon \mathbb{Z}^+ \to \mathbb{N}$. One of the qubits in V is designated as the output qubit. At the $(m-j+1)$st turn for any even j such that $2 \leq j \leq m-1$, V receives a message from a prover, either classical or quantum, which is stored in the quantum register M_{m-j}. When the system is of $t_m \cdots t_1$-QAM type, at the $(m-j+1)$st turn for any even j such that $2 \leq j \leq m$, if $t_j = \mathrm{c}$, V flips a fair coin $q_{\mathsf{M}}(|x|)$ times to obtain a binary string r of length $q_{\mathsf{M}}(|x|)$, then sends r to the prover, and stores r in the quantum register M_{m-j+1}, while if $t_j = \mathrm{q}$, V generates $q_{\mathsf{M}}(|x|)$ EPR

pairs $|\Phi^+\rangle^{\otimes q_{\mathsf{M}}(|x|)}$, then sends the second halves of them to the prover, and stores the first halves of them in M_{m-j+1}. Upon receiving a message at the mth turn from the prover, either classical or quantum, which is stored in the quantum register M_m, V prepares the $q_{\mathsf{V}}(|x|)$-qubit quantum register V, all the qubits of which are initialized to the $|0\rangle$ state. V then performs the final verification procedure by applying the circuit $V(x)$ to $(\mathsf{V}, \mathsf{M}_1, \ldots, \mathsf{M}_m)$ and then measuring the output qubit in the computational basis, where the outcome $|1\rangle$ is interpreted as "accept", and the outcome $|0\rangle$ is interpreted as "reject".

Similarly, an m-turn quantum prover P for generalized quantum Arthur-Merlin proof systems is a mapping from Σ^* to a sequence of $\lceil m/2 \rceil$ unitary transformations with a specification of quantum registers they acts on. No restrictions are placed on the complexity of P. For each x in Σ^*, $P(x)$ is interpreted as a sequence of $\lceil m/2 \rceil$ unitary transformations $P(x)_{2\lceil m/2 \rceil - 1}, \ldots, P(x)_3, P(x)_1$ acting on $(q_{\mathsf{M}}(|x|) + q_{\mathsf{P}}(|x|))$ qubits with a specification of a $q_{\mathsf{P}}(|x|)$-qubit quantum register P, for some polynomially bounded function $q_{\mathsf{M}} \colon \mathbb{Z}^+ \to \mathbb{N}$ and some function $q_{\mathsf{P}} \colon \mathbb{Z}^+ \to \mathbb{N}$. At the beginning of the protocol, P prepares the $q_{\mathsf{P}}(|x|)$-qubit quantum register P (and a $q_{\mathsf{M}}(|x|)$-qubit quantum register M_1 also, if m is odd). Without loss of generality, one can assume that all the qubits in P (and in M_1 when P prepares it) are initialized to the $|0\rangle$ state at the beginning of the protocol. At the $(m-j+1)$st turn for any odd j such that $1 \leq j \leq m-1$, P receives a message from the verifier, either classical or quantum, which is stored in the quantum register M_{m-j+1}. When the system is of $t_m \cdots t_1$-QAM type, at the $(m-j+1)$st turn for any odd j such that $1 \leq j \leq m$, P applies $P(x)_j$ to $(\mathsf{M}_{m-j+1}, \mathsf{P})$. If $t_j = \mathrm{c}$, P further measures each qubit in M_{m-j+1} in the computational basis. P then sends M_{m-j+1} to the verifier.

An m-turn generalized quantum Arthur-Merlin proof system Π is then specified by each message-type t_j in $\{\mathrm{c}, \mathrm{q}\}$ for j in $\{1, \ldots, m\}$ and an m-turn quantum verifier V for generalized quantum Arthur-Merlin proof systems. An m-turn quantum prover P for $t_m \cdots t_1$-QAM-type systems is *compatible* with Π if the function q_{M} of P is the same as that of V. In what follows, provers are always assumed to be compatible. For any generalized quantum Arthur-Merlin proof system Π, let $\mathrm{MAP}_x(\Pi)$ denote the *maximum acceptance probability* in Π on input x in Σ^*, which is the maximum of the acceptance probability of the verifier in Π on input x over all quantum provers compatible with Π. The complexity class $t_m \cdots t_1$-$\mathrm{QAM}(m, c, s)$ derived from generalized quantum Arthur-Merlin proof systems of $t_m \cdots t_1$-QAM type, with completeness c and soundness s, is defined as follows.

▶ **Definition 3.1.** Given a constant m in $\mathbb{N}$, functions $c, s \colon \mathbb{Z}^+ \to [0,1]$ satisfying $c > s$, and each message-type t_j in $\{\mathrm{c}, \mathrm{q}\}$ for j in $\{1, \ldots, m\}$, a promise problem $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ is in $t_m \cdots t_1$-$\mathrm{QAM}(m, c, s)$ if there exists an m-turn quantum verifier V for generalized quantum Arthur-Merlin proof systems, such that, for the $t_m \cdots t_1$-QAM-type proof system Π specified by V and for every input x in Σ^*,
(Completeness) if x is in A_{yes}, $\mathrm{MAP}_x(\Pi)$ is at least $c(|x|)$, and
(Soundness) if x is in A_{no}, $\mathrm{MAP}_x(\Pi)$ is at most $s(|x|)$.

Using this definition, the classes $t_m \cdots t_1$-$\mathrm{QAM}(m)$ and $t_m \cdots t_1$-$\mathrm{QAM}_1(m)$ of problems having generalized quantum Arthur-Merlin proof systems of $t_m \cdots t_1$-QAM type with two-sided bounded error, and those with one-sided bounded error of perfect completeness, respectively, are defined as follows.

▶ **Definition 3.2.** Given a constant m in $\mathbb{N}$ and each message-type t_j in $\{\mathrm{c}, \mathrm{q}\}$ for j in $\{1, \ldots, m\}$, a promise problem $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ is in $t_m \cdots t_1$-$\mathrm{QAM}(m)$ iff A is in $t_m \cdots t_1$-$\mathrm{QAM}(m, 1-\varepsilon, \varepsilon)$ for some negligible function $\varepsilon \colon \mathbb{Z}^+ \to [0,1]$.

▶ **Definition 3.3.** Given a constant m in $\mathbb{N}$ and each message-type t_j in $\{\mathrm{c},\mathrm{q}\}$ for j in $\{1,\ldots,m\}$, a promise problem $A=(A_{\mathrm{yes}},A_{\mathrm{no}})$ is in $t_m\cdots t_1$-$\mathrm{QAM}_1(m)$ iff A is in $t_m\cdots t_1$-$\mathrm{QAM}(m,1,\varepsilon)$ for some negligible function $\varepsilon\colon\mathbb{Z}^+\to[0,1]$.

In the case where the number of turns is clear, the parameter m may be omitted, e.g., ccqq-QAM(4) may be abbreviated as ccqq-QAM.

Similar to general quantum interactive proof systems, the perfect parallel repetition theorem holds for generalized quantum Arthur-Merlin proof systems.

▶ **Lemma 3.4.** *For any generalized quantum Arthur-Merlin proof system Π, for any k in $\mathbb{N}$ and the generalized quantum Arthur-Merlin proof system $\Pi^{\otimes k}$ resulting from the k-fold parallel repetition of Π, and for every input x in Σ^*, it holds that*

$$\mathrm{MAP}_x\big(\Pi^{\otimes k}\big)=\big(\mathrm{MAP}_x(\Pi)\big)^k.$$

Proof. Fix any number m of turns and any message-types $t_1,\ldots,t_m$ in $\{\mathrm{c},\mathrm{q}\}$. For any proof system Π of $t_m\cdots t_1$-QAM type, let $Q(\Pi)$ be the m-turn (general) quantum interactive proof system that exactly simulates Π as follows: on every input x in Σ^*, the verifier in $Q(\Pi)$ behaves exactly in the same manner as Arthur in Π except that, upon receiving the jth message from a prover (resp. sending the jth message to a prover), if $t_j=\mathrm{c}$ in Π, the verifier of $Q(\Pi)$ first makes sure that the received message (resp. the sent message) is indeed classical by taking a copy of the message by CNOT operations (and the copied message will never be touched in the rest of the protocol). Clearly, it is meaningless for a malicious prover in $Q(\Pi)$ to send a quantum message when the original message-type was classical in Π. Therefore, for every input x, the maximum acceptance probability in $Q(\Pi)$ is exactly $\mathrm{MAP}_x(\Pi)$. Now from the perfect parallel repetition theorem for general quantum interactive proofs [11], the k-fold parallel repetition $(Q(\Pi))^{\otimes k}$ of $Q(\Pi)$ has its maximum acceptance probability exactly $\big(\mathrm{MAP}_x(\Pi)\big)^k$ for every x. As the proof system $(Q(\Pi))^{\otimes k}$ is identical to the m-turn (general) quantum interactive proof system $Q(\Pi^{\otimes k})$ that exactly simulates the proof system $\Pi^{\otimes k}$ of $t_m\cdots t_1$-QAM type that is the k-fold parallel repetition of Π, it holds that $\mathrm{MAP}_x\big(\Pi^{\otimes k}\big)=\big(\mathrm{MAP}_x(\Pi)\big)^k$ for every x, as claimed. ◀

Using Lemma 3.4, one can show the following amplification properties on generalized quantum Arthur-Merlin proof systems, which ensure that Definitions 3.2 and 3.3 give a robust definition in terms of completeness and soundness parameters.

▶ **Lemma 3.5.** *For any constant m in $\mathbb{N}$, any message-types $t_1,\ldots,t_m$ in $\{\mathrm{c},\mathrm{q}\}$, any polynomially bounded function $p\colon\mathbb{Z}^+\to\mathbb{N}$, and any polynomial-time computable functions $c,s\colon\mathbb{Z}^+\to[0,1]$ satisfying $c-s\geq\frac{1}{q}$ for some polynomially bounded function $q\colon\mathbb{Z}^+\to\mathbb{N}$,*

$$t_m\cdots t_1\text{-}\mathrm{QAM}(m,c,s)\subseteq t_m\cdots t_1\text{-}\mathrm{QAM}(m,1-2^{-p},2^{-p}).$$

▶ **Lemma 3.6.** *For any constant m in $\mathbb{N}$, any message-types $t_1,\ldots,t_m$ in $\{\mathrm{c},\mathrm{q}\}$, any polynomially bounded function $p\colon\mathbb{Z}^+\to\mathbb{N}$, and any polynomial-time computable function $s\colon\mathbb{Z}^+\to[0,1]$ satisfying $1-s\geq\frac{1}{q}$ for some polynomially bounded function $q\colon\mathbb{Z}^+\to\mathbb{N}$,*

$$t_m\cdots t_1\text{-}\mathrm{QAM}(m,1,s)\subseteq t_m\cdots t_1\text{-}\mathrm{QAM}(m,1,2^{-p}).$$

Proofs of Lemmas 3.5 and 3.6 (Sketch). Lemma 3.6 is immediate from Lemma 3.4 by considering a parallel repetition of an appropriately many number of times.

To prove Lemma 3.5, as in Refs. [1, 21, 14], one first makes the completeness exponentially close to one, while keeping the soundness bounded away from one, by performing a sufficiently

Verifier's qq-QAM Protocol for CITM(a, b)

1. Prepare q_{out}-qubit registers S_1 and S_2, and generate q_{out} EPR pairs $|\Phi^+\rangle^{\otimes q_{\text{out}}}$ in $(\mathsf{S}_1, \mathsf{S}_2)$ so that the jth qubit of S_1 and that of S_2 form an EPR pair, for every j in $\{1, \ldots, q_{\text{out}}\}$. Send S_2 to the prover.
2. Receive a $(q_{\text{all}} - q_{\text{out}})$-qubit quantum register R from the prover. Apply the unitary transformation $U_{Q_x}^\dagger$ to $(\mathsf{R}, \mathsf{S}_1)$. Accept if all the qubits in A are in state $|0\rangle$, and reject otherwise, where A is the quantum register consisting of the last $(q_{\text{all}} - q_{\text{in}})$ qubits of $(\mathsf{R}, \mathsf{S}_1)$ (i.e., the non-input qubits of Q_x).

Figure 1 Verifier's qq-QAM protocol for CITM.

many number of attempts of a given system in parallel and accepting only when a reasonably large fraction of the attempts results in acceptance. Lemma 3.5 is then immediate from Lemma 3.4 by running this system of almost-perfect completeness in parallel appropriately many times. The rigorous proof is found in the full version [19] of this paper. ◀

4 qq-QAM-completeness of CITM

This section proves Theorem 1.2, which states that the CITM problem is complete for the class qq-QAM.

First, it is proved that CITM(a, b) is in qq-QAM for appropriately chosen parameters a and b. The proof is a special case of the proof of the Close Image problem being in QIP(2) [32, 12].

▶ **Lemma 4.1.** *For any constants a and b in $[0, 1]$ satisfying $(1-a)^2 > 1-b^2$,* CITM(a, b) *is in* qq-QAM.

Proof (Sketch). Let Q_x be a quantum circuit of an instance x of CITM(a, b) acting on q_{all} qubits with q_{in} specified input qubits and q_{out} specified output qubits. Without loss of generality, one can assume that the first q_{in} qubits correspond to the input qubits, and the last q_{out} qubits correspond to the output qubits. Let U_{Q_x} denote the unitary operator induced by Q_x. We construct a verifier V of the qq-QAM proof system with completeness $(1-a)^2$ and soundness $1-b^2$ as follows (recall that a and b are constants in the interval $[0, 1]$ such that $(1-a)^2 > 1-b^2$, and thus this qq-QAM proof system is sufficient for the claim).

Let S_1 and S_2 be quantum registers of q_{out} qubits. The verifier V first generates q_{out} EPR pairs $|\Phi^+\rangle^{\otimes q_{\text{out}}}$ in $(\mathsf{S}_1, \mathsf{S}_2)$ so that the jth qubit of S_1 and that of S_2 form an EPR pair, for every j in $\{1, \ldots, q_{\text{out}}\}$. Then V sends S_2 to the prover. Upon receiving a quantum register R of $(q_{\text{all}} - q_{\text{out}})$ qubits, V applies the unitary transformation $U_{Q_x}^\dagger$ to $(\mathsf{R}, \mathsf{S}_1)$. Letting A be the quantum register consisting of the last $(q_{\text{all}} - q_{\text{in}})$ qubits of the register $(\mathsf{R}, \mathsf{S}_1)$ (i.e., corresponding to the *non-input* qubits of Q_x), V accepts x if and only if all the qubits in A are in state $|0\rangle$. Figure 1 summarizes the protocol of the verifier V.

The claim follows from a rigorous analysis of this protocol, which is relegated to the full version [19] of this paper. ◀

Now the CITM problem is proved to be hard for qq-QAM.

▶ **Lemma 4.2.** *For any constants a and b satisfying $0 < a < b < 1$,* CITM(a, b) *is hard for* qq-QAM *under polynomial-time many-one reduction.*

Algorithm Corresponding to Quantum Circuit Q_x

1. Prepare quantum registers V and M, each of q_{V} and q_{M} qubits, respectively. Denote by S and $\overline{\mathsf{S}}$ the quantum registers consisting of the last q_{S} and first $(q_{\mathsf{V}} - q_{\mathsf{S}})$ qubits of V, respectively. The last $(q_{\mathsf{S}} + q_{\mathsf{M}})$ qubits of $(\mathsf{V}, \mathsf{M}) = (\overline{\mathsf{S}}, \mathsf{S}, \mathsf{M})$ (i.e., all the qubits in (S, M)) are designated as the input qubits, while the last q_{S} qubits of $\mathsf{V} = (\overline{\mathsf{S}}, \mathsf{S})$ (i.e., all the qubits in S) are designated as the output qubits.
2. Flip a fair coin, and proceed to Step 2.a if it results in "Heads", and proceed to Step 2.b if it results in "Tails".
   a. Output all the qubits in S.
   b. Perform V_x over $(\mathsf{V}, \mathsf{M}) = (\overline{\mathsf{S}}, \mathsf{S}, \mathsf{M})$. If the first qubit of V is in state $|1\rangle$, output the totally mixed state $(I/2)^{\otimes q_{\mathsf{S}}}$ (by first generating the totally mixed state using fresh ancillae, and then swapping the qubits in S with the generated totally mixed state), and output $|0\rangle^{\otimes q_{\mathsf{S}}}$ otherwise (by swapping the qubits in S with q_{S} fresh ancillae).

Figure 2 The construction of the quantum circuit Q_x.

Proof (Sketch). Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a problem in qq-QAM. Then A has a qq-QAM proof system with completeness c and soundness s for some appropriately chosen constants c and s satisfying $0 < s < c < 1$. Let V be the quantum verifier witnessing this proof system. Fix an input x, and let V and M be quantum registers consisting of q_{V} and q_{M} qubits, respectively, where V corresponds to the private qubits of V and M corresponds to the message qubits V would receive on input x. Without loss of generality, one can assume that the first qubit of V is the output qubit of V, and the last q_{S} qubits of V form the quantum register S corresponding to the halves of the EPR pairs V would keep until the final verification procedure is performed. Let $\overline{\mathsf{S}}$ be the quantum register of $(q_{\mathsf{V}} - q_{\mathsf{S}})$ qubits consisting of the first $(q_{\mathsf{V}} - q_{\mathsf{S}})$ qubits of V (i.e., all the private qubits of V but those belonging to S). Denote by V_x the unitary operator induced by this V on input x.

We construct a quantum circuit Q_x that exactly implements the following algorithm. The circuit Q_x expects to receive a $(q_{\mathsf{S}} + q_{\mathsf{M}})$-qubit state as its input, and prepares the quantum registers $\mathsf{V} = (\overline{\mathsf{S}}, \mathsf{S})$ and M, where the input state is expected to be stored in (S, M). Then with probability one-half, Q_x just outputs the state in the register S. Otherwise Q_x performs V_x over $(\mathsf{V}, \mathsf{M}) = (\overline{\mathsf{S}}, \mathsf{S}, \mathsf{M})$, and outputs the totally mixed state $(I/2)^{\otimes q_{\mathsf{S}}}$ if the first qubit of V is in state $|1\rangle$ (i.e., if the system is in an accepting state of the original verifier V), and outputs $(|0\rangle\langle 0|)^{\otimes q_{\mathsf{S}}}$ if the first qubit of V is in state $|0\rangle$ (i.e., if the system is in a rejecting state of the original verifier V). Figure 2 summarizes the construction of the circuit Q_x.

The qq-QAM-hardness of $\mathrm{CITM}(a, 1/20)$ for any positive constant $a < 1/20$ follows from a rigorous analysis of the properties of this circuit by appropriately choosing c and s, which is found in the full version [19] of this paper. The qq-QAM-hardness of $\mathrm{CITM}(a, b)$ for any constants a and b satisfying $0 < a < b < 1$ then follows from Lemma 2.1 by first creating an instance Q_x of $\mathrm{CITM}(a/k, 1/20)$ according to the construction above, for $k = \lceil 2\frac{\ln(1/(1-b))}{\ln(400/399)} \rceil$, and then constructing another circuit Q'_x that places k copies of Q_x in parallel. ◀

From Lemmas 4.1 and 4.2, Theorem 1.2 follows. Note that, with essentially the same proofs as those of Lemmas 4.1 and 4.2, one can show that for any b in $(0, 1)$, $\mathrm{CITM}(0, b)$ is in qq-QAM_1 and is hard for qq-QAM_1, and thus, the following corollary holds.

▶ **Corollary 4.3.** *For any constant b in $(0, 1)$, $\mathrm{CITM}(0, b)$ is qq-QAM_1-complete under polynomial-time many-one reduction.*

▶ Remark. The proofs of Lemmas 4.1 and 4.2 actually also show that the variant of the CITM problem where the number of output qubits of the circuit is a fixed constant independent of instances is complete for the class $\mathrm{QMA}^{\text{const-EPR}}$ introduced in Ref. [20], and thus, it is QMA-complete since $\mathrm{QMA}^{\text{const-EPR}} = \mathrm{QMA}$ [5].

5 Collapse theorem for qq-QAM

This section proves Theorem 1.1, the quantum analogue of Babai's collapse theorem [4] stating that $\mathrm{c}\cdots\mathrm{cqq\text{-}QAM}(m) = \mathrm{qq\text{-}QAM}$ for any constant $m \geq 2$.

First, it is proved that for any constant $m \geq 4$, $\mathrm{c}\cdots\mathrm{cqq\text{-}QAM}(m) \subseteq \mathrm{ccqq\text{-}QAM}$ holds, meaning that the first $(m-4)$ classical turns can be removed. The proof essentially relies on the observation that the techniques used in the classical result by Babai [4] can be applied to the quantum setting as well.

▶ **Lemma 5.1.** *For any constant $m \geq 4$, $\mathrm{c}\cdots\mathrm{cqq\text{-}QAM}(m) \subseteq \mathrm{ccqq\text{-}QAM}$.*

Proof. It suffices to show that $\mathrm{c}\cdots\mathrm{cqq\text{-}QAM}(m) \subseteq \mathrm{c}\cdots\mathrm{cqq\text{-}QAM}(m-1)$ for any odd constant $m \geq 5$, and $\mathrm{c}\cdots\mathrm{cqq\text{-}QAM}(m) \subseteq \mathrm{c}\cdots\mathrm{cqq\text{-}QAM}(m-2)$ for any even constant $m \geq 6$.

Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a problem in $\mathrm{c}\cdots\mathrm{cqq\text{-}QAM}(m)$. By Lemma 3.5, A has an m-turn $\mathrm{c}\cdots\mathrm{cqq\text{-}QAM}$ proof system Π with completeness $1-2^{-8}$ and soundness 2^{-8}. Without loss of generality, one can assume that, for every input of length n, every classical message exchanged consists of $l(n)$ bits for some polynomially bounded function $l\colon \mathbb{Z}^+ \to \mathbb{N}$.

First consider the case with odd m, where the first turn is for the prover. Fix an input x in Σ^*, and let $w_x(y,r)$ be the maximum of the probability that the prover can make the verifier accept, under the condition that the first message from the prover is y in $\Sigma^{l(|x|)}$ and the second message from the verifier is r in $\Sigma^{l(|x|)}$. Then, the maximum acceptance probability in Π is given by $\mathrm{MAP}_x(\Pi) = \max_{y\in\Sigma^{l(|x|)}}\{\mathrm{E}[w_x(y,r)]\}$, where the expectation is taken over the uniform distribution with respect to r in $\Sigma^{l(|x|)}$. Note that $\mathrm{MAP}_x(\Pi) \geq 1-2^{-8}$ if x is in A_{yes}, and $\mathrm{MAP}_x(\Pi) \leq 2^{-8}$ if x is in A_{no}.

Consider the $(m-1)$-turn $\mathrm{c}\cdots\mathrm{cqq\text{-}QAM}$ proof system Π' specified by the following protocol of the verifier: At the first turn, the verifier sends $k(|x|)$ strings $r_1,\ldots,r_{k(|x|)}$ chosen uniformly at random from $\Sigma^{l(|x|)}$, for some polynomially bounded function $k\colon \mathbb{Z}^+ \to \mathbb{N}$. Upon receiving a string y in $\Sigma^{l(|x|)}$ and $k(|x|)$ strings $z_1,\ldots,z_{k(|x|)}$ in $\Sigma^{l(|x|)}$ at the third turn, the verifier enters the simulations of the last $(m-3)$ turns of communications of Π, by running in parallel $k(|x|)$ attempts of such simulations, where the jth attempt assumes that the first three messages in the original proof system Π were y, r_j, and z_j, respectively, for each j in $\{1,\ldots,k(|x|)\}$. The verifier accepts if and only if more than $k(|x|)/2$ attempts result in acceptance in these simulations of Π. Figure 3 summarizes the protocol of this verifier in Π'.

In fact, the construction of this proof system Π' is exactly the same as in Ref. [4] except that the last two messages exchanged are quantum and the final verification of the verifier is a polynomial-time quantum computation in the present case. The analysis in Ref. [4] works also in the present case, since it only relies on the fact that $w_x(y,r)$ gives the conditional probability defined above, and from Lemma 3.4, the perfect parallel repetition theorem holds for general quantum Arthur-Merlin proof systems. In particular, the following property holds also in the present case (see Lemmas 3.3 and 3.4 of Ref. [4]).

▶ **Claim 1.** $1-2^{k(|x|)}\big(1-\mathrm{MAP}_x(\Pi)\big)^{k(|x|)/2} \leq \mathrm{MAP}_x(\Pi') \leq 2^{k(|x|)+l(|x|)}\big(\mathrm{MAP}_x(\Pi)\big)^{k(|x|)/2}$.

Verifier's Protocol for Reducing the Number of Turns by One (for Odd m)

1. Send $k(|x|)$ strings $r_1, \ldots, r_{k(|x|)}$, each chosen uniformly at random from $\Sigma^{l(|x|)}$, to the prover, for some polynomially bounded function $k\colon \mathbb{Z}^+ \to \mathbb{N}$.
2. Receive a string y in $\Sigma^{l(|x|)}$ and $k(|x|)$ strings $z_1, \ldots, z_{k(|x|)}$ in $\Sigma^{l(|x|)}$ from the prover. Run in parallel $k(|x|)$ attempts of the $(m-3)$-turn protocol that simulates the last $(m-3)$ turns of communications of the original m-turn c$\cdots$cqq-QAM proof system Π on input x, where the jth attempt assumes that the first three messages in Π were y, r_j, and z_j, respectively, for each j in $\{1, \ldots, k(|x|)\}$. Accept if more than $k(|x|)/2$ attempts result in acceptance in these simulations of Π, and reject otherwise.

Figure 3 Verifier's protocol in Π' for reducing the number of turns by one when m is odd.

Now let $k = \lceil \frac{2+l}{3} \rceil$. If x is in A_{yes}, then $\text{MAP}_x(\Pi')$ is at least

$$1 - 2^{k(|x|)}\big(1 - \text{MAP}_x(\Pi)\big)^{k(|x|)/2} \geq 1 - 2^{k(|x|)}\big(2^{-8}\big)^{k(|x|)/2} \geq 1 - \frac{1}{2^{l(|x|)+2}} \geq \frac{3}{4},$$

while if x is in A_{no}, then $\text{MAP}_x(\Pi')$ is at most

$$2^{k(|x|)+l(|x|)}\big(\text{MAP}_x(\Pi)\big)^{k(|x|)/2} \leq 2^{k(|x|)+l(|x|)}\big(2^{-8}\big)^{k(|x|)/2} \leq \frac{1}{4},$$

which completes the proof for the case with odd m.

Next consider the case with even m, where the first message is a random string from a verifier. Let $\Pi^{(-1)}$ be the $(m-1)$-turn c$\cdots$cqq-QAM proof system that on input (x, r) simulates the last $(m-1)$ turns of Π on x under the condition that the first message in Π was r in $\Sigma^{l(|x|)}$. Let $B = (B_{\text{yes}}, B_{\text{no}})$ be the following promise problem in c$\cdots$cqq-QAM$(m-1)$:

$$B_{\text{yes}} = \big\{(x,r)\colon \text{MAP}_{(x,r)}\big(\Pi^{(-1)}\big) \geq 2/3\big\}, \quad B_{\text{no}} = \big\{(x,r)\colon \text{MAP}_{(x,r)}\big(\Pi^{(-1)}\big) \leq 1/3\big\}.$$

Note that, if x is in A_{yes}, then (x, r) is in B_{yes} for at least $(1 - 3 \cdot 2^{-8})$-fraction of the choices of r. Similarly, if x is in A_{no}, then (x, r) is in B_{no} for at least $(1 - 3 \cdot 2^{-8})$-fraction of the choices of r. By the result for the case with odd m above, it holds that B is in c$\cdots$cqq-QAM$(m-2)$. Thus, there exists an $(m-2)$-turn c$\cdots$cqq-QAM proof system $\Pi^{(-2)}$ for B such that if (x, r) is in B_{yes}, $\text{MAP}_{(x,r)}\big(\Pi^{(-2)}\big)$ is at least $2/3$, while if (x, r) is in B_{no}, $\text{MAP}_{(x,r)}\big(\Pi^{(-2)}\big)$ is at most $1/3$. Note that the first turn of $\Pi^{(-2)}$ is a turn for the verifier, and thus, one can merge the turn for sending r with the first turn of $\Pi^{(-2)}$. This results in an $(m-2)$-turn c$\cdots$cqq-QAM proof system Π'' for A in which at the first turn the new verifier sends a string r in $\Sigma^{l(|x|)}$ chosen uniformly at random in addition to the original first message of the verifier in $\Pi^{(-2)}$ on input (x, r), and then behaves exactly in the same manner as the verifier in $\Pi^{(-2)}$ on input (x, r) in the rest of the protocol. If x is in A_{yes}, $\text{MAP}_x(\Pi'')$ is at least $(1 - 3 \cdot 2^{-8}) \cdot (2/3) > 5/8$, while if x is in A_{no}, $\text{MAP}_x(\Pi'')$ is at most $3 \cdot 2^{-8} + (1 - 3 \cdot 2^{-8}) \cdot (1/3) < 3/8$, which is sufficient for the claim, due to Lemma 3.5. ◀

Second, using the fact that CITM is qq-QAM-complete, it is proved that cqq-QAM is included in qq-QAM.

▶ **Lemma 5.2.** cqq-QAM $\subseteq$ qq-QAM.

Proof. Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a problem in cqq-QAM. Then, A has a cqq-QAM proof system Π with completeness $2/3$ and soundness $1/3$. Let $l\colon \mathbb{Z}^+ \to \mathbb{N}$ be the polynomially bounded function that specifies the length of the first message in Π. Consider the qq-QAM

proof system Π^{qq} that on input (x,w) simulates the last two turns of Π on x under the condition that the first message in Π was w in $\Sigma^{l(|x|)}$. Let $B=(B_{\mathrm{yes}},B_{\mathrm{no}})$ be the following promise problem in qq-QAM:

$$B_{\mathrm{yes}}=\big\{(x,w)\colon \mathrm{MAP}_{(x,w)}\big(\Pi^{\mathrm{qq}}\big)\geq 2/3\big\},\quad B_{\mathrm{no}}=\big\{(x,w)\colon \mathrm{MAP}_{(x,w)}\big(\Pi^{\mathrm{qq}}\big)\leq 1/3\big\}.$$

Note that for any x, if x is in A_{yes}, there exists a string w in $\Sigma^{l(|x|)}$ such that (x,w) is in B_{yes}, and if x is in A_{no}, for every string w in $\Sigma^{l(|x|)}$, (x,w) is in B_{no}.

Let $p\colon \mathbb{Z}^+\to\mathbb{N}$ be a non-decreasing polynomially bounded function, which will be fixed later. First notice that B has a qq-QAM proof system that satisfies completeness $1-2^{-p}$ and soundness 2^{-p} (the existence of such a proof system is ensured by Lemma 3.5). Starting from this qq-QAM proof system, the proof of Lemma 4.2 implies the existence of a polynomial-time algorithm that, given (x,w), computes a description of a quantum circuit $Q_{x,w}$ of $q_{\mathrm{in}}(|x|)$ input qubits and $q_{\mathrm{out}}(|x|)$ output qubits with the following properties:

- **(i)** if (x,w) is in B_{yes}, there exists a quantum state ρ consisting of $q_{\mathrm{in}}(|x|)$ qubits such that $D\big(Q_{x,w}(\rho),(I/2)^{\otimes\, q_{\mathrm{out}}(|x|)}\big)\leq 2^{-p(|x|+|w|)-1}<2^{-p(|x|)}$, and
- **(ii)** if (x,w) is in B_{no}, for any quantum state ρ consisting of $q_{\mathrm{in}}(|x|)$ qubits, it holds that $D\big(Q_{x,w}(\rho),(I/2)^{\otimes\, q_{\mathrm{out}}(|x|)}\big)>1/20$.

Let $q\colon\mathbb{Z}^+\to\mathbb{N}$ be another non-decreasing polynomially bounded function satisfying $q(n)\geq\max\{l(n)+4,n\}$ for any n in $\mathbb{Z}^+$. Considering the quantum circuit $Q'_{x,w}$ that runs $k(|x|)$ copies of $Q_{x,w}$ in parallel for the polynomially bounded function $k=\lceil\frac{2\ln 2}{\ln(400/399)}q\rceil$ and taking $p=q+\lceil\log k\rceil$, it follows from Lemma 2.1 (with Φ being the transformation induced by $Q_{x,w}$ and Ψ being the transformation that receives an input state of $q_{\mathrm{in}}(|x|)$ qubits and always outputs the totally mixed state $(I/2)^{\otimes\, q_{\mathrm{out}}(|x|)}$ regardless of the input) that

- **(i)** if x is in A_{yes}, there exist a string w in $\Sigma^{l(|x|)}$ and a quantum state ρ' consisting of $q'_{\mathrm{in}}(|x|)$ qubits such that $D\big(Q'_{x,w}(\rho'),(I/2)^{\otimes\, q'_{\mathrm{out}}(|x|)}\big)<2^{-q(|x|)}$, and
- **(ii)** if x is in A_{no}, for any string w in $\Sigma^{l(|x|)}$ and any quantum state ρ' consisting of $q'_{\mathrm{in}}(|x|)$ qubits, it holds that $D\big(Q'_{x,w}(\rho'),(I/2)^{\otimes\, q'_{\mathrm{out}}(|x|)}\big)>1-2^{-q(|x|)}$,

where $q'_{\mathrm{in}}=kq_{\mathrm{in}}$ and $q'_{\mathrm{out}}=kq_{\mathrm{out}}$.

Now consider the quantum circuit R_x of $\big(l(|x|)+q'_{\mathrm{in}}(|x|)\big)$ input qubits and $q'_{\mathrm{out}}(|x|)$ output qubits that corresponds to the following algorithm:

1. Measure all the $l(|x|)$ qubits in the quantum register W in the computational basis to obtain a classical string w in $\Sigma^{l(|x|)}$, where W corresponds to the first $l(|x|)$ qubits of the input qubits.
2. Compute from (x,w) a description of the quantum circuit $Q'_{x,w}$. Perform the circuit $Q'_{x,w}$ with qubits in the quantum register R as its input qubits, where R corresponds to the last $q'_{\mathrm{in}}(|x|)$ qubits of the input qubits of R_x. Output the qubits corresponding to the output qubits of $Q'_{x,w}$.

We claim that the circuit R_x satisfies the following two properties:

- **(i)** if x is in A_{yes}, there exists a quantum state σ consisting of $\big(l(|x|)+q'_{\mathrm{in}}(|x|)\big)$ qubits such that $D\big(R_x(\sigma),(I/2)^{\otimes\, q'_{\mathrm{out}}(|x|)}\big)<2^{-q(|x|)}$, and
- **(ii)** if x is in A_{no}, for any quantum state σ consisting of $\big(l(|x|)+q'_{\mathrm{in}}(|x|)\big)$ qubits, it holds that $D\big(R_x(\sigma),(I/2)^{\otimes\, q'_{\mathrm{out}}(|x|)}\big)>1/\,q'_{\mathrm{out}}(|x|)$.

In fact, the item (i) is obvious from the construction of R_x.

To prove the item (ii), suppose that x is in A_{no}. Then, for any string w in $\Sigma^{l(|x|)}$ and any quantum state ρ' of $q'_{\mathrm{in}}(|x|)$ qubits, it holds that $D\big(Q'_{x,w}(\rho'),(I/2)^{\otimes\, q'_{\mathrm{out}}(|x|)}\big)>1-2^{-q(|x|)}$.

From Lemma 2.2 and the second inequality of Lemma 2.3, it follows that

$$S(R_x(\sigma)) < l(|x|)+q'_{\mathrm{out}}(|x|)-q(|x|)+2 \leq q'_{\mathrm{out}}(|x|)-2 \leq \left(1-\frac{1}{q'_{\mathrm{out}}(|x|)}-2^{-q'_{\mathrm{out}}(|x|)}\right) q'_{\mathrm{out}}(|x|).$$

Hence, the first inequality of Lemma 2.3 ensures that $D\bigl(R_x(\sigma), (I/2)^{\otimes\, q'_{\mathrm{out}}(|x|)}\bigr) > 1/\, q'_{\mathrm{out}}(|x|)$.

Finally, consider the quantum circuit R'_x that runs $k'(|x|)$ copies of R_x in parallel for the polynomially bounded function $k' = \bigl\lceil \frac{2\ln(1/2)}{\ln(1-(1/(q'_{\mathrm{out}})^2))} \bigr\rceil \leq 2(q'_{\mathrm{out}})^2$. Assuming that $\bigl(q'_{\mathrm{out}}(|x|)\bigr)^2 \leq 2^{q(|x|)-4}$ (otherwise $|x|$ is at most some fixed constant since q'_{out} is a polynomially bounded function and $q(|x|) \geq |x|$, and thus, it can be checked trivially whether x is in A_{yes} or in A_{no}), it follows from Lemma 2.1 that

(i) if x is in A_{yes}, there exists a quantum state σ consisting of $q''_{\mathrm{in}}(|x|)$ qubits such that $D\bigl(R'_x(\sigma), (I/2)^{\otimes\, q''_{\mathrm{out}}(|x|)}\bigr) < 1/8$, and

(ii) if x is in A_{no}, for any quantum state σ consisting of $q''_{\mathrm{in}}(|x|)$ qubits, it holds that $D\bigl(R'_x(\sigma), (I/2)^{\otimes\, q''_{\mathrm{out}}(|x|)}\bigr) > 1/2$,

where $q''_{\mathrm{in}} = k'(l + q'_{\mathrm{in}})$ and $q''_{\mathrm{out}} = k'q'_{\mathrm{out}}$.

Thus, R'_x is a yes-instance of CITM$(1/8, 1/2)$ if x is in A_{yes}, while R'_x is a no-instance of CITM$(1/8, 1/2)$ if x is in A_{no}. This implies that any problem A in cqq-QAM is reducible to CITM$(1/8, 1/2)$ in polynomial time, and thus in qq-QAM by Lemma 4.1, which completes the proof. ◀

▶ Remark. Combined with Lemma 2.3, the reduction from the problem B to the circuit $Q'_{x,w}$ in the proof of Lemma 5.2 essentially shows the qq-QAM-hardness of the MaxOutQEA problem. On the other hand, the fact that MaxOutQEA is in qq-QAM is easily proved by a straightforward modification of the arguments in Refs. [6, 8] that place the Quantum Entropy Approximation (QEA) problem in NIQSZK. Hence, the MaxOutQEA problem is also qq-QAM-complete, giving Theorem 1.3. A rigorous proof of MaxOutQEA being in qq-QAM is presented in Appendix A, and a separate proof of the qq-QAM-hardness of MaxOutQEA is found in the full version [19] of this paper.

Finally, using Lemma 5.2, it is proved that ccqq-QAM $\subseteq$ qq-QAM.

▶ **Lemma 5.3.** ccqq-QAM $\subseteq$ qq-QAM.

Proof. Let $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ be a problem in ccqq-QAM. By Lemma 3.5, one can assume that A has a ccqq-QAM proof system Π with completeness $1 - 2^{-8}$ and soundness 2^{-8}. Let $l\colon \mathbb{Z}^+ \to \mathbb{N}$ be the polynomially bounded function that specifies the length of the first message in Π. Consider the cqq-QAM proof system $\Pi^{(-1)}$ that on input (x, r) simulates the last three turns of Π on x assuming that the first message in Π was r in $\Sigma^{l(|x|)}$. Let $B = (B_{\mathrm{yes}}, B_{\mathrm{no}})$ be the following promise problem in cqq-QAM:

$$B_{\mathrm{yes}} = \bigl\{(x,r)\colon \mathrm{MAP}_{(x,r)}\bigl(\Pi^{(-1)}\bigr) \geq 2/3\bigr\}, \quad B_{\mathrm{no}} = \bigl\{(x,r)\colon \mathrm{MAP}_{(x,r)}\bigl(\Pi^{(-1)}\bigr) \leq 1/3\bigr\}.$$

Note that, if x is in A_{yes}, then (x, r) is in B_{yes} for at least $(1 - 3 \cdot 2^{-8})$-fraction of the choices of r, while if x is in A_{no}, then (x, r) is in B_{no} for at least $(1 - 3 \cdot 2^{-8})$-fraction of the choices of r. By Lemma 5.2, it holds that B is in qq-QAM. Thus, there exists a qq-QAM proof system Π' for B such that $\mathrm{MAP}_{(x,r)}(\Pi')$ is at least $2/3$ if (x, r) is in B_{yes}, while $\mathrm{MAP}_{(x,r)}(\Pi')$ is at most $1/3$ if (x, r) is in B_{no}. Here, the first turn of Π' is a turn for the verifier, and thus one can merge the turn for sending r with the first turn of Π'. This results in another qq-QAM proof system Π'' for A in which at the first turn the new verifier sends a string r in $\Sigma^{l(|x|)}$ chosen uniformly at random in addition to the original first message of the verifier

in Π' on input (x, r), and then behaves exactly in the same manner as the verifier in Π' on input (x, r) in the rest of the protocol. Notice that sending a random string r of length $l(|x|)$ can be exactly simulated by sending the halves of $l(|x|)$ EPR pairs and measuring in the computational basis all the remaining halves of them that the verifier possesses. If x is in A_{yes}, $\text{MAP}_x(\Pi'')$ is at least $(1 - 3 \cdot 2^{-8}) \cdot (2/3) > 5/8$, while if x is in A_{no}, $\text{MAP}_x(\Pi'')$ is at most $3 \cdot 2^{-8} + (1 - 3 \cdot 2^{-8}) \cdot (1/3) < 3/8$, which is sufficient for the claim, due to Lemma 3.5. ◀

Now one inclusion of Theorem 1.1 is immediate from Lemmas 5.1 and 5.3, and the other inclusion is trivial, which completes the proof of Theorem 1.1.

In fact, all the proofs of Lemmas 5.1, 5.2, and 5.3 can be easily modified to preserve the perfect completeness property, and the following corollary holds.

▶ **Corollary 5.4.** *For any constant $m \geq 2$, $\text{c} \cdots \text{cqq-QAM}_1(m) = \text{qq-QAM}_1$.*

Proof. The proof of Lemma 5.1 can be modified so that it preserves the perfect completeness property by taking B_{yes} to be the set of (x, r)'s such that $\text{MAP}_{(x,r)}\left(\Pi^{(-1)}\right)$ is one, and using Lemma 3.6 instead of Lemma 3.5. This shows that $\text{c} \cdots \text{cqq-QAM}_1(m)$ is included in ccqq-QAM_1 for any constant $m \geq 4$. With a similar modification to the set B_{yes} as well as using Corollary 4.3 instead of Theorem 1.2, the proof of Lemma 5.2 can be modified to present a reduction from any problem in cqq-QAM_1 to $\text{CITM}(0, b)$, which shows that cqq-QAM_1 is included in qq-QAM_1. Using this inclusion instead of Lemma 5.2 and again with a similar modification to B_{yes} and a replacement of Lemma 3.5 by Lemma 3.6, the proof of Lemma 5.3 can be modified so that ccqq-QAM_1 is shown to be in qq-QAM_1. ◀

6 QAM versus one-sided error qq-QAM

This section shows that qq-QAM proof systems of perfect-completeness are already as powerful as the standard QAM proof systems of two-sided bounded error (Theorem 1.4). As mentioned at the end of Section 5, the collapse theorem for qq-QAM holds even for the perfect-completeness variants. In particular, the inclusion $\text{ccqq-QAM}_1 \subseteq \text{qq-QAM}_1$ holds. Hence, for the proof of Theorem 1.4, it suffices to show that any problem in cq-QAM ($=$ QAM) is necessarily in the class ccqq-QAM_1. As mentioned earlier, this can be shown by combining the classical technique in Ref. [7] for proving $\text{AM} = \text{AM}_1$, which originates in the proof of $\text{BPP} \subseteq \Sigma_2^{\text{P}}$ due to Lautemann [22], and the recent result that sharing a constant number of EPR pairs can make QMA proofs perfectly complete [20].

Proof of Theorem 1.4 (Sketch). Intuitively, with two classical turns of communications, the classical technique in Ref. [7] can be used to generate polynomially many instances of a (promise) QMA problem such that all these instances are QMA yes-instances if the input was a yes-instance, while at least one of these instances is a QMA no-instance with high probability if the input was a no-instance (some of the QMA instances may violate the promise if the input was a no-instance, but this does not matter, as the important point is that at least one instance is a no-instance in this case). Now one makes use of the $\text{QMA}_1^{\text{const-EPR}}$ proof system in Ref. [20] for each QMA instance, by running polynomially many attempts of such a system in parallel to see that none of them results in rejection. The resulting proof system is thus of ccqq-QAM type, as $\text{QMA}_1^{\text{const-EPR}}$ proof systems are special cases of qq-QAM proof systems. The perfect completeness of this proof system follows from the fact that all the QMA instances generated from an input of yes-instance are QMA yes-instances, and all of them are accepted without error in the attempts of the $\text{QMA}_1^{\text{const-EPR}}$ system due to the perfect completeness property of the system. The soundness of this proof

system follows from the fact that at least one QMA instance generated from an input of no-instance is a QMA no-instance with high probability, for which the $\mathrm{QMA}_1^{\text{const-EPR}}$ proof system results in rejection with reasonably high probability, due to the soundness property of it. The rigorous proof is found in the full version [19] of this paper. ◀

The fact that perfect completeness is achievable in cc-QAM (Theorem 1.6) can be proved in a similar fashion, except that now one uses the fact $\mathrm{MQA} = \mathrm{MQA}_1$ (a.k.a., $\mathrm{QCMA} = \mathrm{QCMA}_1$) that any classical-witness QMA proofs can be made perfectly complete shown in Ref. [15] instead of the inclusion $\mathrm{QMA} \subseteq \mathrm{QMA}_1^{\text{const-EPR}}$. Each QMA instance in the argument above are replaced by an MQA (QCMA) instance in this case. Notice that no additional turn is necessary in this case, as the second turn is a classical turn for a prover and witnesses for the MQA instances can be sent also at this turn. Hence, the resulting proof system corresponding to Π'' is immediately a cc-QAM proof system of perfect completeness.

7 Collapse theorem for general quantum Arthur-Merlin proof systems

Before the proof of Theorem 1.7, first observe the simple fact that one can always replace classical turns by quantum ones without diminishing the verification power, by letting the verifier simulate classical turns by quantum turns via CNOT applications.

▶ **Proposition 7.1.** *For any constant m in $\mathbb{N}$, any j in $\{1,\ldots,m\}$, and any message-types $t_1,\ldots,t_m$ in $\{\mathrm{c},\mathrm{q}\}$,*

$$t_m \cdots t_{j+1}\, t_j\, t_{j-1} \cdots t_1\text{-QAM}(m) \subseteq t_m \cdots t_{j+1}\, \mathrm{q}\, t_{j-1} \cdots t_1\text{-QAM}(m).$$

As generalized quantum Arthur-Merlin proofs are nothing but a special case of general quantum interactive proofs, it is obvious that for any constant m and any message-types $t_1,\ldots,t_m$ in $\{\mathrm{c},\mathrm{q}\}$, $t_m \cdots t_1\text{-QAM}(m)$ is contained in $\mathrm{QIP} = \mathrm{PSPACE}$ [13]. As mentioned in Section 1, Marriott and Watrous [24] proved that qcq-QAM (= QMAM) already hits the ceiling, i.e., coincides with QIP. Next lemma states that one can slightly improve this and even the third message is not necessary to be quantum to have the full power of quantum interactive proofs. The proof is based on a simulation of the original qcq-QAM system by a qcc-QAM system using quantum teleportation.

▶ **Lemma 7.2.** qcq-QAM $\subseteq$ qcc-QAM.

Proof (Sketch). Let $A = (A_{\text{yes}}, A_{\text{no}})$ be a problem in qcq-QAM, meaning that A has a qcq-QAM proof system Π with completeness 2/3 and soundness 1/3 that is specified by the protocol of the verifier of the following form for every input x:

1. Receive a quantum register M_1 from the prover, and then send a random string r to the prover.
2. Receive a quantum register M_2 from the prover. Prepare a private quantum register V, and perform the final verification procedure over $(\mathsf{M}_1, \mathsf{M}_2, \mathsf{V})$.

Let $l\colon \mathbb{Z}^+ \to \mathbb{N}$ be the polynomially bounded function that specifies the number of qubits in M_2. Consider the teleportation-based simulation of Π by the qcc-QAM proof system $\widetilde{\Pi}$, where the verifier performs the following protocol for every input x:

1. Receive a quantum register S_1 of $l(|x|)$ qubits, in addition to the quantum register M_1, from the prover. Send a random string r to the prover as would be done in Π.

2. Receive a binary string b of length $2\,l(|x|)$ from the prover. Apply $X^{b_{j,1}}Z^{b_{j,2}}$ to the jth qubit of S_1, for each j in $\{1,\ldots,l(|x|)\}$, where $b_{j,1}$ and $b_{j,2}$ denote the $(2j-1)$st and $(2j)$th bits of b, respectively. Finally, prepare his/her private quantum register V as in Π, and simulate the final verification procedure of the verifier in Π with $(\mathsf{M}_1, \mathsf{S}_1, \mathsf{V})$.

The claim follows from a rigorous analysis of this protocol, which is relegated to the full version [19] of this paper. ◀

With Lemma 7.2 in hand, Theorem 1.7 is proved as follows.

Proof of Theorem 1.7. For the item (i), first notice that qcq-QAM is shown to be in qccc-QAM by an argument very similar to the proof of Lemma 7.2, with not the honest prover but the verifier preparing the EPR pairs. As qcq-QAM = QMAM = QIP = PSPACE, together with Lemma 7.2, this implies that qccc-QAM = qcc-QAM = PSPACE. As adding more turns to $\mathrm{q}t_3t_2t_1$-QAM and $\mathrm{q}t_2t_1$-QAM proof systems does not diminish the verification power for any t_1, t_2, and t_3 in $\{\mathrm{q},\mathrm{c}\}$, this establishes the claim in the item (i).

For the item (ii), again with a similar argument to the proof of Lemma 7.2, it holds that $\mathrm{c}\cdots\mathrm{cqq}$-QAM$(m)$ is included in $\mathrm{c}\cdots\mathrm{cqc}$-QAM$(m)$ for any constant $m \geq 2$, and thus, combined with Theorem 1.1 and Proposition 7.1, the claim follows.

For the item (iii), it suffices to show that, for any constant $m \geq 3$, $\mathrm{c}\cdots\mathrm{cq}$-QAM$(m)$ is included in $\mathrm{c}\cdots\mathrm{cq}$-QAM$(m-1)$. The case with $m \geq 5$ is proved with an argument similar to that in the proof of Lemma 5.1, since the first three (resp. four) turns of the m-turn $\mathrm{c}\cdots\mathrm{cq}$-QAM proof systems are classical when m is odd (resp. when m is even). In the case where $m = 3$, one modifies the construction of Π' in the proof of Lemma 5.1 so that the message from the prover at the second turn (corresponding to Step 2 of Π') is quantum, consisting of $(k(|x|)+1)$ parts: the Y part and each Z_j part for j in $\{1,\ldots,k(|x|)\}$, corresponding to y and each z_j in Step 2 of Π'. In order to force the content in the Y part to be classical, the verifier simply measures each qubit in the Y part in the computational basis. The analysis in the proof of Lemma 5.1 then works with the case where $m = 3$, i.e., the case where a ccq-QAM system is simulated by a cq-QAM system. The case where $m = 4$ can then be proved using this result with $m = 3$, with the same argument as in the proof of Lemma 5.1.

Finally, for the item (iv), it suffices to show that, for any constant $m \geq 3$, $\mathrm{c}\cdots\mathrm{c}$-QAM$(m)$ is included in $\mathrm{c}\cdots\mathrm{c}$-QAM$(m-1)$, which easily follows from an argument similar to that in the proof of Lemma 5.1, since all the messages are classical. ◀

8 Conclusion

This paper has introduced the generalized model of quantum Arthur-Merlin proof systems to provide some new insights on the power of two-turn quantum interactive proofs. A number of open problems are listed below concerning generalized quantum Arthur-Merlin proof systems and other related topics:

- Is there any natural problem, other than CITM and MaxOutQEA, in qq-QAM that is not known to be in the standard QAM? Or is qq-QAM equal to QAM?
- Currently no upper-bound is known for qq-QAM other than QIP(2). Can a better upper-bound be placed on qq-QAM? Is qq-QAM contained in BP · PP?
- Does qq-QAM = qq-QAM$_1$? In other words, is perfect completeness achievable in qq-QAM? Similar questions remain open even for QIP(2) and QAM.
- What happens if some of the messages are restricted to be classical in the standard quantum interactive proof systems? Does a collapse theorem similar to the qq-QAM case hold even with the QIP(2) case? More precisely, is the power of m-turn quantum

interactive proof systems equivalent to QIP(2) for any constant $m \geq 2$, when the first $(m-2)$ turns are restricted to exchange only classical messages?

For the last question above, note that one might be able to show a similar collapse theorem even with QIP(2) when the verifier *cannot* use quantum operations at all during the first $(m-2)$ turns (possibly by extending the argument due to Goldwasser and Sipser [10] to replace the classical interaction of the first $(m-2)$ turns by an m-turn classical public-coin interaction, and then applying arguments similar to those in this paper, using some appropriate QIP(2)-complete problem like the Close Image problem [32, 12], although the authors do not know if this approach works). A more difficult, but more natural and interesting case is where the verifier can use quantum operations to generate his/her classical messages even for the first $(m-2)$ turns, to which the Goldwasser-Sipser technique does not seem to apply any longer. A collapse theorem for such a case, if provable, would be very helpful when trying to put more problems in QIP(2) and more generally investigating the properties of two-turn quantum interactive proof systems.

Acknowledgements. The authors are grateful to Francesco Buscemi and Richard Cleve for very useful discussions. This work is supported by the Grant-in-Aid for Scientific Research (A) No. 24240001 of the Japan Society for the Promotion of Science and the Grant-in-Aid for Scientific Research on Innovative Areas No. 24106009 of the Ministry of Education, Culture, Sports, Science and Technology in Japan. HN also acknowledges support from the Grant-in-Aids for Scientific Research (A) Nos. 21244007 and 23246071 and (C) No. 25330012 of the Japan Society for the Promotion of Science.

References

1 Scott Aaronson, Salman Beigi, Andrew Drucker, Bill Fefferman, and Peter Shor. The power of unentanglement. *Theory of Computing*, 5:1–42 (article 1), 2009.

2 Dorit Aharonov. A simple proof that Toffoli and Hadamard are quantum universal. arXiv.org e-Print archive, arXiv:quant-ph/0301040, 2003.

3 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.

4 László Babai. Trading group theory for randomness. In *Proceedings of the Seventeenth Annual ACM Symposium on Theory of Computing*, pages 421–429, 1985.

5 Salman Beigi, Peter Shor, and John Watrous. Quantum interactive proofs with short messages. *Theory of Computing*, 7:101–117 (article 7), 2011.

6 Avraham Ben-Aroya, Oded Schwartz, and Amnon Ta-Shma. Quantum expanders: Motivation and constructions. *Theory of Computing*, 6:47–79 (article 3), 2010.

7 Jin-Yi Cai. Lectures in computational complexity, August 2012. Available at `http://www.cs.wisc.edu/~jyc/710/book.pdf`.

8 André Chailloux, Dragos Florin Ciocan, Iordanis Kerenidis, and Salil Vadhan. Interactive and noninteractive zero knowledge are equivalent in the help model. In *Theory of Cryptography, Fifth Theory of Cryptography Conference, TCC 2008*, volume 4948 of *Lecture Notes in Computer Science*, pages 501–534, 2008. A full version available as Cryptology ePrint Archive, Report 2007/467, 2007.

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

10 Shafi Goldwasser and Michael Sipser. Private coins versus public coins in interactive proof systems. In Silvio Micali, editor, *Randomness and Computation*, volume 5 of *Advances in Computing Research*, pages 73–90. JAI Press, 1989.

11 Gustav Gutoski. *Quantum Strategies and Local Operations*. PhD thesis, David R. Cheriton School of Computer Science, University of Waterloo, 2009. arXiv.org e-Print archive, arXiv:1003.0038 [quant-ph].

12 Patrick Hayden, Kevin Milner, and Mark M. Wilde. Two-message quantum interactive proofs and the quantum separability problem. *Quantum Information and Computation*, 14(5–6):0384–0416, 2014.

13 Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP = PSPACE. *Journal of the ACM*, 58(6):article 30, 2011.

14 Rahul Jain, Sarvagya Upadhyay, and John Watrous. Two-message quantum interactive proofs are in PSPACE. In *50th Annual Symposium on Foundations of Computer Science*, pages 534–543, 2009.

15 Stephen P. Jordan, Hirotada Kobayashi, Daniel Nagaj, and Harumichi Nishimura. Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. *Quantum Information and Computation*, 12(5–6):0461–0471, 2012.

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 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.

18 Hirotada Kobayashi. Non-interactive quantum perfect and statistical zero-knowledge. In *Algorithms and Computation, 14th International Symposium, ISAAC 2003*, volume 2906 of *Lecture Notes in Computer Science*, pages 178–188, 2003.

19 Hirotada Kobayashi, François Le Gall, and Harumichi Nishimura. Generalized quantum Arthur-Merlin games. arXiv.org e-Print archive, arXiv:1312.4673v2 [quant-ph], 2014.

20 Hirotada Kobayashi, François Le Gall, and Harumichi Nishimura. Stronger methods of making quantum interactive proofs perfectly complete. *SIAM Journal on Computing*, 44(2):243–289, 2015.

21 Hirotada Kobayashi, Keiji Matsumoto, and Tomoyuki Yamakami. Quantum Merlin-Arthur proof systems: Are multiple Merlins more helpful to Arthur? *Chicago Journal of Theoretical Computer Science*, 2009:article 3, 2009.

22 Clemens Lautemann. BPP and the polynomial hierarchy. *Information Processing Letters*, 17(4):215–217, 1983.

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

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

25 Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

26 Christos H. Papadimitriou. Games against nature. *Journal of Computer and System Sciences*, 31(2):288–301, 1985.

27 Bill Rosgen and John Watrous. On the hardness of distinguishing mixed-state quantum computations. In *Twentieth Annual IEEE Conference on Computational Complexity*, pages 344–354, 2005.

28 Adi Shamir. IP = PSPACE. *Journal of the ACM*, 39(4):869–877, 1992.

29 Alexander Shen. IP = PSPACE: Simplified proof. *Journal of the ACM*, 39(4):878–880, 1992.

30 Yaoyun Shi. Both Toffoli and Controlled-NOT need little help to do universal quantum computing. *Quantum Information and Computation*, 3(1):084–092, 2003.

31 Peter W. Shor. Fault-tolerant quantum computation. In *37th Annual Symposium on Foundations of Computer Science*, pages 56–65, 1996.

32 John Watrous. Capturing quantum complexity classes via quantum channels. Talk at the 6th Workshop on Quantum Information Processing, December 2002.

33 John Watrous. Limits on the power of quantum statistical zero-knowledge. In *43rd Annual Symposium on Foundations of Computer Science*, pages 459–468, 2002.

34 John Watrous. PSPACE has constant-round quantum interactive proof systems. *Theoretical Computer Science*, 292(3):575–588, 2003.

35 John Watrous. Zero-knowledge against quantum attacks. *SIAM Journal on Computing*, 39(1):25–58, 2009.

36 Stephanie Wehner. Entanglement in interactive proof systems with binary answers. In *STACS 2006, 23rd Annual Symposium on Theoretical Aspects of Computer Science*, volume 3884 of *Lecture Notes in Computer Science*, pages 162–171, 2006.

37 Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013.

A qq-QAM-completeness of MaxOutQEA

This section presents a proof of the MaxOutQEA problem being in qq-QAM. As the proof of Lemma 5.2 essentially shows the qq-QAM-hardness of MaxOutQEA (a separate proof of which is found in the full version [19] of this paper), this proves Theorem 1.3, the qq-QAM-completeness of MaxOutQEA.

▶ **Lemma A.1.** MaxOutQEA *is in* qq-QAM.

Proof. We present a reduction from the MaxOutQEA problem to the CITM problem (with some appropriate parameters), by modifying the reduction from the QEA problem to the Quantum State Closeness to Totally Mixed (QSCTM) problem presented in the full version of Ref. [8], which relies on the analysis found in Section 5.3 of Ref. [6].

Let $x = (Q, t)$ be an instance of MaxOutQEA, where Q is a description of a quantum circuit that specifies a quantum channel Φ, and t is a positive integer. For simplicity, in what follows, we identify the description Q and the quantum circuit it induces. Suppose that Q acts on m_{all} qubits with m_{in} specified input qubits and m_{out} specified output qubits. Let q and ε be two functions that appear in Eqs. (5.1) and (5.2) of Ref. [6][1] to be specified later. We consider the quantum circuit $Q^{\otimes q(|x|)}$ that runs $q(|x|)$ copies of Q in parallel, and the (qt, d, ε)-quantum extractor E on $q(|x|)\, m_{\mathrm{out}}$ qubits given in Ref. [6, Section 5.3], which is written as $E = \frac{1}{2^d} \sum_{j=1}^{2^d} E_j$, where $E_j(\rho) = U_j \rho U_j^\dagger$ for unitary operators U_j. Let R be the quantum circuit that runs $Q^{\otimes q(|x|)}$ and then applies E to the output state of $q(|x|)\, m_{\mathrm{out}}$ qubits. By following the analysis found in Ref. [6], one can show that

(i) if $x = (Q, t)$ is a yes-instance of MaxOutQEA, there exists a quantum state ρ consisting of $q(|x|)\, m_{\mathrm{in}}$ qubits such that $D(R(\rho), (I/2)^{\otimes q(|x|)\, m_{\mathrm{out}}}) \leq \frac{3}{2}\varepsilon$, and

(ii) if $x = (Q, t)$ is a no-instance of MaxOutQEA, for any quantum state ρ consisting of $q(|x|)\, m_{\mathrm{in}}$ qubits, it holds that $D\big(R(\rho), (I/2)^{\otimes q(|x|)\, m_{\mathrm{out}}}\big) \geq \frac{1}{4\, q(|x|)\, m_{\mathrm{out}}}$.

In fact, the item (i) follows from exactly the same analysis as in Ref. [6], by taking $\rho = \sigma^{\otimes q(|x|)}$ with σ being a quantum state of m_{in} qubits such that $S(Q(\sigma)) \geq t + 1$ (the condition $S_{\max}(\Phi) \geq t + 1$ ensures the existence of such a state σ).

[1] Rigorously speaking, q in the present case corresponds to $\frac{q}{2}$ in the left-hand sides of Eqs. (5.1) and (5.2) of Ref. [6]. This is due to the fact that the MaxOutQEA problem in this paper is defined using threshold values $t + 1$ and $t - 1$, while the QEA problem in Ref. [6] is defined using threshold values $t + \frac{1}{2}$ and $t - \frac{1}{2}$.

To prove the item (ii), first notice that, if $x = (Q, t)$ is a no-instance of MaxOutQEA, it holds that $S(Q(\sigma)) \leq S_{\max}(\Phi) \leq t - 1$ for any quantum state σ of m_{in} qubits. Take an arbitrary quantum state ρ of $q(|x|)\, m_{\text{in}}$ qubits. By Lemma 2.2, it holds that

$$S(R(\rho)) = S\left(\frac{1}{2^d}\sum_{j=1}^{2^d} U_j\, Q^{\otimes q(|x|)}(\rho)\, U_j^\dagger\right) \leq S\big(Q^{\otimes q(|x|)}(\rho)\big) + d.$$

For each j in $\{1, \ldots, q(|x|)\}$, let R_j be the output quantum register of the jth copy of Q (hence, the whole output state $Q^{\otimes q(|x|)}(\rho)$ of $Q^{\otimes q(|x|)}$ is in $\big(\mathsf{R}_1, \ldots, \mathsf{R}_{q(|x|)}\big)$), and let σ_{R_j} be the reduced state of $Q^{\otimes q(|x|)}(\rho)$ of m_{out} qubits obtained by tracing out all the qubits except those in R_j. By the subadditivity of von Neumann entropy, it follows that

$$S\big(Q^{\otimes q(|x|)}(\rho)\big) \leq \sum_{j=1}^{q(|x|)} S(\sigma_{\mathsf{R}_j}) \leq \sum_{j=1}^{q(|x|)} \max_{\sigma} S(Q(\sigma)) \leq (t-1)\, q(|x|),$$

which implies that

$$S(R(\rho)) \leq (t-1)\, q(|x|) + d.$$

Now the item (ii) follows from exactly the same analysis as in Ref. [6].

To complete the reduction, similarly to the full version of Ref. [8], one takes $\varepsilon = 2^{-k}$ for a polynomially bounded function $k\colon \mathbb{Z}^+ \to \mathbb{N}$ such that $k(n) \geq n$ for any n in $\mathbb{Z}^+$ and $k(n) \in O(n)$, and a polynomially bounded function $q\colon \mathbb{Z}^+ \to \mathbb{N}$ such that $q(n) \in \Theta(n^4)$ so that Eqs. (5.1) and (5.2) of Ref. [6] are satisfied. Consider the quantum circuit R' that runs $r(|x|)$ copies of R in parallel for a polynomially bounded function $r\colon \mathbb{Z}^+ \to \mathbb{N}$ such that $r(n) = \left\lceil \frac{2\ln(1/2)}{\ln(1-(1/(2\,q(n)\,m_{\text{out}})^2))} \right\rceil \leq 2(2\,q(n)\,m_{\text{out}})^2$ for all n in $\mathbb{Z}^+$. Assuming that $r(|x|) \leq 2^{|x|}/12$ (otherwise $|x|$ is at most some fixed constant as r is a polynomially bounded function, and thus, it can be checked trivially whether $x = (Q, t)$ is a yes-instance or a no-instance), it follows from Lemma 2.1 that

- **(i)** if $x = (Q, t)$ is a yes-instance of MaxOutQEA, there exists a quantum state σ consisting of $r(|x|)\, q(|x|)\, m_{\text{in}}$ qubits such that $D\big(R'(\sigma), (I/2)^{\otimes r(|x|)\, q(|x|)\, m_{\text{out}}}\big) \leq 1/8$, and
- **(ii)** if $x = (Q, t)$ is a no-instance of MaxOutQEA, for any quantum state σ consisting of $r(|x|)\, q(|x|)\, m_{\text{in}}$ qubits, it holds that $D\big(R'(\sigma), (I/2)^{\otimes r(|x|)\, q(|x|)\, m_{\text{out}}}\big) \geq 1/2$.

Hence, MaxOutQEA is reducible to CITM$(1/8, 1/2)$ in polynomial time, and thus in qq-QAM by Lemma 4.1. ◀