Quantum Merlin-Arthur with multiple Merlins: a survey

Wei Zheng Teo, Sandip Nair

April 29, 2022

Contents

1 Introduction

It has been demonstrated time and again that quantum algorithms have the potential to solve certain problems much more efficiently than classical algorithms. Therefore, it is imperative to study how much more powerful quantum computation is compared to classical computation, in order to better understand the limits of computation. The computational complexity community has introduced complexity classes dedicated to quantum computation in order to study the power of quantum computation, and our report will be about one such complexity class: quantum Merlin-Arthur (QMA). QMA can be considered as a single-message interactive proof system in which the prover (Merlin) sends a quantum state as a proof to the verifier (Arthur), and the verifier has to decide using the proof whether an input string belongs to a language. For our project in particular, we look at the question of whether multiple Merlins can grant us additional computational power. In classical Merlin-Arthur (MA), multiple Merlins are no different from a single Merlin, but it appears that multiple Merlins are more powerful than a single Merlin in the quantum case due to quantum phenomena such as entanglement. In this report, we will summarize some of the work and discoveries with regards to this question. We will show a detailed proof sketch of how $\mathsf{QMA}(k) = \mathsf{QMA}(2)$ (that is, QMA with k and 2 Merlins respectively), and demonstrate some supporting evidence that suggests $\mathsf{QMA}(2) \neq \mathsf{QMA}$.

The layout of the remainder of this report is as follows: we first present some relevant background about the MA and QMA complexity classes in Section 2. In Section 3, we go through some attempts to prove $\mathsf{QMA}(k) = \mathsf{QMA}(2)$ and a detailed proof sketch of Harrow & Montanaro's (2013) proof of $\mathsf{QMA}(k) = \mathsf{QMA}(2)$. In Section 4, we go through some arguments (albeit not complexity-theoretic ones) that support the case for $\mathsf{QMA}(2) \neq \mathsf{QMA}$, and also introduce some problems that are known to be in QMA and $\mathsf{QMA}(2)$. Finally, in Section 5, we go through some of the other open problems with regards to QMA.

2 Background

2.1 Complexity classes and interactive proofs

Formally, a complexity class defines a set of languages for which we are able to determine whether an input string belongs to that language (i.e. we can determine the membership of an input string in that language), using some model of computation. For example, the P (polynomial time) complexity class contains the set of all languages for which we can determine the membership of an input string in polynomial time with a deterministic Turing machine. In general, these membership problems can be used as an abstraction for much more practical problems, and therefore the study of complexity classes is crucial to understanding on a theoretical level the kinds of problems that we can or cannot solve using computation with reasonable resources. One of the most important unsolved questions of computer science and mathematics is the question of whether $\mathsf{P} = \mathsf{NP}$, and proving either result will cause widespread ramifications throughout the whole mathematical and scientific community.

Interactive proofs are a model of computation that can be used to solve the membership problem

as described earlier. As the name suggests, an interactive proof involves interaction between two parties, a prover and a verifier. The job of the verifier is to determine if an input string is in a given language, and the prover's job is to try and convince the verifier that the input string is indeed in the language. We typically consider the prover to have unlimited resources and the verifier to have limited resources (i.e. time and space polynomial in the length of the input string). The prover and verifier can interact by sending messages to each other, and at the end of the interaction, the verifier has to produce a binary output (accept/reject) which is the verifier's guess of whether the input string belongs to the language. Many of the most studied complexity classes can in fact be modelled under an interactive proof system. For example, the P complexity class can be seen as a zero-message interactive proof in which the verifier executes a deterministic polynomial time by itself to determine the membership of the input string. This is similar for the classes BPP (bounded-error probabilistic polynomial time) and BQP (bounded-error quantum polynomial time), except that the verifier now runs a bounded-error probabilistic or quantum algorithm for BPP and BQP respectively. However, we note that since these algorithms can produce wrong outcomes due to their probabilistic nature, we typically require these algorithms to produce the correct output at least $\frac{2}{3}$ of the time (*completeness* condition) and the wrong output at most $\frac{1}{3}$ of the time (*soundness* condition). In practice, the completeness and soundness gap can be amplified to tend exponentially close to 1 simply through repetition. Lastly, we can model the NP (non-deterministic polynomial time) complexity class as a single message interactive proof, where the prover sends a polynomial-size proof to the verifier and the verifier checks the proof with a deterministic polynomial time algorithm. There are many other complexity classes that can be modelled with interactive proofs, and one interesting fact is that the complexity class IP (which contains all the languages that we can use an interactive proof system to determine membership) is equal to the complexity class PSPACE (the set of all languages for which we need polynomial space to determine membership) (Shamir, 1992).

2.2 Merlin-Arthur

The Merlin-Arthur complexity class MA is very similar to the complexity class NP. Both NP and MA are single-message interactive proof systems, with the prover sending a single proof to the verifier for checking. The difference is that in NP, the verifier runs a deterministic polynomial-time algorithm, while for MA, the verifier can run a probabilistic polynomial-time algorithm. Due to the probabilistic nature of the verifier, we now have to also define error bounds like in BPP and BQP. The key concept to capture is that if the input string is in the language, the prover should be able to convince the verifier of this, and if not, the prover should not be able to falsely convince the verifier that the string is in the language. With this, we have the following definition:

Definition 1 *Let $\mathcal{L}$ be a language in* MA*. Let x be the input string. Then there exists a probabilistic polynomial-time algorithm V such that:*

- *If $x \in \mathcal{L}$, then there exists a string y with $|y| = poly(|x|)$ such that $V(x, y) = 1$ (i.e. V accepts) with probability at least $\frac{2}{3}$ (completeness).*
- *If $x \notin \mathcal{L}$, then for every string y with $|y| = poly(|x|)$, $V(x, y) = 1$ (i.e. V accepts) with probability at most $\frac{1}{3}$ (soundness).*

Finally, one thing to note about MA is that Arthur refers to the verifier and Merlin refers to the prover, as a reference to the mortal and oracle capabilities of Arthur and Merlin in folklore. In this report, we will freely interchange between the terms prover/verifier and Merlin/Arthur. Additionally, the MA complexity class should not be confused with the Arthur-Merlin complexity class AM. In AM, Arthur has to first tell Merlin about its random rolls (a.k.a. coin tosses), before Merlin sends Arthur a proof. From then on, Arthur can only run a deterministic polynomial-time algorithm using its coin tosses and Merlin's proof.

2.3 Quantum Merlin-Arthur

As its name suggests, Quantum Merlin-Arthur (QMA) is the quantum version of MA. In QMA, Merlin can now send a quantum state as a proof, and Arthur can run a quantum algorithm. Therefore, the definition of QMA is very similar to MA.

Definition 2 *Let $\mathcal{L}$ be a language in* QMA*. Let x be the input string. Then there exists a polynomial-time quantum algorithm V such that:*

- *If $x \in \mathcal{L}$, then there exists a state $|\psi\rangle$ with poly$(|x|)$ qubits such that $V(|x\rangle, |\psi\rangle) = 1$ (i.e. V accepts) with probability at least $\frac{2}{3}$ (completeness).*
- *If $x \notin \mathcal{L}$, then for every state $|\psi\rangle$ with poly$(|x|)$ qubits, $V(|x\rangle, |\psi\rangle) = 1$ (i.e. V accepts) with probability at most $\frac{1}{3}$ (soundness).*

If one refers to BQP as the quantum analogue of P, then one can refer to QMA as the quantum analogue of NP.

2.4 Multiple Merlins

Expanding on the interactive proof system, one can consider a system in which there is more than one Merlin. We denote the MA complexity class and the QMA complexity class with k Merlins as $\mathsf{MA}(k)$ and $\mathsf{QMA}(k)$ respectively (with k being polynomial). Do multiple Merlins make a difference in the computations that can be done, i.e. are there languages for which we cannot solve the membership problem with one Merlin, but we can if we use more than one Merlin? For the case of $\mathsf{MA}(k)$, we have a very simple argument that shows that $\mathsf{MA} = \mathsf{MA}(k)$. In $\mathsf{MA}(k)$, the k Merlins send Arthur k proofs in total, and Arthur executes its algorithm using these k proofs. However, we do not actually need k Merlins to send k proofs, and they can all be sent by just one Merlin by concatenating the proofs. The total size of the proofs sent is still polynomial since k is polynomial and each individual proof is polynomial-size. Therefore, we can simulate any $\mathsf{MA}(k)$ procedure with one Merlin, i.e. $\mathsf{MA}(k) \subseteq \mathsf{MA}(k)$. Clearly $\mathsf{MA} \subseteq \mathsf{MA}(k)$ since Arthur can just ignore all proofs other than the first one so as to simulate an MA algorithm. Therefore, $\mathsf{MA} = \mathsf{MA}(k)$.

For $\mathsf{QMA}(k)$, it is in fact an open problem whether $\mathsf{QMA}(k) = \mathsf{QMA}$ (or just $\mathsf{QMA}(2) = \mathsf{QMA}$; we show a proof sketch of $\mathsf{QMA}(k) = \mathsf{QMA}(2)$ in this report). The classical method of simply having a single Merlin concatenate multiple proofs does not work in the quantum case. While k independent Merlins are guaranteed to provide a product of k unentangled states, a single Merlin

who is supposed to send a product of k states might cheat by entangling the k states. There is no straightforward way to convert a generic states to a product of k states (Aaronson et al., 2008), nor check whether a single state is a k-partite state or far from any k-partite state (Harrow & Montanaro, 2013). Therefore, it appears that a single Merlin cannot easily simulate a multiple-Merlin protocol, and thus having multiple Merlins seems to lend us additional computational power, although there is no formal complexity-theoretic proof of this yet.

3 QMA(k) = QMA(2)

In this section we will first go through some previous work that have attempted to prove $\mathsf{QMA}(k) = \mathsf{QMA}(2)$, and present a proof sketch of Harrow & Montanaro's (2013) theorem that $\mathsf{QMA}(k) = \mathsf{QMA}(2)$.

3.1 Previous work

The notion of $\mathsf{QMA}(k)$ was first introduced by Kobayashi et al. (2003). We will use the notation used by Kobayashi et al. (2003) in this paper.

Definition 3 *Let $\mathcal{L}$ be a language in $\mathsf{QMA}(k, c, s)$. Let x be the input string. Then there exists a polynomial-time quantum algorithm V such that:*

- *If $x \in \mathcal{L}$, then there exists states $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_k\rangle$ with poly($|x|$) qubits such that $V(|x\rangle, |\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_k\rangle) = 1$ (i.e. V accepts) with probability at least c (completeness).*
- *If $x \notin \mathcal{L}$, then for every set of k states $|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_k\rangle$ with poly($|x|$) qubits, $V(|x\rangle, |\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_k\rangle) = 1$ (i.e. V accepts) with probability at most s (soundness).*

Furthermore, we define $\mathsf{QMA}(k, \frac{2}{3}, \frac{1}{3}) = \mathsf{QMA}(k)$ and $\mathsf{QMA}(1) = \mathsf{QMA}$.

Kobayashi et al. (2003) also proposed a method of reducing the number of Merlins at the expense of soundness. They showed that

$$\mathsf{QMA}(3k + r, 1 - \varepsilon, 1 - \delta) \subseteq \mathsf{QMA}(2k + r, 1 - \frac{\varepsilon}{2}, 1 - \frac{\delta}{20})$$

We now present a brief illustration of this procedure using a reduction from 3 to 2 Merlins (as described by Kobayashi et al. (2003)). The generic case of reducing from $3k + r$ to $2k + r$ Merlins is a generalization of this procedure. Let V be the verification algorithm in the $\mathsf{QMA}(3, 1-\varepsilon, 1-\delta)$ system (which also describes a unitary) taking in an input x. Let $q_{\mathcal{V}}(|x|)$ be the number of private qubits used by V, and let $q_{\mathcal{M}}(|x|)$ be the number of qubits in each proof, where $q_{\mathcal{V}}$ and $q_{\mathcal{M}}$ are polynomials. Let $|\phi_1\rangle, |\phi_2\rangle, |\phi_3\rangle$ be the 3 proofs that are expected to be sent in this system. Now, let the verifier for the $\mathsf{QMA}(2, 1 - \frac{\varepsilon}{2}, 1 - \frac{\delta}{20})$ system be W. W requires four registers R_1, R_2, S_1, S_2 (each having $q_M(|x|)$ qubits) for storing the proofs, one register T (with $q_{\mathcal{V}}(|x|)$ qubits) for its private qubits, and a single-qubit register B. W now expects to receive proofs $|\psi_1\rangle = |\phi_1\rangle \otimes |\phi_3\rangle$ and $|\psi_2\rangle = |\phi_2\rangle \otimes |\phi_3\rangle$. When W receives the proofs $|\psi_1\rangle, |\psi_2\rangle$, they are stored in registers (R_1, S_1) and (R_2, S_2) respectively. Then W does one of the following (each with $\frac{1}{2}$ probability):

- Separability test: do a controlled swap test on S_1 and S_2 using B as the control bit, i.e. first apply a Hadamard gate to B, use B to control the swap of registers S_1 and S_2, apply a Hadamard gate to B again and measure B.
- Consistency test: simply apply the original procedure V to registers T, R_1, R_2, S_1.

To show completeness, we can show that having two accepting proofs as expected would always pass the separability test, since the controlled swap test always passes when swapping identical states, and indeed S_1 and S_2 are supposed to both contain $|\phi_3\rangle$. The consistency test is simply the original verifier algorithm which has a completeness of $1-\varepsilon$. Therefore, the overall completeness probability is now $1-\frac{\varepsilon}{2}$. To show soundness, they showed considered $\mathrm{Tr}(\rho\sigma)$, the trace of the product of the density matrices of the states in S_1 and S_2. If $\mathrm{Tr}(\rho\sigma) \leq 1-\frac{\delta}{5}$, the separability test passes with probability at most $1-\frac{\delta}{10}$, and if $\mathrm{Tr}(\rho\sigma) > 1-\frac{\delta}{5}$, the consistency test passes with probability at most $1-\frac{\delta}{10}$ as well. Therefore, the overall soundness is upper bounded by $1-\frac{\delta}{20}$.

The main problem with Kobayashi et al.'s (2003) reduction is the issue of increasing soundness. To use this method to show that $\mathsf{QMA}(k) = \mathsf{QMA}(2)$, we have to assume the possibility of reducing the soundness probability. In classical settings, this is usually achieved through simple repetition. We can make use of independent runs of the algorithm, and accept/reject based on what fraction of all runs accepted. Using Chernoff bounds, we can obtain a soundness probability that decreases exponentially with the number of runs. In QMA settings, we can simulate repetitions by having each Merlin send r copies of a proof if there are to be r repetitions. However, due to the quantum nature of the proofs, a dishonest Merlin (attempting to convince Arthur that the input x is in the language when it is not) can choose to entangle the copies of the proof. Then when Arthur runs its verifier algorithm on one of these copies, he can introduce entanglement into the previously unentangled proofs from the independent Merlins that have not been measured yet. This is the phenomenon of *entanglement swapping*, and its occurrence implies that the proofs are no longer guaranteed to be unentangled, when previously we assumed that the proofs are unentangled. Therefore, our arguments for completeness and soundness break down. We demonstrate a simple illustration of entanglement swapping here:

$$
\begin{aligned}
|\psi_1\rangle_{AB} &= |\Psi^+\rangle \\
|\psi_2\rangle_{CD} &= |\Psi^-\rangle \\
|\psi\rangle_{ABCD} &= |\psi_1\rangle_{AB}|\psi_2\rangle_{CD} \\
|\psi\rangle_{BCAD} &= \frac{1}{2}\left(|\Psi^+\rangle_{BC}|\Psi^-\rangle_{AD} + |\Psi^-\rangle_{BC}|\Psi^+\rangle_{AD} + |\Phi^+\rangle_{BC}|\Phi^-\rangle_{AD} + |\Phi^-\rangle_{BC}|\Phi^+\rangle_{AD}\right)
\end{aligned}
$$

In this example, when we measure qubits B and C in the Bell basis, the unmeasured qubits A and D become one of the Bell states as well and hence are entangled, even though these two qubits were previously unentangled.

Aaronson et al. (2008) also proposed a reduction from $\mathsf{QMA}(k)$ to $\mathsf{QMA}(2)$, by proposing a method to minimize the impact of entanglement swapping. The idea is to have the Merlins send a lot more copies of the proof than Arthur is going to check (although still a polynomial number of them), and Arthur picks the copies to check uniformly at random. After measuring each copy, the remaining unmeasured copies are supposed to be close to separable, as the entanglement will be

more "spread out" among the large number of copies. However, results from König & Renner (2005) show that we require an exponential number of copies to achieve this. Aaronson et al. (2008) however proposed that using a suitable measure of entanglement, we only need a polynomial amount of copies. One measure of entanglement that is conjectured to obey these properties is the *entanglement of formation* (Bennett et al., 1996), but this conjecture is only true if we assume that a weak version of the Additivity Conjecture (King & Ruskai, 2001; Shor, 2004) is true (note that the actual Additivity Conjecture was proven false (Hastings, 2009)). As of now, this assumption has not yet been proven to be true.

3.2 Proof of QMA(k) = QMA(2)

Finally, we present a detailed proof sketch of Harrow & Montanaro's (2013) proof of $\mathsf{QMA}(k) = \mathsf{QMA}(2)$. Let V be the original $\mathsf{QMA}(k, c, s)$ verifier algorithm. If the input x is in the language, then let $|\phi_1\rangle, |\phi_2\rangle, \ldots |\phi_k\rangle$ be the proofs that would be accepted by V with probability at least c. Let W be the algorithm for 2 Merlins, and if x is in the language, W expects to receive two copies $|\psi_1\rangle$ and $|\psi_2\rangle$ that are both $|\phi_1\rangle|\phi_2\rangle \ldots |\phi_k\rangle$. Then with $\frac{1}{2}$ probability each, W does one of the following:

- Perform product test using $|\psi_1\rangle$ and $|\psi_2\rangle$ as input.
- Use one of $|\psi_1\rangle$ or $|\psi_2\rangle$ to execute V and output the same result.

We now describe the product test. The product test is simply k controlled swap tests performed on the k "proofs" of $|\psi_1\rangle$ and $|\psi_2\rangle$, and the product test accepts if and only if all of these controlled swap tests accept. The purpose of the product test is to check if the two states are k-partite (i.e. a product of k states). It is clear that if the two Merlins send the two proofs in the expected format, then the product test will always pass, since the controlled swap test passes with probability 1 if used on two identical states. Next, Harrow & Montanaro (2013) proved that if the state $|\psi\rangle = |\psi_1\rangle = |\psi_2\rangle$ has at most a $1 - \varepsilon$ overlap with any other k-partite state (i.e. $|\langle\psi|\phi\rangle|^2 \leq 1 - \varepsilon$ where $|\phi\rangle$ is a k-partite state), then the product test passes with probability at most $1 - \Theta(\varepsilon)$.

Harrow & Montanaro (2013) proved that the procedure for W above results in a completeness and soundness of $c' = \frac{1+c}{2}$ and $s' = 1 - \frac{(1-s)^2}{100}$ respectively, i.e. only a polynomial blow-up. Thus, $\mathsf{QMA}(k, c, s) \subseteq \mathsf{QMA}(2, c', s')$. We have encountered the same problem of increasing soundness as in Kobayashi et al.'s (2003) approach, however, Harrow & Montanaro (2013) proved that in this protocol, Arthur only has to make *separable measurements*. Define SEP as the set of all measurements M that can be written in the form $M = \sum_i \alpha_i \otimes \beta_i$ for some positive semidefinite matrices $\{\alpha_i\}$ and $\{\beta_i\}$. Then we can write the stronger statement $\mathsf{QMA}(k, c, s) \subseteq \mathsf{QMA}^{SEP}(2, c', s')$, where QMA^{SEP} implies that Arthur is only allowed to make measurements belonging to SEP (and thus clearly $\mathsf{QMA}^{SEP}(k, c, s) \subseteq \mathsf{QMA}(k, c, s)$). The most important property of separable measurements is that entanglement will *not* be introduced in the unmeasured states, thus allowing us to avoid the whole problem of entanglement swapping. With this insight, we can now write $\mathsf{QMA}^{SEP}(2, c', s') \subseteq \mathsf{QMA}^{SEP}(2, (c')^r, (s')^r)$. This is achieved by simply repeating the whole procedure r times and accepting if and only if all runs accept, and this is now possible since we know that entanglement swapping will not occur. Therefore, we now have a way to reduce the soundness probability exponentially. The final issue is that the

completeness also decreases exponentially if the initial completeness $c \neq 1$. However, this can be fixed using a method introduced by both Kobayashi et al. (2003) and Aaronson et al. (2008) to bring the completeness of a $\mathsf{QMA}(k)$ procedure exponentially close to 1 with only a polynomial blow-up in soundness. The method simply involves a polynomial number of repetitions of the original algorithm (by multiplying the number of Merlins and thus achieving independent runs of the algorithm) and accepting if and only if a certain fraction of the runs accepted. We then use Chernoff bounds to calculate the increase in completeness and Markov's inequality to calculate the increase in soundness. This is the last piece of the puzzle and the final steps for converting a $\mathsf{QMA}(k)$ to $\mathsf{QMA}(2)$ procedure is as follows:

- Increase completeness to exponentially close to 1 (by introducing more Merlins to execute multiple (polynomially many) repetitions of the algorithm).
- Apply the $\mathsf{QMA}(k, c, s)$ to $\mathsf{QMA}^{SEP}(2, c', s')$ procedure.
- Repeat the everything r (polynomial) times to get completeness and soundness of $(c')^r$ and $(s')^r$.

By choosing appropriate polynomials in the first and third step above, we can eventually achieve a completeness and soundness of $1 - \exp(-p(|x|))$ and $\exp(-p(|x|))$ respectively for some polynomial p. Therefore,

$$\mathsf{QMA}(k, c, s) \subseteq \mathsf{QMA}^{SEP}(2, 1 - \exp(-p(|x|)), \exp(-p(|x|))) \subseteq \mathsf{QMA}\left(2, \frac{2}{3}, \frac{1}{3}\right) = \mathsf{QMA}(2)$$

4 QMA(2) vs. QMA

In this section, we explore some evidence which supports the claim that $\mathsf{QMA}(2) \neq \mathsf{QMA}$, which means that it is likely that having multiple Merlins does increase the possibilities of languages which can be accepted. Currently, it is not known whether this claim is true, and it is difficult to even give an oracle separation. There exist problems that are known to be in QMA(2) but their membership in QMAis unknown, which suggests that it might not be possible to simulate multiple Merlins using a single Merlin (simulating a QMA(2) protocol in QMA). We shall discuss briefly about one such problem: Pure State N-representability (Liu et al., 2007).

Aaronson et al. (2008) showed that the number of qubits used for a 3SAT proof can be reduced almost quadratically if a bounded number of unentangled quantum witnesses are available. It is not known how to acheieve the same improvement with a single quantum witness, again demonstrating the possible superiority of multiple quantum witnesses. In the same work, they also rule out one possibility of showing that QMA(2) protocols can be simulated in QMA, by showing that "perfect disentanglers" do not exist.

4.1 Pure State N-representability

In quantum chemistry, the *Local Hamiltonian Problem* involves determining the ground state energy of a spin Hamiltonian that is a sum of 2-local terms (in n qubits). This problem has been shown to be a QMA-*complete* problem, which means that it is in QMA and any problem in QMA can be reduced to it (Kempe et al., 2005). This work gives two proofs for this result, one using the *projection lemma* (approximating a non-local Hamiltonian by a local Hamiltonian) and elementary linear algebra, and the other based on *pertubation theory*, which is based on techniques used to analyze sums of Hamiltonians.

The N-representability problem involves verifying (up to some tolerable precision) whether a given 2-particle (fermion) density matrix represents the state of an N particle system with all particles other than the two represented by the matrix traced out from the overall quantum state of the system. Liu et al. (2007) showed that this problem is QMA-complete. A sketch of their proof is to first give a quantum verifier for a candidate solution to this problem, showing that it is in QMA. They then reduce this problem to the local Hamiltonian problem, which is QMA-complete, hence proving that N-representability is QMA-hard, and hence QMA-complete.

If it is also the case that the overall state of the N fermions in the N-representability instance is a *pure* state, then this special case is called the *pure state N-representability* problem. Here, the verifier (Arthur) is "promised" that the state of the system he receives is a pure state. The issue that arises in this case is that the prover (Merlin) can now cheat, and hand over a correlated (mixed) state to Arthur. This situation is similar to what distinguishes $\mathsf{QMA}(k)$ from QMA: in $\mathsf{QMA}(k)$, the verifier is promised to receive a tensor product of quantum states as a witness. Hence, the pure state version of the N-representability problem is contained in the complexity class $\mathsf{QMA}(k)$, which is not known to be the same as QMA, so this problem is conjectured to be harder than standard N-representability.

4.2 Proving 3SAT with $\tilde{O}(\sqrt{m})$ qubits

If φ is a 3SAT instance with n variables, if Merlin has to prove to Arthur that it is satisfiable using a single proof/witness, it has to be n bits long. This is because if there was a $o(n)$-size witness, one could iterate over all possible witnesses to have a $2^{o(n)}$ algorithm for 3SAT, which is known to be unlikely. This turns out to be true even in the quantum setting, where a $o(n)$-qubit witness for 3SAT would imply a $2^{o(n)}$-time quantum algorithm. However, if the verifier (Arthur) is given access to multiple unentangled quantum proofs, Aaronson et al. (2008) proved that 3SAT has a *sublinear* proof, which was not possible with a single quantum proof.

Theorem 1 *Let φ be a satisfiable 3SAT instance with n variables and $m \geq n$ clauses. Then its satisfiability can be proved, with perfect completeness and constant soundness, using $\tilde{O}(\sqrt{m})$ unentangled quantum proofs, each with $O(\log m)$ qubits.*

If $m = O(n)$, then the number of unentangled quantum proofs needed is $\tilde{O}(\sqrt{n}) = O(\sqrt{n}\,\mathrm{polylog}(n))$, which is almost a quadratic improvement over the linear witness size that is known to be the best possible one in both the classical and quantum setting for a single

witness, demonstrating the possible superiority of multiple witnesses.

The outline of the algorithm proposed by Aaronson et al. (2008) is as follows. We first reduce the 3SAT instance φ to a specific format of SAT using classical reductions to produce the following properties (in this order):

- Probabilistically checkable (PCP): The formula is either satisfiable, or at most a $1 - \varepsilon$ fraction of the clauses are satisfiable. Such a reduction is possible due to Dinur (2007) with a polylog(n) blowup of the size of the instance.
- Balanced: Every variable occurs in at most a constant number of clauses. Such a reduction is possible due to Papadimitriou & Yannakakis (1991) with a constant blowup of the size of the instance and without affecting the PCP property.
- 2-out-of-4 SAT: Every clause now has 4 variables, and the whole formula is satisfied if and only if two variables in each clause are set to 1. Such a reduction is possible due to Khanna et al. (2000) with a constant blowup of the size of the instance and without affecting the previous two properties.

Now let ϕ be the SAT formula equivalent to φ but in the desired format. If ϕ has a satisfying assignment and we only have one Merlin, this Merlin can send a proof of the form

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} (-1)^{x_i} |i\rangle$$

where N is the number of variables in ϕ, and $x_1, \ldots, x_N$ is a satisfying assignment for ϕ. Assuming Arthur receives such a proof, he can perform the following Satisfiability Test. Split the clauses into a constant number of blocks $B_1, \ldots B_s$ such that no variable appears in more than one clause in each block. Next, choose a uniformly random block B_r and measure $|\psi\rangle$ in the basis where each clause in B_r is a projector. Suppose that after measurement, we obtain a reduced state $|\psi_{ijkl}\rangle$ corresponding to a clause containing variables (i, j, k, l). $|\psi_{ijkl}\rangle$ will look like

$$|\psi_{ijkl}\rangle = \frac{1}{2}((-1)^{x_i}|i\rangle + (-1)^{x_j}|j\rangle + (-1)^{x_k}|k\rangle + (-1)^{x_l}|l\rangle)$$

Recall that in a satisfying assignment, exactly two variables are set to 1 (since ϕ is a 2-out-of-4 SAT instance). Thus we have $\binom{4}{2} = 6$ possible satisfying assignments out of the possible $2^4 = 16$. This gives us 3 orthogonal states (since we have 3 pairs of states, where each pair is the negation of each other), and we can perform another projective measurement to determine which of these 3 states we have. Thus, by performing another projective measurement on $|\psi_{ijkl}\rangle$, we can accept with probability 1 if this clause has two variables set to 1, and reject with constant probability otherwise. Overall, the soundness probability is constant, since we have a constant probability of encountering an unsatisfied clause (i.e. the clause does not have two variables set to 1) due to the PCP property, and a constant probability of rejecting when we measure the reduced state from such a clause.

However, if Merlin is cheating, we are not guaranteed to obtain proofs in the desired form. Therefore, we need another test to detect if the Merlins are sending states of the proper form.

Aaronson et al. (2008) used the following Uniformity Test, which requires k Merlins. Choose a matching $\mathcal{M}$ on $[N]$ randomly. Construct a basis containing orthonormal vectors $\frac{1}{\sqrt{2}}(|i\rangle + |j\rangle)$ and $\frac{1}{\sqrt{2}}(|i\rangle - |j\rangle)$ for each edge $(i,j) \in \mathcal{M}$, then measure all the proofs $|\psi_1\rangle, \ldots |\psi_k\rangle$ in this basis. What is special about this basis is that if all the k proofs are identical and in the correct format as defined earlier, then it is not possible to measure both $\frac{1}{\sqrt{2}}(|i\rangle + |j\rangle)$ and $\frac{1}{\sqrt{2}}(|i\rangle - |j\rangle)$ among the k measurements. To have a constant probability that at least two provers obtained a measurement corresponding to the same edge in $\mathcal{M}$ (and thus set up the possibility of measuring both $\frac{1}{\sqrt{2}}(|i\rangle + |j\rangle)$ and $\frac{1}{\sqrt{2}}(|i\rangle - |j\rangle)$), we require $k = \Theta(\sqrt{N}) = \tilde{O}(\sqrt{m})$ Merlins due to a generalized version of the Birthday Paradox. Therefore, the final algorithm for k Merlins is to, with probability $\frac{1}{2}$, do either: (1) execute the Satisfiability Test on a randomly chosen proof, or (2) execute the Uniformity Test. It was proved that this algorithm has perfect completeness and constant soundness (by showing that one of the tests will reject with constant soundness in all cases), and thus 3SAT is in $\mathsf{QMA}(k, 1, s)$. Based on the earlier result, this means that 3SAT is in $\mathsf{QMA}(2)$.

4.3 Non-existence of perfect "disentanglers"

Showing that $\mathsf{QMA}(2) = \mathsf{QMA}$ is to show that $\mathsf{QMA}(2)$ protocols can be simulated in QMA. One potential approach of doing this is to have the verifier (Arthur) use a *disentangler*, a quantum operation which can convert possibly entangled witness states from the prover (Merlin) into separable witness states (tensored states). Aaronson et al. (2008) showed that in finite-dimensional Hilbert spaces, there is no such disentangling operation possible.

A *superoperator* is a mapping between density matrices that preserves traces.

Definition 4 *Let $\mathcal{H}, \mathcal{K}$ be finite dimensional Hilbert spaces. A superoperator $\Phi : \mathcal{H} \to \mathcal{K} \times \mathcal{K}$ is an (ϵ, δ)-disentangler if*

1. *$\Phi(\rho)$ is ϵ-close to a separable state for every state ρ*
2. *For every separable state σ, there exists a ρ such that $\Phi(\rho)$ is δ-close to σ.*

If either ϵ or δ is non-zero but small, then such disentanglers do exist, where either there is a specific output close to every separable state or every output is close to a specific separable state. For the first approach, a classical description of the separable state to be prepared is measured in the standard basis in order to prepare it. For the second approach, for some sufficiently large N, a quantum state on $N+1$ registers $R_0, R_1, ..., R_N$ is taken, an index $i \in [N]$ is sampled uniformly at random and the joint state of R_0, R_i is output, discarding everything else. By the finite quantum de Finetti theorem (König & Renner, 2005), with high probability this state will be close to separable.

Watrous proposed the following conjecture:

Conjecture 1 *For all constants $\epsilon, \delta < 1$, any (ϵ, δ)-disentangler requires $\dim \mathcal{H} = 2^{\Omega(\dim \mathcal{K})}$.*

A proof of this conjecture would be an important formal result supporting the claim that $\mathsf{QMA}(2) \neq \mathsf{QMA}$, and could even lead to a quantum oracle separation between the two classes. In the case

where $\epsilon = \delta = 0$, that is for "perfect" disentanglers, it has been shown that they do not exist in *any* finite dimension (Aaronson et al., 2008).

Theorem 2 *Let $\Phi : \mathcal{H} \to \mathcal{K} \otimes \mathcal{K}$ be any superoperator whose image is the set of separable states. Then*

$$\dim \mathcal{K} \geq 2 \implies \dim \mathcal{H} = \infty$$

This result rules out the possibility of perfect disentanglers as an approach for simulating $\mathsf{QMA}(2)$ protocols in QMA, which suggests that a separation between these two classes might be possible.

5 Open Problems

It is still unknown whether Pure-State N-representability is $\mathsf{QMA}(k)$-complete, and that is an interesting direction of study, along with the search for other $\mathsf{QMA}(k)$-complete promise problems. The class $\mathsf{QMA}(2)$ is still not well understood. For instance, a "classical" problem in $\mathsf{QMA}(2)$ but not obviously in QMA like the group-theoretic problem in Watrous (2000) is not known. Watrous' conjecture that for any approximate disentangler the dimension of the input Hilbert space is at least exponential in the dimension of the output Hilbert space is a central open question about $\mathsf{QMA}(2)$. Another interesting class is QCMA, where advice is in the form of *classical* strings, but Merlin and Arthur use quantum computers. Aaronson & Kuperberg (2007) gives a quantum oracle separation between QCMA and QMA, but a classical oracle separation between them is still an open question.

6 Conclusion

In this report, we have explored the complexity class $\mathsf{QMA}(k)$ (QMA with multiple Merlins) and its relevant results. We first discussed results leading to the fact that $\mathsf{QMA}(k) = \mathsf{QMA}(2)$, which means that k Merlins can be simulated using 2 Merlins. We then gave a proof sketch for the theorem by Harrow & Montanaro (2013) which establishes this result, along with the necessary amplification of completeness and soundness probabilities which make it possible. Next, we discussed evidence which indicates that $\mathsf{QMA}(2)$ might not be the same as QMA, though there is no concrete theoretical result which proves the same. We discussed the pure state N-representability problem, which is known to be in $\mathsf{QMA}(k)$ but its membership in QMA is unknown. Then, we talked about Aaronson et al. (2008)'s result that satisfiable 3SAT instances have sublinear proofs if multiple quantum witnesses are permitted, which demonstrates an almost quadratic improvement over the best known (linear) result for the one witness setting. Finally, we ruled out a potential approach for showing that $\mathsf{QMA}(2) = \mathsf{QMA}$ by proving the non-existence of perfect "disentanglers": quantum operations which can convert possibly entangled states into a tensor product of states.

It has been observed time and again that nature has a lot of untapped potential as we can see how quantum computation is able to do what does not seem possible for classical computation. Being a relatively nascent area of research, quantum complexity and its developments have a lot to tell us about what is and what is not possible to achieve using the power of quantum computation.

References

Aaronson, S., Beigi, S., Drucker, A., Fefferman, B., & Shor, P. (2008). *The Power of Unentanglement.* arXiv. Retrieved from https://arxiv.org/abs/0804.0802 doi: 10.48550/ARXIV.0804.0802

Aaronson, S., & Kuperberg, G. (2007). Quantum versus Classical Proofs and Advice. In *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)* (p. 115-128). doi: 10.1109/CCC.2007.27

Bennett, C. H., DiVincenzo, D. P., Smolin, J. A., & Wootters, W. K. (1996, nov). Mixed-state entanglement and quantum error correction. *Physical Review A*, *54*(5), 3824–3851. Retrieved from https://doi.org/10.1103%2Fphysreva.54.3824 doi: 10.1103/physreva.54.3824

Dinur, I. (2007, jun). The PCP Theorem by Gap Amplification. *J. ACM*, *54*(3), 12–es. Retrieved from https://doi.org/10.1145/1236457.1236459 doi: 10.1145/1236457.1236459

Harrow, A. W., & Montanaro, A. (2013, feb). Testing Product States, Quantum Merlin-Arthur Games and Tensor Optimization. *J. ACM*, *60*(1). Retrieved from https://doi.org/10.1145/2432622.2432625 doi: 10.1145/2432622.2432625

Hastings, M. B. (2009, mar). Superadditivity of communication capacity using entangled inputs. *Nature Physics*, *5*(4), 255–257. Retrieved from https://doi.org/10.1038%2Fnphys1224 doi: 10.1038/nphys1224

Kempe, J., Kitaev, A., & Regev, O. (2005). The Complexity of the Local Hamiltonian Problem. In K. Lodaya & M. Mahajan (Eds.), *FSTTCS 2004: Foundations of Software Technology and Theoretical Computer Science* (pp. 372–383). Berlin, Heidelberg: Springer Berlin Heidelberg.

Khanna, S., Sudan, M., Trevisan, L., & Williamson, D. P. (2000). The Approximability of Constraint Satisfaction Problems. *SIAM Journal on Computing*, *30*(6), 1863–1920.

King, C., & Ruskai, M. B. (2001). Minimal entropy of states emerging from noisy quantum channels. *IEEE Trans. Inf. Theory*, *47*, 192-209. Retrieved from https://arxiv.org/abs/quant-ph/9911079

Kobayashi, H., Matsumoto, K., & Yamakami, T. (2003). Quantum Merlin-Arthur Proof Systems: Are Multiple Merlins More Helpful to Arthur? In T. Ibaraki, N. Katoh, & H. Ono (Eds.), *Algorithms and Computation* (pp. 189–198). Berlin, Heidelberg: Springer Berlin Heidelberg.

König, R., & Renner, R. (2005, dec). A de Finetti representation for finite symmetric quantum states. *Journal of Mathematical Physics*, *46*(12), 122108. Retrieved from https://doi.org/10.1063%2F1.2146188 doi: 10.1063/1.2146188

Liu, Y.-K., Christandl, M., & Verstraete, F. (2007, Mar). Quantum Computational Complexity of the N-Representability Problem: QMA Complete. *Phys. Rev. Lett.*, *98*, 110503. Retrieved from https://link.aps.org/doi/10.1103/PhysRevLett.98.110503 doi: 10.1103/PhysRevLett.98.110503

Papadimitriou, C. H., & Yannakakis, M. (1991). Optimization, Approximation, and Complexity Classes. *J. Comput. Syst. Sci.*, *43*, 425-440.

Shamir, A. (1992, oct). IP = PSPACE. *J. ACM*, *39*(4), 869–877. Retrieved from https://doi.org/10.1145/146585.146609 doi: 10.1145/146585.146609

Shor, P. W. (2004, apr). Equivalence of Additivity Questions in Quantum Information Theory. *Communications in Mathematical Physics*, *246*(3), 473–473. Retrieved from https://doi.org/10.1007%2Fs00220-004-1071-1 doi: 10.1007/s00220-004-1071-1

Watrous, J. (2000). *Succinct quantum proofs for properties of finite groups.* arXiv. Retrieved from https://arxiv.org/abs/cs/0009002 doi: 10.48550/ARXIV.CS/0009002