It all concerns rejection: a new approach to the QMA(1) $\stackrel{?}{=}$ QMA(2) problem

Giona Cantarutti[1], Riccardo Romanello[2]

[1]Graduate School of Informatics, Nagoya University, Nagoya, Japan
[1]DMIF, University of Udine, Via Le Scienze, 206, Udine, Italy

Abstract

The relationship between the complexity classes Quantum Merlin-Arthur, QMA(1), and Quantum Merlin-Arthur with two unentangled provers, QMA(2), is one of the most intriguing open questions in quantum complexity theory. In this paper, we study the problem through the lens of rejection capabilities. We prove that for any promise problem K in QMA(2) there exists a promise problem L in QMA(1) such that L is the *best attempt* to recognize K with a verifier in QMA(1). The only difference between the two problems, if any, lies in the set of rejected words. We call such L a *Single-Merlin Approximation* of K. By proving its existence and exploiting its properties, we derive a novel characterization of the QMA(1) $\stackrel{?}{=}$ QMA(2) problem. We then extend our approach to verification-based complexity classes in general: we consider classes whose proof sets are in a subset relation and prove that a general notion of approximation yields a technique to prove or disprove equality between such classes.

Keywords

QMA, QMA(2), quantum complexity, verification-based classes, promise problems, complexity separation

1. Introduction

The study of quantum complexity classes is central to understanding the computational power of quantum systems. Among these classes, Quantum Merlin-Arthur with one and two certificates, QMA(1) and QMA(2), play a pivotal role in exploring the boundaries of quantum verification. The class QMA(1) involves a single quantum proof (or witness) verified by a quantum polynomial-time verifier, while QMA(2) extends this to two unentangled quantum proofs. Whether these two classes are equal, i.e., whether QMA(1) = QMA(2), remains a fundamental open question in quantum complexity theory.

The question is not merely academic but has deep implications for entanglement, quantum cryptographic protocols, and the structure of quantum verification. In [1], Aaronson et al. proposed the *Strong Amplification Conjecture*, which implies QMA(2) $\subseteq$ PSPACE, and disproved the existence of a perfect disentangler that could simulate QMA(2) in QMA(1). This does not, however, exclude other paths towards proving the equivalence of the two classes. Along these lines, the result in [2] showed that QMA(2) and QMA(1) coincide when the verifier is restricted to one-way LOCC protocols. Other approaches have sought to relate QMA(2) to classical complexity classes. The only known classical bound is QMA(2) $\subseteq$ NEXP. In [3] it was proven that QMA(2) = NEXP would imply that the Quantum Polynomial Hierarchy—QPH, [3]—collapses to its second level, interpreted as the non-increasing expressiveness of alternating quantifiers in the quantum setting.

One of the most recent approaches to the QMA(2) $\stackrel{?}{=}$ NEXP question is due to [4], which considers $\mathrm{QMA}^+(2)$: the same as QMA(2) but requiring proofs with non-negative amplitudes in the computational basis. It was shown that $\mathrm{QMA}^+(2)$ at some completeness-soundness gap equals QMA(2), while at another constant gap it equals NEXP. This means that if $\mathrm{QMA}^+(2)$ where to exhibit gap amplification then QMA(2) = NEXP. In the same work however, the class $\mathrm{QMA}^+(1)$ was defined symmetrically. As proved in [5], $\mathrm{QMA}^+(1)$ equals QMA(1) for some constant gap, yet equals NEXP for another. This means that any gap amplification procedure found for $\mathrm{QMA}^+(2)$ would need to crucially exploit

ICTCS 2026: 27th Italian Conference on Theoretical Computer Science, September 2026, Udine, Italy
giona.cantarutti@gmail.com (G. Cantarutti); riccardo.romanello@uniud.it (R. Romanello)

disentanglement because if it were to be applicable to $\mathsf{QMA}^+(1)$ it would cause a major collapse in classical complexity theory. Later on [6] introduced new variants requiring internal separability and reached very similar results without however incurring in the risk of collapse. Nevertheless, the problem remains open.

In this work, we propose a novel approach to the $\mathsf{QMA}(1) \stackrel{?}{=} \mathsf{QMA}(2)$ question by focusing on the rejection capabilities of these classes. We introduce the notion of *Single-Merlin Approximation* and prove that every problem $K \in \mathsf{QMA}(2)$ admits one. We show that $\mathsf{QMA}(1) \neq \mathsf{QMA}(2)$ if and only if there exists $K \notin \mathsf{QMA}(1)$ whose Single-Merlin approximation has non-empty, non-factorizable extensions—where the extensions witness the words that QMA(1) cannot properly reject. We then embed both classes into a broader landscape of verification-based complexity classes: classes where the only difference is the proof set. Both QMA(1) and QMA(2) have the same verifier complexity and the same completeness and soundness parameters; their essential difference is that the proof set of QMA(2) consists solely of *separable* (factorizable) quantum witnesses, a proper subset of those available to QMA(1). We formalize a general notion of approximation for such pairs of classes and prove that it provides a robust tool to characterize their separation.

This paper is organized as follows. Section 2 recalls the notions required throughout the paper. Section 3 develops the notion of a Single-Merlin approximation and proves our main characterization of the $\mathsf{QMA}(1) \stackrel{?}{=} \mathsf{QMA}(2)$ question. Section 4 generalizes this framework to other verification-based complexity classes. Finally, Section 5 concludes the paper.

2. Basic notions

In this section we recall the theoretical concepts required throughout the paper. A more detailed introduction is given in the appendix. We begin with a fundamental concept in complexity theory.

Definition 1 (Promise Problem)**.** *A Promise Problem K is a pair of languages $K_{yes} \subseteq \{0,1\}^*$ and $K_{no} \subseteq \{0,1\}^*$ such that $K_{yes} \cap K_{no} = \emptyset$.*

The union $K_{\text{yes}} \cup K_{\text{no}}$ is known as the *promise*. From this point forward, all problems are assumed to be promise problems. We write K_{NA} for the set $\Sigma^* \setminus (K_{\text{yes}} \cup K_{\text{no}})$, so a promise problem K is represented as a partition $K = \{K_{\text{yes}}, K_{\text{NA}}, K_{\text{no}}\}$ into three classes.

We now turn to the quantum class QMA(1), whose problems are decided by a Quantum Verifier.

Definition 2 (Quantum Merlin-Arthur)**.** *Let $L = \{L_{yes}, L_{NA}, L_{no}\}$ be a promise problem. The problem L belongs to* QMA(1) *if there exists a polynomial-time (single-proof) Quantum Verifier V and a polynomial $p(n)$ such that for every input $x \in \{0,1\}^n$:*

- ***(Completeness)** If $x \in L_{yes}$, then there exists a quantum proof $|\psi\rangle$ over $p(n)$ qubits such that $\Pr[V(x, |\psi\rangle) = 1] \geq \frac{2}{3}$.*
- ***(Soundness)** If $x \in L_{no}$, then for all quantum proofs $|\psi\rangle$ over $p(n)$ qubits, $\Pr[V(x, |\psi\rangle) = 1] \leq \frac{1}{3}$.*
- *The behavior of V is unconstrained when the input belongs to L_{NA}.*

Let L be a promise problem and V the Quantum Verifier witnessing $L \in \mathsf{QMA}(1)$. We say that V *recognizes* L, that V is *complete* for L_{yes}, and *sound* for L_{no}.

Allowing the verifier to receive k proofs leads to the class $\mathsf{QMA}(k)$. With $k = 2$, QMA(2) arises.

Definition 3 (QMA(2))**.** *Let $K = \{K_{yes}, K_{NA}, K_{no}\}$ be a promise problem. The problem K belongs to* QMA(2) *if there exists a polynomial-time Quantum Verifier V and a polynomial $p(n)$ such that for every input $x \in \{0,1\}^n$:*

- ***(Completeness)** If $x \in K_{yes}$, then there exist quantum proofs $|\psi_1\rangle, |\psi_2\rangle$, both over $p(n)$ qubits, such that $\Pr[V(x, |\psi_1\rangle, |\psi_2\rangle) = 1] \geq \frac{2}{3}$.*
- ***(Soundness)** If $x \in K_{no}$, for all pairs $|\psi_1\rangle, |\psi_2\rangle$ over $p(n)$ qubits, $\Pr[V(x, |\psi_1\rangle, |\psi_2\rangle) = 1] \leq \frac{1}{3}$.*

- *The behavior of V is unconstrained when the input belongs to K_{NA}.*

It was shown in [7] that QMA(2) = QMA(k) for $k \geq 2$. The question of whether QMA(1) = QMA(2) remains open.

3. QMA(1) $\stackrel{?}{=}$ QMA(2): It boils down to rejection

The goal of this section is that of introducing the central notion of this work. Informally speaking, what we were able to show is that the actual witness of the difference between QMA(1) and QMA(2) is their rejection capability.

Definition 4 (Single-Merlin Approximation)**.** *Let $K = \{K_{yes}, K_{NA}, K_{no}\}$ and $L = \{L_{yes}, L_{NA}, L_{no}\}$ be two promise problems, and let $L \in$ QMA(1). We say that L is a* Single-Merlin approximation *of K if and only if there exist $C \subseteq L_{yes}$, $U \subseteq L_{NA}$, and a polynomial-time Quantum Verifier V that recognizes L such that:*

- $K = \{L_{yes} \setminus C,\ L_{NA} \setminus U,\ L_{no} \cup C \cup U\}$, *and*
- *there exists a polynomial $p(n)$ such that for every $x \in K_{yes}$ with $|x| = n$ there exist $|\psi_1\rangle, |\psi_2\rangle$, both over $p(n)$ qubits, with*

$$\Pr[V(x, |\psi_1\rangle \otimes |\psi_2\rangle) = 1] \geq \tfrac{2}{3}.$$

The two sets C and U are called the *extensions* of K into L. We write $K \rightsquigarrow_{C,U} L$ whenever L is a Single-Merlin approximation of K with extensions C and U. Note that while V is sound for L_{no}, the requirement on K_{yes} is stricter than completeness alone: words in K_{yes} must be accepted by V via *factorizable* certificates.

A Single-Merlin approximation L of a problem K is an attempt to place K within QMA(1), that is if $K \rightsquigarrow_{C,U} L$, then $L \in$ QMA(1) by definition. $K \in$ QMA(1) holds if and only if there exists a Single-Merlin approximation with both C and U empty; otherwise we obtain a problem $L \in$ QMA(1) distinct from K, and $C \cup U$ witnesses the difference: words in C and U belong to K_{no} but are placed in L_{yes} and L_{NA}, respectively.

The first useful result concerns the existence of Single-Merlin approximations for problems in QMA(2).

Lemma 1. *Let $K = \{K_{yes}, K_{NA}, K_{no}\} \in$ QMA(2) be a promise problem. There exist L, C, and U such that $K \rightsquigarrow_{C,U} L$.*

Proof. Let $K = \{K_{\text{yes}}, K_{\text{NA}}, K_{\text{no}}\} \in$ QMA(2), accepted by a two-proof quantum verifier V_2 that is complete for K_{yes} and sound for K_{no}.

We construct a single-proof quantum verifier V_1 as follows. For every pair $(x, |\psi\rangle)$ such that $|\psi\rangle$ factorizes into $|\psi_1\rangle \otimes |\psi_2\rangle$, the verifier $V_1(x, |\psi\rangle)$ behaves exactly as $V_2(x, |\psi_1\rangle, |\psi_2\rangle)$. For pairs without a factorizable certificate, the only requirement imposed is polynomial-time execution. It is important to note that defining this behavior does not solve the separability problem: V_1 is merely a copy of V_2, which treats the qubits as if they were factorizable. If they are not, V_2 will behave unpredictably.

By construction, V_1 runs in polynomial time. We now characterize the promise problem L recognized by V_1. Let $x \in K_{\text{yes}}$. Since $K \in$ QMA(2), there exist $|\psi_1\rangle, |\psi_2\rangle$ such that $\Pr[V_2(x, |\psi_1\rangle, |\psi_2\rangle) = 1] \geq \frac{2}{3}$. Setting $|\psi\rangle := |\psi_1\rangle \otimes |\psi_2\rangle$, since $|\psi\rangle$ is factorizable, $V_1(x, |\psi\rangle)$ simulates $V_2(x, |\psi_1\rangle, |\psi_2\rangle)$, and so

$$\Pr[V_1(x, |\psi\rangle) = 1] = \Pr[V_2(x, |\psi_1\rangle, |\psi_2\rangle) = 1] \geq \tfrac{2}{3}.$$

Therefore V_1 is complete for K_{yes}.

We now turn to K_{no}. For any $x \in K_{\text{no}}$ and any factorizable $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, V_1 simulates V_2 and so $\Pr[V_1(x, |\psi\rangle) = 1] \leq \frac{1}{3}$. However, there may exist non-factorizable certificates $|\psi'\rangle$ with $\Pr[V_1(x, |\psi'\rangle) = 1] > \frac{1}{3}$. Define

$$|\psi^x_{\max}\rangle = \arg\max_{|\psi\rangle} \Pr[V_1(x, |\psi\rangle) = 1].$$

We split $x \in K_{\text{no}}$ into three cases according to the value of $\Pr[V_1(x, |\psi^x_{\max}\rangle) = 1]$: if it is at most $\frac{1}{3}$, then x is rejected by V_1; if it lies in $(\frac{1}{3}, \frac{2}{3})$, we place x into a set U; and if it is at least $\frac{2}{3}$, we place x into a set C.

We define $L = \{L_{\text{yes}}, L_{\text{NA}}, L_{\text{no}}\}$ as: $L_{\text{yes}} = K_{\text{yes}} \cup C$, $L_{\text{NA}} = K_{\text{NA}} \cup U$, and $L_{\text{no}} = K_{\text{no}} \setminus (C \cup U)$. By construction, V_1 witnesses the relation $K \rightsquigarrow_{C,U} L$, and K has a Single-Merlin approximation. □

A special case of $K \rightsquigarrow_{C,U} L$ is $C \cup U = \emptyset$, in which case $K \in \mathsf{QMA}(2)$ also belongs to $\mathsf{QMA}(1)$. This is formalized in the following lemma.

Lemma 2. *If* $\mathsf{QMA}(1) \neq \mathsf{QMA}(2)$*, then*

$$\exists K \in \mathsf{QMA}(2).\ \forall L \in \mathsf{QMA}(1)\ \big(K \rightsquigarrow_{C,U} L\ \Rightarrow\ C \cup U \neq \emptyset\big).$$

Proof. We prove the contrapositive. Suppose that for all $K \in \mathsf{QMA}(2)$ there exists $L \in \mathsf{QMA}(1)$ with $K \rightsquigarrow_{C,U} L$ and $C \cup U = \emptyset$. Then $L = K$, so $K \in \mathsf{QMA}(1)$, and hence $\mathsf{QMA}(1) = \mathsf{QMA}(2)$. □

With Lemma 1 we proved the existence of Single-Merlin approximations. Lemma 2 shows how the definition can be used to characterize the difference between $\mathsf{QMA}(1)$ and $\mathsf{QMA}(2)$.

We now investigate the properties of the extensions C and U. The following definition leads to a sharper version of Lemma 2.

Definition 5 (Non-factorizable extensions)**.** *Let $K \in \mathsf{QMA}(2)$ and let L, C, U be such that $K \rightsquigarrow_{C,U} L$. Let V be the single-proof Quantum Verifier witnessing the approximation. We say that C and U are* non-factorizable *if and only if for every $x \in (C \cup U)$ and every $|\psi\rangle$ with $\Pr[V(x, |\psi\rangle) = 1] > \frac{1}{3}$, there exist no $|\psi_1\rangle, |\psi_2\rangle$ with $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$.*

This definition captures those extensions that contain only words whose relevant certificates cannot be factorized as a tensor product.

Lemma 3. *Let $K = \{K_{yes}, K_{NA}, K_{no}\} \in \mathsf{QMA}(2)$ be a promise problem such that $K \notin \mathsf{QMA}(1)$. There exist L, C, U such that $K \rightsquigarrow_{C,U} L$ with $C \cup U \neq \emptyset$ and C, U non-factorizable.*

Proof. Let $K \in \mathsf{QMA}(2)$ be accepted by V_2, with $K \notin \mathsf{QMA}(1)$. By Lemma 1, there exists at least one Single-Merlin approximation $K \rightsquigarrow_{C,U} L$, witnessed by V_1. Since $K \in \mathsf{QMA}(2) \setminus \mathsf{QMA}(1)$, Lemma 2 ensures that all Single-Merlin approximations of K satisfy $C \cup U \neq \emptyset$.

Recall from the proof of Lemma 1 that, for the approximation L, C and U contain exactly those $x \in K_{\text{no}}$ for which there exists a non-factorizable certificate $|\psi\rangle$ with $\Pr[V_1(x, |\psi\rangle) = 1] > \frac{1}{3}$. Suppose there also exists a factorizable $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ with $\Pr[V_1(x, |\psi\rangle) = 1] > \frac{1}{3}$. Since V_1 mimics V_2 on factorizable inputs, this would give $\Pr[V_2(x, |\psi_1\rangle, |\psi_2\rangle) = 1] > \frac{1}{3}$, contradicting soundness of V_2 for $x \in K_{\text{no}}$. Therefore all certificates $|\psi\rangle$ with $\Pr[V_1(x, |\psi\rangle) = 1] > \frac{1}{3}$ are non-factorizable, and both C and U are non-factorizable. □

This lemma shows that when the attempt to place $K \in \mathsf{QMA}(2)$ into $\mathsf{QMA}(1)$ fails, the obstacle is precisely the presence of non-factorizable certificates that prevent the words in $C \cup U$ from being properly rejected.

Interestingly, the converse direction holds as well.

Lemma 4. *Let $K = \{K_{yes}, K_{NA}, K_{no}\}$ be a promise problem. If there exists a Single-Merlin approximation $K \rightsquigarrow_{C,U} L$ such that C and U are non-factorizable and $C \cup U \neq \emptyset$, then $K \in \mathsf{QMA}(2)$.*

Proof. Let L, C, U be as given, with V_1 the single-proof verifier witnessing the approximation. We construct a two-proof quantum verifier

$$V_2(x, |\psi_1\rangle, |\psi_2\rangle) := V_1(x, |\psi_1\rangle \otimes |\psi_2\rangle).$$

This runs in polynomial time. By definition of Single-Merlin approximation, V_2 is complete for K_{yes} and sound for $L_{\text{no}} = K_{\text{no}} \setminus (C \cup U)$.

It remains to show soundness for $C \cup U$. Let $x \in C$ and suppose there exist $|\psi_1\rangle, |\psi_2\rangle$ with $\Pr[V_2(x, |\psi_1\rangle, |\psi_2\rangle) = 1] > \frac{1}{3}$. By definition, $\Pr[V_1(x, |\psi_1\rangle \otimes |\psi_2\rangle)] > \frac{1}{3}$. But the extensions are non-factorizable, so no certificate of the form $|\psi_1\rangle \otimes |\psi_2\rangle$ can achieve this, a contradiction. Hence $\Pr[V_2(x, |\psi_1\rangle, |\psi_2\rangle) = 1] \leq \frac{1}{3}$ for all pairs. The same argument applies to $x \in U$.

Therefore V_2 is complete for K_{yes} and sound for $L_{\text{no}} \cup (C \cup U) = K_{\text{no}}$, so $K \in \text{QMA}(2)$. □

Joining all results, we obtain our main characterisation.

Theorem 1 (QMA(1) vs. QMA(2))**.** $\text{QMA}(1) \neq \text{QMA}(2)$ *if and only if there exists* $K \notin \text{QMA}(1)$ *such that* K *has a Single-Merlin approximation* $K \rightsquigarrow_{C,U} L$ *with* $C \cup U \neq \emptyset$ *and* C, U *non-factorizable.*

Proof. If $\text{QMA}(1) \neq \text{QMA}(2)$, there exists $K \in \text{QMA}(2)$ with $K \notin \text{QMA}(1)$. By Lemma 3, K has a Single-Merlin approximation $K \rightsquigarrow_{C,U} L$ with $C \cup U \neq \emptyset$ and C, U non-factorizable.

Conversely, suppose $K \notin \text{QMA}(1)$ has a Single-Merlin approximation $K \rightsquigarrow_{C,U} L$ with $C \cup U \neq \emptyset$ and C, U non-factorizable. By Lemma 4, $K \in \text{QMA}(2)$. Hence $\text{QMA}(1) \neq \text{QMA}(2)$. □

Theorem 1 provides a new characterization of the potential difference between QMA(1) and QMA(2). Being able to prove that the two classes differ is now equivalent to exhibiting a problem K all of whose Single-Merlin approximations have non-empty extensions.

4. Generalizing Single-Merlin Approximations

The notion of Single-Merlin approximation can be lifted to generic verification-based classes. With this term we refer to all complexity classes where the decision process is carried out by a machine whose input is composed of a word and a proof provided by an omniscient oracle. One example in classical computation is NP, where $L \in \text{NP}$ can be expressed in terms of *proofs* [8]. In the quantum setting, examples are the aforementioned QMA(1) and QMA(2). While at first sight the two classes differ only in the number of certificates, a more careful inspection shows that entanglement is the key distinction [1]: the proof set of QMA(2) consists solely of *factorizable* certificates—quantum witnesses expressible as a tensor product—and is therefore a proper subset of the proof set of QMA(1). We now generalize this observation.

We formalize the notion of a verification-based complexity class $R_{\mathscr{C},\mathscr{P}}(c, s)$, where $\mathscr{C}$ is the verifier complexity, $\mathscr{P}$ is the proof set, and c, s are the completeness and soundness bounds. We say that $B = R_{\mathscr{C},\mathscr{P}'}(c, s)$ is a *restricted version* of $A = R_{\mathscr{C},\mathscr{P}}(c, s)$ whenever $\mathscr{P}' \subset \mathscr{P}$.

Definition 6 (Verification-Based Complexity Class)**.** *Let* $\mathscr{C}$ *be a complexity class, let* $c, s \in [0, 1]$*, and let* $\mathscr{P}$ *be a set of words. We define* $\mathscr{R}_{\mathscr{C},\mathscr{P}}(c, s)$ *as the set of all promise problems* $L = \{L_{yes}, L_{NA}, L_{no}\}$ *for which there exists a promise problem* $L^V(c, s) = \{L^V(c, s)_{yes}, L^V(c, s)_{NA}, L^V(c, s)_{no}\} \in \mathscr{C}$ *and* $f \in \mathscr{F}$ *such that:*

- $\forall x \in L_{yes},\ \exists p \in \mathscr{P}$ *with* $|p| \leq f(|x|)$ *and* $(x, p) \in L^V(c, s)_{yes}$*,*
- $\forall x \in L_{no},\ \forall p \in \mathscr{P}$ *with* $|p| \leq f(|x|)$ *it holds* $(x, p) \in L^V(c, s)_{no}$*.*

The parameters c *and* s *are the* completeness *and* soundness *bounds. We say that* $\mathscr{R}_{\mathscr{C},\mathscr{P}}(c, s)$ *is a verification-based complexity class with verifier complexity* $\mathscr{C}$ *and proof set* $\mathscr{P}$*.*

An example is NP, with verifier complexity P, bounds $c = 1$ and $s = 0$, and where $\mathscr{F}$ is the set of polynomials. The class QMA(1) has verifier complexity BQP and proof set $\mathscr{P} = \mathbb{C}^{2^k}$ for polynomially bounded k, while QMA(2) has the same verifier complexity and bounds but proof set $\mathscr{P}' = \{|\psi\rangle \in \mathscr{P} : |\psi\rangle \text{ is factorizable}\}$. Another example is the comparison of QMA(2) with its positive version $\text{QMA}^+(2)$from [4]: the two classes share the same verifier complexity, number of proofs, and completeness and soundness, but $\text{QMA}^+(2)$restricts proofs to non-negative amplitudes.

Let $R_{\mathscr{C},\mathscr{P}}(c, s)$ be a verification-based class. We now consider a second class $R_{\mathscr{C},\mathscr{P}'}(c, s)$ with $\mathscr{P}' \subset \mathscr{P}$—the two classes differ only in the proof set.

Definition 7 (Restricted Variant of a Verification-based Class)**.** *Let $R_{\mathscr{C},\mathscr{P}}(c,s)$ and $R_{\mathscr{C}',\mathscr{P}'}(c',s')$ be two verification-based complexity classes. We say that $R_{\mathscr{C}',\mathscr{P}'}(c',s')$ is a* restricted variant *of $R_{\mathscr{C},\mathscr{P}}(c,s)$ if $\mathscr{C}' = \mathscr{C}$, $c' = c$, $s' = s$, and $\mathscr{P}' \subset \mathscr{P}$. The set $R = \mathscr{P} \setminus \mathscr{P}'$ is called the* restriction.

We can now lift the idea of Single-Merlin Approximation (Definition 4) to deal with generic verification-based complexity classes.

Definition 8 (Relaxed Approximation)**.** *Let $A = R_{\mathscr{C},\mathscr{P}}(c,s)$ and $B = R_{\mathscr{C},\mathscr{P}'}(c,s)$ be a verification-based class and one of its restricted versions, respectively. Let $K = \{K_{yes}, K_{NA}, K_{no}\}$ be a promise problem in B. We say that $L = \{L_{yes}, L_{NA}, L_{no}\} \in A$ is a* relaxed approximation *of K in A if and only if there exist $C \subseteq L_{yes}$, $U \subseteq L_{NA}$ and a Verifier V that recognizes L such that:*

- $K = \{L_{yes} \setminus C,\ L_{NA} \setminus U,\ L_{no} \cup C \cup U\}$,
- *the machine V has complexity $\mathscr{C}$,*
- *for each word $x \in K_{yes}$, there exists $\psi \in \mathscr{P}'$ such that* $\Pr[V(x,\psi) = 1] \geq c$.

Symmetrically to Definition 4, it is redundant to state that V is sound for L_{no}, while the requirement on K_{yes} is strictly stronger than completeness: words in K_{yes} must be accepted using a certificate from the restricted set $\mathscr{P}'$.

The notion of relaxed approximation recovers Single-Merlin approximation when $A = \mathsf{QMA}(1)$ and $B = \mathsf{QMA}(2)$, since the only *forbidden* proofs (those in $\mathscr{P} \setminus \mathscr{P}'$) are exactly the non-factorizable witnesses. What we obtain is the notion of Approximation as presented in Definition 8.

L is an *attempt* to simulate K on all words except those in $C \cup U$. If that union is empty, L is a perfect simulation of K.

Definition 9 (Non-trivial Extensions)**.** *Let $A = R_{\mathscr{C},\mathscr{P}}(c,s)$ and $B = R_{\mathscr{C},\mathscr{P}'}(c,s)$. Let $K \in B$ and let L be a relaxed approximation of K in A with extensions C, U. We say that C, U are* non-trivial *if and only if $C \cup U \neq \emptyset$.*

If both C and U are empty we say the approximation is *perfect* and the extensions are *trivial*.

Lemma 5. *Let $A = R_{\mathscr{C},\mathscr{P}}(c,s)$ and $B = R_{\mathscr{C},\mathscr{P}'}(c,s)$ with $A \subsetneq B$. Let $K \in B \setminus A$. Every relaxed approximation of K in A is non-perfect.*

Proof. Let L be a perfect approximation of K in A. Since L is perfect, $C = U = \emptyset$, so $L = K$ and $K \in A$, contradicting $K \notin A$. □

The result is clear: it is impossible to perfectly approximate a problem $K \notin A$ with a problem $L \in A$.

We now turn to a central result of this section, showing that whenever we have $A = R_{\mathscr{C},\mathscr{P}}(c,s)$ and $B = R_{\mathscr{C},\mathscr{P}'}(c,s)$, every problem in B has an approximation in A. First we characterize what kind of restriction is called *simple*.

Definition 10 (Simple Restriction)**.** *Let $A = R_{\mathscr{C},\mathscr{P}}(c,s)$ and $B = R_{\mathscr{C},\mathscr{P}'}(c,s)$. We say that the restriction $R = \mathscr{P} \setminus \mathscr{P}'$ is* simple *if there exists a function $\varphi : \mathscr{P} \to \mathscr{P}'$ such that φ^{-1} exists and is computable with complexity $\mathscr{C}$.*

Informally, a restriction is simple if any forbidden proof can be encoded into a non-forbidden one such that the decoding is done efficiently. For example, let $\mathscr{P}$ and $\mathscr{P}'$ be the proof sets of $\mathsf{QMA}(1)$ and $\mathsf{QMA}(2)$, respectively. A non-factorizable forbidden proof $|\psi\rangle$ can be mapped to $|\psi'\rangle = |\psi\rangle \otimes |0\rangle$—a factorizable proof obtained by adding one extra qubit—and this extra qubit can be discarded to recover $|\psi\rangle$.

Definition 11 (Simply restricted classes)**.** *Let $A = R_{\mathscr{C},\mathscr{P}}(c,s)$ and $B = R_{\mathscr{C},\mathscr{P}'}(c,s)$, with $R = \mathscr{P} \setminus \mathscr{P}'$ simple. We say that (A,B) are* simply restricted classes *with restriction R.*

Henceforth, within the context of (A,B) simply restricted classes, $\mathscr{P}$and $\mathscr{P}'$ denote the proof sets of A and B, respectively.

Lemma 6. *Let (A, B) be simply restricted classes with restriction R. It holds that $A \subseteq B$.*

Proof. Let $L \in A$ be a promise problem accepted by V_A in complexity $\mathscr{C}$. We construct a machine V_B that uses proof set $\mathscr{P}'$ and recognizes L, showing $L \in B$. Given a proof $\psi \in \mathscr{P}'$, the machine V_B computes $\varphi^{-1}(\psi) \in \mathscr{P}$and runs V_A on the result. Since φ^{-1} is computable in time $\mathscr{C}$ and V_A runs in time $\mathscr{C}$, and $\mathscr{F}$ is closed under composition, V_B has complexity $\mathscr{C}$.

For $x \in L_{\text{yes}}$ there exists $\psi_A \in \mathscr{P}$with $\Pr[V_A(x, \psi_A) = 1] \geq c$. Since the restriction is simple, $\varphi(\psi_A) \in \mathscr{P}'$, and

$$\Pr[V_B(x, \varphi(\psi_A)) = 1] = \Pr\big[V_A(x, \varphi^{-1}(\varphi(\psi_A))) = 1\big] = \Pr[V_A(x, \psi_A) = 1] \geq c.$$

For $x \in L_{\text{no}}$, $\Pr[V_A(x, \psi_A) = 1] \leq s$ for every $\psi_A \in \mathscr{P}$. Since $\mathscr{P}' \subset \mathscr{P}$, no certificate in $\mathscr{P}'$ can violate the soundness of V_B. Hence $L \in B$. □

With the above Lemma we proved how inclusions between complexity classes can be established via the concept of restricted variant (Definition 7). The next result is crucial to connect that notion with approximations.

Lemma 7. *Let (A, B) be simply restricted classes with restriction R. For every promise problem $K = \{K_{yes}, K_{NA}, K_{no}\} \in B$, there exists a relaxed approximation of K in A.*

Proof. Let $K \in B$ be accepted by machine V_B, complete for K_{yes} and sound for K_{no}. We define an *unrestricted* machine V_A that works exactly as V_B. We claim V_A witnesses an approximation of K in A.

By construction, V_A runs in time $\mathscr{C}$. For every $x \in K_{\text{yes}}$, there exists $\psi_B \in \mathscr{P}'$ with $\Pr[V_B(x, \psi_B) = 1] \geq c$. Since $\mathscr{P}' \subset \mathscr{P}$, we have $\psi_B \in \mathscr{P}$ as well, and $\Pr[V_A(x, \psi_B) = 1] = \Pr[V_B(x, \psi_B) = 1] \geq c$. Therefore V_A is complete for K_{yes}.

For $x \in K_{\text{no}}$, there may exist $\psi_A \in \mathscr{P} \setminus \mathscr{P}'$ that fool V_A. Define

$$\psi^x_{\max} = \arg\max_{\psi \in \mathscr{P}} \Pr[V_A(x, \psi) = 1].$$

Splitting according to the achieved probability: if it is at least c, put x into C; if it lies in (s, c), put x into U; otherwise $x \in K_{\text{no}} \setminus (C \cup U)$.

The promise problem L is defined as $L_{\text{yes}} = K_{\text{yes}} \cup C$, $L_{\text{NA}} = K_{\text{NA}} \cup U$, and $L_{\text{no}} = K_{\text{no}} \setminus (C \cup U)$. Then L is an approximation of K in A with witness V_A and extensions C, U. □

The nature of the extensions C and U is key to the main result of this section. Before stating it, we introduce a useful concept parallel to that of non-factorizable extensions.

Definition 12 (Non-Compliant Extensions)**.** *Let (A, B) be simply restricted classes with restriction R. Let $K \in B$ and let $L \in A$ be its approximation with extensions C, U and witness V. We say that C, U are* non-compliant *if and only if*

$$\forall x \in (C \cup U),\ \forall \psi \in \mathscr{P}\big(\Pr[V(x, \psi) = 1] > s \ \Rightarrow\ \psi \notin \mathscr{P}'\big).$$

Lemma 8. *Let (A, B) be simply restricted classes with restriction R. Let $K \in B$ with $K \notin A$. There exists an approximation L of K with non-compliant non-trivial extensions C and U.*

Proof. The existence of L follows from Lemma 7. Non-triviality of C, U follows from Lemma 5.

The sets C and U contain those $x \in K_{\text{no}}$ for which there exists $\psi \in \mathscr{P}$with $\Pr[V(x, \psi) = 1] > s$. Since $x \in K_{\text{no}}$ and the machine recognising K (restricted to $\mathscr{P}'$) is sound, such ψ cannot belong to $\mathscr{P}'$. Therefore C and U are non-compliant. □

We can now prove the other direction.

Lemma 9. *Let (A, B) be simply restricted classes with restriction R. Let $K = \{K_{yes}, K_{NA}, K_{no}\}$ be a promise problem with an approximation in A with non-trivial non-compliant extensions. Then $K \in B$.*

Proof. Let $L \in A$ be the approximation of K, witnessed by V_A, with C, U non-trivial and non-compliant. We construct a restricted verifier V_B that works exactly as V_A. By definition of approximation, V_B runs in time $\mathscr{C}$, is complete for K_{yes}, and sound for $K_{\text{no}} \setminus (C \cup U)$.

For $x \in C$, suppose $\psi \in \mathscr{P}$with $\Pr[V_A(x, \psi) = 1] > s$. Since C is non-compliant, $\psi \notin \mathscr{P}'$. Hence no $\psi \in \mathscr{P}'$ can violate soundness, and V_B is sound for C. The same holds for U.

Therefore V_B has complexity $\mathscr{C}$, is complete for K_{yes}, sound for $L_{\text{no}} \cup (C \cup U) = K_{\text{no}}$, and uses proof set $\mathscr{P}'$, so $K \in B$. □

To conclude, we state our general result, which joins all the above.

Theorem 2 (Generalisation)**.** *Let $A = R_{\mathscr{C},\mathscr{P}}(c, s)$ and $B = R_{\mathscr{C},\mathscr{P}'}(c, s)$ be a verification-based class and one of its restricted versions, with $R = \mathscr{P} \setminus \mathscr{P}'$ simple. Then $A \neq B$ if and only if there exists $K \notin A$ such that K has an approximation in A with non-trivial non-compliant extensions.*

Proof. If $A \neq B$, there exists $K \in B$ with $K \notin A$. By Lemma 7, K has an approximation in A with non-trivial non-compliant extensions. Conversely, if K has an approximation in A with non-trivial non-compliant extensions and $K \notin A$, then by Lemma 9, $K \in B$, so $A \neq B$. □

Theorem 2 is the generalised version of Theorem 1, and the approximation notion turns out to be a novel way to prove separation between verification-based complexity classes. We believe these results are a step forward in understanding not only the relation between quantum complexity classes, but verification-based classes more broadly.

5. Conclusions

The classes QMA(1) and QMA(2) are the quantum counterpart of Merlin-Arthur classes with one and two proofs, respectively. While it has been proved that QMA(k) = QMA(2) for $k \geq 2$ [7], the question of whether QMA(1) = QMA(2) remains open. A milestone was obtained in [1] with the non-existence of a *perfect disentangler*. Since then, the QMA(1) vs. QMA(2) question has been approached via equivalence with classical complexity classes such as NEXP [3].

In this paper, we introduced a novel perspective on the QMA(1) vs. QMA(2) problem by focusing on rejection capabilities. We proved that for any $K \in$ QMA(2) there exists a promise problem $L \in$ QMA(1) that differs from K only in its rejected words. By formalizing the verifier that recognizes L, we developed the notion of *Single-Merlin approximation* and used it to establish a necessary and sufficient condition for QMA(1) $\neq$ QMA(2): if the two classes differ, there must exist a problem $K \in$ QMA(2) all of whose Single-Merlin approximations fail to fully capture K, witnessing the difference through non-factorizable certificates.

Extending beyond this specific case, we introduced verification-based complexity classes and characterized the difference between two such classes in terms of their proof sets. We generalized Single-Merlin approximation to *relaxed approximation*, a versatile tool for analyzing class separations, and showed that the QMA(1) vs. QMA(2) result is a special case of this broader framework.

Our findings offer a new approach for proving separations between complexity classes, particularly in cases where separation is conjectured but remains unproven. Future research could explore applications of our method to other quantum and classical complexity classes, potentially resolving long-standing open questions in computational complexity theory.

6. Declaration on generative AI

During the preparation of this work, the authors used **ChatGPT, Google Gemini and Claude** in order to: **paraphrase and reword, improve writing style and check grammar and spelling**. After using these tools and services, the authors reviewed and edited the content as needed and take full responsibility for the publication's content

References

[1] S. Aaronson, S. Beigi, A. Drucker, B. Fefferman, P. Shor, The power of unentanglement, IEEE Computer Society, 2008, p. 223–236. doi:10.1109/CCC.2008.5.

[2] F. G. Brandão, M. Christandl, J. Yard, A quasipolynomial-time algorithm for the quantum separability problem, in: Proceedings of the forty-third annual ACM symposium on Theory of computing, STOC'11, ACM, 2011, p. 343–352. doi:10.1145/1993636.1993683.

[3] S. Gharibian, M. Santha, J. Sikora, A. Sundaram, J. Yirka, Quantum generalizations of the polynomial hierarchy with applications to QMA(2), Computational Complexity 31 (2022). doi:10.1007/s00037-022-00231-8.

[4] F. G. Jeronimo, P. Wu, The power of unentangled quantum proofs with non-negative amplitudes, 2024. URL: https://arxiv.org/abs/2402.18790. arXiv:2402.18790.

[5] R. Bassirian, B. Fefferman, K. Marwaha, Quantum merlin-arthur and proofs without relative phase, 2023. URL: https://arxiv.org/abs/2306.13247. arXiv:2306.13247.

[6] R. Bassirian, B. Fefferman, I. Leigh, K. Marwaha, P. Wu, Quantum merlin-arthur with an internally separable proof, 2024. URL: https://arxiv.org/abs/2410.19152. arXiv:2410.19152.

[7] A. W. Harrow, A. Montanaro, Testing product states, quantum merlin-arthur games and tensor optimization, J. ACM 60 (2013). doi:10.1145/2432622.2432625.

[8] C. H. Papadimitriou, Computational Complexity, John Wiley and Sons Ltd., GBR, 1993, p. 260–265.

[9] O. Goldreich, On Promise Problems: A Survey, Springer Berlin Heidelberg, 2006, pp. 254–290. doi:10.1007/11685654_12.

[10] S. Gharibian, The 7 faces of quantum NP, ACM SIGACT News 54 (2023) 54–91. doi:10.1145/3639528.3639535.

Appendix on Languages, Problems, QMA(1), and QMA(2)

Let Σ be a finite set of symbols, or *alphabet*. In classical complexity theory, a *problem* P is represented by a language $L \subseteq \Sigma^*$ consisting of all words that constitute correct solutions to P.

For instance, consider the problem of deciding whether two graphs are isomorphic. The corresponding language L includes all pairs of graphs for which an isomorphism exists. A language L is decided by a Turing Machine M if

$$M(x) = 1 \;\leftrightarrow\; x \in L.$$

Every word $y \notin L$ must be *rejected* by M, i.e., M outputs 0. The complement $\overline{L} = \{0,1\}^* \setminus L$ contains all such words, which split naturally into two categories:

- Words $y \in \overline{L}$ encoding pairs of non-isomorphic graphs.
- Words $z \in \overline{L}$ that do not encode a valid graph at all, representing *invalid* inputs.

Thus, before proceeding, a machine M must verify whether the input is well-formatted. When defining a problem P through a language L, one prefers $\overline{L}$ to consist solely of correctly formatted inputs that do not satisfy the property defined by P. This can be handled in two ways:

1. Assume all inputs are well-formed.
2. Use the notion of *promise problems*.

A promise problem P is defined by a pair of languages $P_{\text{yes}} \subseteq \Sigma^*$ and $P_{\text{no}} \subseteq \Sigma^*$ with $P_{\text{yes}} \cap P_{\text{no}} = \emptyset$. The words in P_{yes} correspond to the language L. Unlike $\overline{L}$, however, P_{no} consists only of well-formatted inputs that must be rejected. The union $P_{\text{yes}} \cup P_{\text{no}}$ is the *promise*, and $\Sigma^* \setminus (P_{\text{yes}} \cup P_{\text{no}})$ contains invalid inputs.

From this point forward, we assume all problems to be promise problems. We write P_{NA} for $\Sigma^* \setminus (P_{\text{yes}} \cup P_{\text{no}})$. A promise problem P is thus represented as $P = \{P_{\text{yes}}, P_{\text{NA}}, P_{\text{no}}\}$, with $P_{\text{yes}} \cap P_{\text{no}} = \emptyset$ and $P_{\text{yes}} \cup P_{\text{no}} = \Sigma^* \setminus P_{\text{NA}}$.

For further discussion on promise problems, see [9]. Promise problems play a crucial role in defining complexity classes in quantum computation, such as BQP, QMA(1), and QMA(2).

Before introducing these complexity classes, we define families of quantum circuits, following [10].

Definition 13 (P-uniform quantum circuit family)**.** *A family of quantum circuits $\{C_n\}$ is* P*-uniform if there exists a polynomial-time Turing Machine M that, given input 1^n, outputs a classical description of C_n.*

Definition 14 (BQP)**.** *Let $P = \{P_{yes}, P_{NA}, P_{no}\}$ be a promise problem. The problem P belongs to* BQP *if there exists a* P*-uniform quantum circuit family $\{C_n\}$ such that for every input $x \in \{0,1\}^n$, the circuit C_n operates on $n + m$ qubits with $m \in \mathrm{poly}(n)$, and a measurement of the output qubit satisfies:*

- *If $x \in P_{yes}$, then C_n accepts with probability at least $\frac{2}{3}$.*
- *If $x \in P_{no}$, then C_n accepts with probability at most $\frac{1}{3}$.*

The acceptance condition for P_{yes} is *completeness*; the bound for P_{no} is *soundness*.

This definition is the quantum analogue of BPP. Similarly, we introduce the quantum analogue of NP using the notion of a *certificate*. A language belongs to NP if and only if

$$L \in \mathsf{NP} \leftrightarrow \left(\exists \mathscr{R} \subseteq \Sigma^* \times \Sigma^* \mid x \in L \leftrightarrow \exists y \text{ s.t. } (x, y) \in \mathscr{R}\right),$$

where the certificate y has polynomial length and $\mathscr{R}$ is polynomially decidable. Extending this characterisation to the quantum setting gives one of the seven possible definitions of Quantum NP [10], namely the class QMA—equivalently, QMA(1)—defined as follows.

Definition 15 (Quantum Merlin-Arthur)**.** *Let $P = \{P_{yes}, P_{NA}, P_{no}\}$ be a promise problem. The problem P belongs to* QMA *if there exists a* P*-uniform quantum circuit family $\{C_n\}$ such that for every input $x \in \{0,1\}^n$, the circuit C_n takes $n + p + m$ qubits with $m, p \in \mathrm{poly}(n)$, and a measurement of the output qubit satisfies:*

- *If $x \in P_{yes}$, then there exists a quantum proof $|\psi\rangle \in \mathbb{C}^{2^p}$ such that C_n accepts with probability at least $\frac{2}{3}$.*
- *If $x \in P_{no}$, then for all quantum proofs $|\psi\rangle$, C_n accepts with probability at most $\frac{1}{3}$.*
- *If $x \in P_{NA}$, the circuit may accept or reject arbitrarily.*

This definition can equivalently be framed using a polynomial-time quantum verifier V. Writing $\Pr[V(x, |\psi\rangle) = 1]$ for the probability of acceptance, completeness and soundness become:

- **(Completeness)** If $x \in P_{\text{yes}}$, then there exists $|\psi\rangle$ with $\Pr[V(x, |\psi\rangle) = 1] \geq \frac{2}{3}$.
- **(Soundness)** If $x \in P_{\text{no}}$, then for all $|\psi\rangle$, $\Pr[V(x, |\psi\rangle) = 1] \leq \frac{1}{3}$.

If V is both complete for P_{yes} and sound for P_{no}, we say that V *recognises* P.

The class QMA is sometimes denoted QMA(c, s), where $c, s \in [0, 1]$ are the completeness and soundness parameters. Our definition corresponds to QMA$(\frac{2}{3}, \frac{1}{3})$.

A natural question is whether multiple quantum proofs increase the expressiveness of the QMA model. The class QMA(k) is the extension where the verifier receives k quantum proofs. In [7] it was proved that QMA(k) = QMA(2) for any $k > 2$, i.e., QMA(k, c, s) = QMA$(2, \frac{2}{3}, \frac{1}{3})$ = QMA(2). Whether QMA(1) = QMA(2) remains open.