CHICAGO JOURNAL OF THEORETICAL COMPUTER SCIENCE 2016, Article 04, pages 1–17
http://cjtcs.cs.uchicago.edu/

QMA with subset state witnesses

Alex B. Grilo Iordanis Kerenidis Jamie Sikora

Received November 5, 2015; Revised March 10, 2016; Published March 19, 2016

Abstract: The class QMA plays a fundamental role in quantum complexity theory and it has found surprising connections to condensed matter physics and in particular in the study of the minimum energy of quantum systems. In this paper, we further investigate the class QMA and its related class QCMA by asking what makes quantum witnesses potentially more powerful than classical ones. We provide a definition of a new class, SQMA, where we restrict the possible quantum witnesses to the "simpler" subset states, i.e. a uniform superposition over the elements of a subset of n-bit strings. Surprisingly, we prove that this class is equal to QMA, hence providing a new characterisation of the class QMA. We also prove the analogous result for QMA(2) and describe a new complete problem for QMA and a stronger lower bound for the class QMA$_1$.

1 Introduction

One of the notions at the heart of classical complexity theory is the class NP and the fact that deciding whether a boolean formula is satisfiable or not is NP-complete [6, 17]. The importance of NP-completeness became apparent through the plethora of combinatorial problems that can be cast as constraint satisfaction problems and shown to be NP-complete. Moreover, the famous PCP theorem [3, 4] provided a new, surprising description of the class NP: any language in NP can be verified efficiently by accessing probabilistically a constant number of bits of a polynomial-size witness. This opened the way to showing that in many cases, approximating the solution of NP-hard problems remains as hard as solving them exactly. An equivalent definition of the PCP theorem states that it remains NP-hard to decide whether an instance of a constraint satisfaction problem is satisfiable or any assignment violates at least a constant fraction of the constraints.

Not surprisingly, the quantum analog of the class NP, defined by Kitaev [15] and called QMA, has been the subject of extensive study in the last decade. Many important properties of this class are

Key words and phrases: computational complexity, quantum computation

DOI: 10.4086/cjtcs.2016.004

known, including a strong amplification property and an upper bound of PP [18], as well as numerous complete problems related to the ground state energy of different types of Hamiltonians [15, 14, 19, 7, 9]. Nevertheless, there are still many open questions about the class QMA, including whether it admits perfect completeness or not.

Moreover, it is still wide-open if a quantum PCP theorem exists. One way to phrase the quantum PCP theorem is that any problem in QMA can be verified efficiently by a quantum verifier accessing a constant number of qubits of a polynomial-size quantum witness. Another way would be that the problem of approximating the ground state energy of a local Hamiltonian within a constant is still QMA-hard. There have been a series of results, mostly negative, towards the goal of proving or disproving the quantum PCP theorem, but there is still no conclusive evidence [2].

Another important open question about the class QMA is whether the witness really need be a quantum state or it is enough for the polynomial-time quantum verifier to receive a classical witness. In other words, whether the class QMA is equal to the class QCMA, which is the class of problems that are decidable by a polynomial-time quantum verifier who receives a polynomial-size classical witness. Needless to say, resolving this question can also have implications to the quantum PCP theorem, since in case the two classes are the same, the quantum witness can be replaced by a classical one, which may be more easily checked locally. In addition, we know that perfect completeness is achievable for the class QCMA [12].

In this paper, we investigate the class QMA by asking the following simple, yet fundamental question: what makes a quantum witness potentially more powerful than a classical one? Is it the fact that to describe a quantum state one needs to specify an exponential number of possibly different amplitudes? Is it the different relative phases in the quantum state? Or is it something else altogether?

QMA with subset state witnesses. We provide a definition of a new class, where we restrict the quantum witnesses to be as "classical" as possible, without having by definition an efficient classical description (otherwise our class would be trivially equal to QCMA). All definitions and statements of the results are made formal in their respective sections.

For any subset $S \subseteq [d]$, we define the subset state $|S\rangle \in \mathbb{C}^d$, as the uniform superposition over the elements of S. More precisely, $|S\rangle := \frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle$.

The class SQMA. A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in SQMA (**S**ubset state **QMA**) if for every $x \in A_{\text{yes}} \cup A_{\text{no}}$, there exists a polynomial time quantum verifier V_x, such that

- *(completeness)* for all $x \in A_{\text{yes}}$, there exists a subset state witness $|S\rangle$, such that the verifier accepts with probability at least $2/3$.
- *(soundness)* for all $x \in A_{\text{no}}$ and all quantum witnesses $|\psi\rangle$, the verifier accepts with probability at most $1/3$.

The only difference from QMA is that in the yes-instances, we ask that there exists a *subset state witness* that makes the quantum verifier accept with high probability. In other words, an honest prover need only provide such subset states, which in principle are conceptually simpler.

Notice, nevertheless, that the Group Non-Membership Problem is in SQMA, since the witness in the known QMA protocol is a subset state [20]. Moreover, we can define a version of our class with two

non-entangled provers, similarly to QMA(2), and we can again see that the protocol of Blier and Tapp [5] which shows that any language in NP has a QMA(2) proof system with logarithmic size quantum messages uses such subset states. Hence, even though the witnesses we consider are quite restricted, some of the most interesting containments still hold for our class.

Even more surprisingly, our main result shows that SQMA is, in fact, equal to QMA and the same for the two-prover case.

Result 1. $\mathrm{SQMA} = \mathrm{QMA}$ and $\mathrm{SQMA}(2) = \mathrm{QMA}(2)$.

Hence, for any problem in QMA, the quantum witness can be a subset state. This provides a new way of looking at QMA and shows that if quantum witnesses are more powerful than classical ones, then this relies solely on the fact that a quantum witness can, in some sense, convey information about an arbitrary subset of classical strings through a uniform superposition of its elements. On the other hand, one way to prove that classical witnesses are as powerful as quantum witnesses, is to find a way to replace such subset states with a classical witness, possibly by enforcing more structure on the accepting subset states.

Our proof relies on a geometric lemma, which shows, for instance, that for any unit vector in $\mathbb{C}^{2^n}$, there exists a subset state, such that their inner product is $\Omega(1/\sqrt{n})$. This lemma, in conjunction with standard amplification techniques for QMA imply our main result.

Complete problems. The canonical QMA-complete problem is the following: Given a Hamiltonian acting on an n-qubit system, which is a sum of "local" Hamiltonians each acting on a constant number of qubits, decide whether the ground state energy is at most a or all states have energy at least b, where $b-a \geq 1/poly(n)$. The first question is whether we can show that the same problem is complete if we look at the energy of any subset state instead of the ground state. In fact, we do not know how to show that this problem is complete: when we try to follow Kitaev's proof of completeness and approximate his *history state* with a subset state, we cannot retain a sufficient energy gap. Moreover, there exist Hamiltonians with a low energy ground state, but the energy of all subset states is close to 1.

In this work, we provide one new complete problem for QMA related to subset states. This problem is based on the QCMA-complete problem Identity Check on Basis States [23].

Result 2. The following Basis State Check on Subset States problem is QMA-complete:

- Input: Let x be a classical description of a quantum circuit Z_x on m qubits and y be an m'-bit string, where $n := |x|$ and $m' \leq m$. Given the promise that x satisfies one of the following cases for some polynomial[1] q, decide which is true:
- Yes: there is a subset S such that $\| (\langle y| \otimes I) Z_x |S\rangle \|_2^2 \geq 1 - 1/q(n)$,
- No: for all subsets S, we have $\| (\langle y| \otimes I) Z_x |S\rangle \|_2^2 \leq 1/q(n)$.

Perfect completeness. Another important open question about QMA is whether it admits perfect

[1] This polynomial needs to have degree at least that of m (see Theorem 5.2 for a formal statement).

completeness. Using our characterisation, this question can be reduced to the question of whether SQMA is equal to SQMA_1. On one hand, the result of [1] can be used to show that there exists a quantum oracle A relative to which these two classes are not equal, i.e., $\mathrm{SQMA}^A \neq \mathrm{SQMA}_1^A$. On the other hand, proving perfect completeness for SQMA may be an easier problem to solve, since unlike QMA, the amplitudes involved in the subset states are much easier to handle. Even though we are unable to prove perfect completeness for SQMA, we prove perfect completeness for the following closely related class.

The class oSQMA. A promise problem $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ is in oSQMA (**o**ptimal **S**ubset state **QMA**) if for every $x \in A_{\mathrm{yes}} \cup A_{\mathrm{no}}$, there exists a polynomial time quantum verifier V_x, such that

- *(completeness)* for all $x \in A_{\mathrm{yes}}$, there exists a subset state witness $|S\rangle$ that maximizes the probability the verifier accepts and this probability is at least $2/3$.
- *(soundness)* for all $x \in A_{\mathrm{no}}$ and all quantum witnesses $|\psi\rangle$, the verifier accepts with probability at most $1/3$.

This class still contains the Group Non-Membership problem, while its two-prover version has short proofs for NP. It remains open to understand whether demanding that a subset state is the optimal witness, instead of just an accepting one, reduces the computational power of the class. Moreover, these two classes coincide in the case of perfect completeness, since all accepting witnesses are also optimal. We prove that the class oSQMA admits perfect completeness, which implies a stronger lower bound for the class QMA_1 than the previously known QCMA bound.

Result 3. $\mathrm{SQMA}_1 = \mathrm{oSQMA}_1 = \mathrm{oSQMA}$ and hence, $\mathrm{oSQMA} \subseteq \mathrm{QMA}_1 \subseteq \mathrm{QMA}$.

The fact that for the class oSQMA there exists a subset state which is an optimal witness implies that the maximum acceptance probability is rational and moreover, it is the maximum eigenvalue of the verifier's operator. These two facts enable us to extend the rewind technique used by Kobayashi, Le Gall and Nishimura [16] and prove our result.

2 Preliminaries

2.1 Definitions

Let $\Sigma = \{0,1\}$. For $n \in \mathbb{N}$, we define $[n] := \{1,...,n\}$. The Hilbert-Schmidt or trace inner product between two operators A and B is defined as $\langle A, B\rangle = \mathrm{Tr}(A^\dagger B)$. For a complex number $x = a + ib$, $a, b \in \mathbb{R}$, we define its norm $|x|$ by $\sqrt{a^2+b^2}$. For a vector $|v\rangle \in \mathbb{C}^d$, its p-norm is defined as $\| |v\rangle \|_{\mathrm{p}} := \left(\sum_{1\leq i\leq d} |v_i|^p\right)^{\frac{1}{p}}$. For an operator A, the trace norm is $\|A\|_{\mathrm{tr}} := \mathrm{Tr}\sqrt{A^\dagger A}$, which is the sum of the singular values of A.

We now state two identities which we use in our analysis. For normalized $|v\rangle, |w\rangle \in \mathbb{C}^d$, we have

$$\max_{0\preceq C\preceq I} |\langle C, |v\rangle\langle v| - |w\rangle\langle w|\rangle| = \frac{1}{2} \| |v\rangle\langle v| - |w\rangle\langle w| \|_{\mathrm{tr}}, \tag{2.1}$$

since $|v\rangle\langle v| - |w\rangle\langle w|$ has largest eigenvalue $\lambda \geq 0$, smallest eigenvalue $-\lambda$, and the rest are 0, and the trace norm of a Hermitian matrix is the sum of the absolute values of its eigenvalues. We also have that for $|v\rangle, |w\rangle \in \mathbb{C}^d$,

$$\| |v\rangle\langle v| - |w\rangle\langle w| \|_{\mathrm{tr}} = 2\sqrt{1 - |\langle v|w\rangle|^2}. \tag{2.2}$$

2.2 Complexity classes and complete problems

We start by defining the known quantum complexity classes we will study and a complete problem.

Definition 2.1 (QMA)**.** A promise problem $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ is in QMA if and only if there exist polynomials p, q and a polynomial-time uniform family of quantum circuits $\{Q_n\}$, where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$, a $p(n)$-qubit quantum state, and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:

- (completeness) If $x \in A_{\mathrm{yes}}$, then there exists a $p(n)$-qubit quantum state $|\psi\rangle$ such that Q_n accepts $(x, |\psi\rangle)$ with probability at least $2/3$.
- (soundness) If $x \in A_{\mathrm{no}}$, then for any $p(n)$-qubit quantum state $|\psi\rangle$, Q_n accepts $(x, |\psi\rangle)$ with probability at most $1/3$.

We can restrict QMA in order to always accept yes-instances, a property called *perfect completness*.

Definition 2.2 (QMA_1)**.** A promise problem $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ is in QMA_1 if and only if there exist polynomials p, q and a polynomial-time uniform family of quantum circuits $\{Q_n\}$, where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$, a $p(n)$-qubit quantum state, and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:

- (completeness) If $x \in A_{\mathrm{yes}}$, then there exists a $p(n)$-qubit quantum state $|\psi\rangle$ such that Q_n accepts $(x, |\psi\rangle)$ with probability exactly 1.
- (soundness) If $x \in A_{\mathrm{no}}$, then for any $p(n)$-qubit quantum state $|\psi\rangle$, Q_n accepts $(x, |\psi\rangle)$ with probability at most $1/3$.

Another way we can restrict QMA is only allowing classical witnesses, resulting in the definition of the class QCMA (sometimes also referred to as MQA [21, 8]).

Definition 2.3 (QCMA)**.** A promise problem $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ is in QCMA if and only if there exist polynomials p, q and a polynomial-time uniform family of quantum circuits $\{Q_n\}$, where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$, a $p(n)$-bit string, and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:

- (completeness) If $x \in A_{\mathrm{yes}}$, then there exists a $p(n)$-bit string y such that Q_n accepts (x, y) with probability at least $2/3$.
- (soundness) If $x \in A_{\mathrm{no}}$, then for any $p(n)$-bit string y, Q_n accepts (x, y) with probability at most $1/3$.

We state here one QCMA-complete problem, the *Identity Check on Basis States* problem [23].

Definition 2.4 (Identity Check on Basis States [23])**.** Let x be a classical description of a quantum circuit Z_x on m qubits. Given the promise that Z_x satisfies one of the following cases for $\mu - \delta \geq 1/\text{poly}(|x|)$, decide which one is true:

- either there is a binary string z such that $|\langle z| Z_x |z\rangle|^2 \leq 1-\mu$, i.e., Z_x does not act as the identity on the basis states,
- or for all binary strings z, $|\langle z| Z_x |z\rangle|^2 \geq 1-\delta$, i.e., Z_x acts "almost" as the identity on the basis states.

We also consider the two (unentangled) provers version of QMA, defined below.

Definition 2.5 (QMA(2))**.** A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in QMA(2) if and only if there exist polynomials p, q and a polynomial-time uniform family of quantum circuits $\{Q_n\}$, where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$, two unentangled $p(n)$-qubit quantum states, and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:

- (completeness) If $x \in A_{\text{yes}}$, then there exists two unentangled $p(n)$-qubit quantum states $|\psi\rangle$ and $|\phi\rangle$ such that Q_n accepts $(x, |\psi\rangle, |\phi\rangle)$ with probability at least $2/3$.
- (soundness) If $x \in A_{\text{no}}$, then for any two unentangled $p(n)$-qubit quantum states $|\psi\rangle$ and $|\phi\rangle$, Q_n accepts $(x, |\psi\rangle, |\phi\rangle)$ with probability at most $1/3$.

3 Subset state approximations

In this section we state and prove the Subset State Approximation Lemma which intuitively says that any quantum state can be well-approximated by a subset state, defined below.

Definition 3.1. For a subset $S \subseteq [d]$, a *subset state*, denoted here as $|S\rangle \in \mathbb{C}^d$, is a uniform superposition over the the elements of S. More specifically, it has the form

$$|S\rangle := \frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle .$$

We now state and prove a useful technical lemma.

Lemma 3.2 (Geometric Lemma)**.** *For a vector $v \in \mathbb{C}^d$, there exists a subset $S \subseteq [d]$ such that*

$$\frac{1}{\sqrt{|S|}} \left| \sum_{j \in S} v_j \right| \geq \frac{\|v\|_2}{8\sqrt{\log_2(d)+3}}.$$

Proof. If $v = 0$, the lemma statement is trivially true. Suppose $v \in \mathbb{C}^d$ is a nonzero vector and decompose v into real and imaginary parts as $v = u + iw$, where $u, w \in \mathbb{R}^d$. Note that

$$\|v\|_2 \leq \|u\|_2 + \|w\|_2 ,$$

by the triangle inequality, implying at least one has norm at least $\|v\|_2/2$. Let us say it is u (the argument for w proceeds analogously). We now partition u into positive and negative entries such that $u = x - y$ where $x, y \geq 0$ and are orthogonal. By the same argument as above, we know at least one has norm at least $\|v\|_2/4$. Without loss of generality, suppose it is x.

Let T denote the support of x, i.e., $j \in T$ if and only if $x_j > 0$. The idea is to partition T into a small number of sets, where the entries x_j that belong to each set are roughly the same size, and the sum of the entries corresponding to one set is a large enough fraction of the norm of the entire vector.

More precisely, let us partition T into the following sets:

$$T_k := \left\{ j \in T : \frac{\|x\|_2}{2^k} < x_j \leq \frac{\|x\|_2}{2^{k-1}} \right\}, \text{ for } k \in [\gamma], \quad T_{\gamma+1} := \left\{ j \in T : 0 < x_j \leq \frac{\|x\|_2}{2^\gamma} \right\}$$

for $\gamma := \left\lceil \frac{\log_2(d)+1}{2} \right\rceil$. We have

$$\sum_{j \in \cup_{k\in[\gamma]} T_k} (x_j)^2 = \|x\|_2^2 - \sum_{j \in T_{\gamma+1}} (x_j)^2 \geq \|x\|_2^2 - d\frac{\|x\|_2^2}{2^{2\gamma}} = \|x\|_2^2 \left(1 - \frac{d}{2^{2\gamma}}\right).$$

This implies that there exists $k' \in [\gamma]$ such that

$$\sum_{j \in T_{k'}} (x_j)^2 \geq \frac{\|x\|_2^2}{\gamma} \left(1 - \frac{d}{2^{2\gamma}}\right).$$

Using the definition of T_k, we have

$$|T_{k'}| \frac{\|x\|_2^2}{2^{2(k'-1)}} \geq \sum_{j \in T_{k'}} (x_j)^2 \geq \frac{\|x\|_2^2}{\gamma} \left(1 - \frac{d}{2^{2\gamma}}\right),$$

which implies the following lower bound for the size of $T_{k'}$

$$|T_{k'}| \geq \frac{2^{2(k'-1)}}{\gamma} \left(1 - \frac{d}{2^{2\gamma}}\right). \tag{3.1}$$

Using again the definition of T_k and Equation (3.1), we have

$$\frac{1}{\sqrt{|T_{k'}|}} \sum_{j \in T_{k'}} x_j \geq \frac{\sqrt{|T_{k'}|}\,\|x\|_2}{2^{k'}} \geq \frac{\|x\|_2 2^{(k'-1)}}{2^{k'}\sqrt{\gamma}} \sqrt{1 - \frac{d}{2^{2\gamma}}} \geq \frac{\|v\|_2}{8\sqrt{\log_2(d)+3}}.$$

Let $S := T_{k'}$ and s be the vector where $s_j = \frac{1}{\sqrt{|S|}}$ if $j \in S$ and 0 otherwise. We have

$$\frac{1}{\sqrt{|S|}} \left| \sum_{j \in S} v_j \right| = |\langle s, v \rangle| = |\langle s, u \rangle + i\langle s, w \rangle| \geq |\langle s, u \rangle| = \left| \frac{1}{\sqrt{|S|}} \sum_{j \in S} x_j \right| \geq \frac{\|v\|_2}{8\sqrt{\log_2(d)+3}}$$

as desired. □

The technique used above of splitting the amplitudes into sets is similar to a proof in [11] which showed a result for approximating bipartite states by a uniform superposition of their Schmidt basis vectors. Note that our result holds for any state and, since we are concerned with a particular fixed basis, we need to deal with arbitrary complex amplitudes.

Lemma 3.3 (Subset State Approximation Lemma)**.** *For any n-qubit state $|\psi\rangle$, there is a subset $S \subseteq [N]$, where $N := 2^n$, such that $|\langle S|\psi\rangle| \geq \frac{1}{8\sqrt{n+3}}$.*

Remark 3.4. We can further assume the size of the subset is a power of 2 and lose at most a constant factor in the approximation (equal to $\frac{1}{2}$).

We also show that this approximation factor is optimal by presenting an n-qubit state $|\psi_n\rangle$, for any n, where the above bound is tight (up to constant factors). In high level, the state has 2^ℓ basis states with amplitude $\frac{1}{\sqrt{n}\sqrt{2^\ell}}$, for $0 \leq \ell \leq n$, and hence, each of these n subsets of basis states has only a $1/n$ fraction of the total "weight" and the amplitudes between different subsets are sufficiently different.

Lemma 3.5. *For any n, define the following n-qubit state*

$$|\psi_n\rangle := \sum_{1 \leq i \leq 2^n - 1} \frac{1}{\sqrt{n}\sqrt{2^{\lfloor \log i \rfloor}}} |i\rangle .$$

Then we have that $\langle \psi_n|S\rangle \leq \frac{2+\sqrt{2}}{\sqrt{n}}$, for all $S \subseteq [2^n]$.

Proof. We see that the amplitudes are non-increasing and thus a subset state that would approximate it the best would be of the form $S = [m]$ for some $m \leq 2^n - 1$. Thus, we prove now that for all m, $S = [m]$ gives an approximation of at most $\frac{\sqrt{2}+2}{\sqrt{n}}$.

Let $k \in \{0, 1, \ldots, n-1\}$ be such that $2^k \leq m \leq 2^{k+1} - 1$. We see that

$$\sum_{i=1}^{m} \frac{1}{\sqrt{n}\sqrt{2^{\lfloor \log i \rfloor}}} \leq \sum_{i=1}^{2^{k+1}-1} \frac{1}{\sqrt{n}\sqrt{2^{\lfloor \log i \rfloor}}} = \sum_{t=0}^{k} \frac{2^t}{\sqrt{n}\sqrt{2^t}} = \sum_{t=0}^{k} \frac{\sqrt{2^t}}{\sqrt{n}} = \frac{\left(1+\sqrt{2}\right)\left(\sqrt{2^{k+1}}-1\right)}{\sqrt{n}},$$

where the last equality follows from the formula for a truncated geometric series. We have

$$\frac{1}{\sqrt{m}} \sum_{i-1}^{m} \frac{1}{\sqrt{n}\sqrt{2^{\lfloor \log i \rfloor}}} \leq \frac{\left(1+\sqrt{2}\right)\left(\sqrt{2^{k+1}}-1\right)}{\sqrt{n}\sqrt{2^k}} \leq \frac{\left(1+\sqrt{2}\right)\sqrt{2^{k+1}}}{\sqrt{n}\sqrt{2^k}} = \frac{2+\sqrt{2}}{\sqrt{n}},$$

as desired. □

4 Alternative characterisations of QMA and QMA(2)

In this section, we prove that QMA and its two-prover variant can be characterized such that they accept subset states. We start by defining formally the new complexity class that is by definition contained in QMA.

Definition 4.1 (SQMA)**.** A promise problem $A = (A_{\text{yes}}, A_{\text{no}})$ is in SQMA if and only if there exist polynomials p, q and a polynomial-time uniform family of quantum circuits $\{Q_n\}$, where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$, a $p(n)$-qubit quantum state, and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:

- (completeness) If $x \in A_{\text{yes}}$, then there exists a subset $S \subseteq [2^{q(n)}]$ such that Q_n accepts $(x, |S\rangle)$ with probability at least $2/3$.
- (soundness) If $x \in A_{\text{no}}$, then for any $p(n)$-qubit quantum state $|\psi\rangle$, Q_n accepts $(x, |\psi\rangle)$ with probability at most $1/3$.

Remark. Note that we restricted the witness only in the completeness criterion. In fact, it is straightforward to adapt any QMA protocol to have a subset state being an optimal witness in the soundness criterion. For example, the prover can send an extra qubit with the original witness and the verifier can measure it in the computational basis. If the outcome is 0, he continues verifying the proof. If it is 1, he flips a coin and accepts with probability, say, $1/3$. It is easy to see that an optimal witness for the soundness probability is the string of all 1's, which is classical, hence a subset state! Therefore, restricting the proofs in the completeness criterion is the more natural and interesting case.

We prove now that, surprisingly, this restriction does not change the computational power of QMA.

Theorem 4.2. QMA = SQMA.

Proof. We have trivially that SQMA $\subseteq$ QMA by definition, thus we only need to show that QMA $\subseteq$ SQMA.

Suppose we have a QMA protocol which verifies a $p(n)$-qubit proof $|\psi\rangle$ with the two-outcome POVM measurement $\{C, I - C\}$. More precisely, without loss of generality, we assume that there exists a polynomial r such that if $x \in A_{\text{yes}}$, there exists a state $|\psi\rangle$ such that $\langle\psi|C|\psi\rangle \geq 1 - 2^{-r(n)}$ and if $x \in A_{\text{no}}$, we have for every $|\psi\rangle$, that $\langle\psi|C|\psi\rangle \leq 2^{-r(n)}$. We show that the same verification above accepts a subset state with probability at least $\Omega(1/p(n))$, from which we conclude that the same instance can be decided with a SQMA protocol using standard error reduction techniques.

If $x \in A_{\text{no}}$ there is nothing to show (since the soundness condition for QMA and SQMA coincide). Suppose $x \in A_{\text{yes}}$ and let $|\psi\rangle$ be a proof which maximizes the acceptance probability. We then use the Subset State Approximation Lemma (Lemma 3.3) to approximate $|\psi\rangle$ with $|S\rangle$, where $S \subseteq [2^{p(n)}]$, satisfies:

$$|\langle\psi|S\rangle| \geq \frac{1}{8\sqrt{p(n)+3}} \tag{4.1}$$

We now show that the acceptance probability of $|S\rangle$ is not too small. Note that

$$\langle S|C|S\rangle = \langle C, |S\rangle\langle S|\rangle = \langle C, |\psi\rangle\langle\psi|\rangle - \langle C, |\psi\rangle\langle\psi| - |S\rangle\langle S|\rangle \tag{4.2}$$

and since $\langle C, |\psi\rangle\langle\psi|\rangle \geq 1 - 2^{-r(n)}$, we concentrate now on bounding $\langle C, |\psi\rangle\langle\psi| - |S\rangle\langle S|\rangle$. Clearly, we have

$$\langle C, |\psi\rangle\langle\psi| - |S\rangle\langle S|\rangle \leq \max_{0\preceq C\preceq I} |\langle C, |\psi\rangle\langle\psi| - |S\rangle\langle S|\rangle| = \frac{1}{2}\,\| |\psi\rangle\langle\psi| - |S\rangle\langle S| \|_{\text{tr}}\,, \tag{4.3}$$

where the last equality comes from Equation (2.1).

We now have

$$\| |\psi\rangle\langle\psi| - |S\rangle\langle S| \|_{\mathrm{tr}} = 2\sqrt{1-|\langle\psi|S\rangle|^2} \leq 2-|\langle\psi|S\rangle|^2, \tag{4.4}$$

where the equality follows from Equation (2.2) and the inequality from the fact that, for $x \geq 0$, we have $\sqrt{1-x^2} \leq 1-x^2/2$. Combining Equations (4.1), (4.2), (4.3), and (4.4), we have

$$\langle S|C|S\rangle \geq 1-2^{-r(n)} - \frac{1}{2}\left(2-|\langle\psi|S\rangle|^2\right) = \frac{1}{2}|\langle\psi|S\rangle|^2 - 2^{-r(n)} \geq \frac{1}{128(p(n)+3)} - 2^{-r(n)}.$$

Thus, $|S\rangle$ is accepted with probability $\Omega\left(\frac{1}{p(n)}\right)$, as required. □

We now define formally the class SQMA(2).

Definition 4.3 (SQMA(2))**.** A promise problem $A = (A_{\mathrm{yes}}, A_{\mathrm{no}})$ is in SQMA(2) if and only if there exist polynomials p, q and a polynomial-time uniform family of quantum circuits $\{Q_n\}$, where Q_n takes as input a string $x \in \Sigma^*$ with $|x| = n$, two unentangled $p(n)$-qubit quantum states, and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:

- (completeness) If $x \in A_{\mathrm{yes}}$, then there exists two subsets $S, T \subseteq [2^{p(n)}]$ such that Q_n accepts $(x, |S\rangle, |T\rangle)$ with probability at least $2/3$.
- (soundness) If $x \in A_{\mathrm{no}}$, then for any two unentangled $p(n)$-qubit quantum states $|\psi\rangle$ and $|\phi\rangle$, Q_n accepts $(x, |\psi\rangle, |\phi\rangle)$ with probability at most $1/3$.

Theorem 4.4. QMA(2) = SQMA(2).

Proof. We can use error reduction techniques [10] to assume the completeness and soundness of the QMA(2) protocol are $1-2^{-r(n)}$ and $2^{-r(n)}$, respectively, for some polynomial r. If we approximate both witnesses using subset states and use the same analysis from the one-prover case, we have an inverse polynomial gap between completeness (using the two subset state witnesses) and the soundness. One can again use the error reduction techniques from [10] since the witnesses (in the reduced error protocol) can be a tensor product of these subset states. □

5 A QMA-complete problem based on subset states

In this section, we give a complete problem for QMA based on circuits mapping subset states to a basis state. This is similar to the QCMA-complete problem Identity Check on Basis States (see Definition 2.4).

Definition 5.1 (Basis State Check on Subset States (BSCSS(α)))**.** Let x be a classical description of a quantum circuit Z_x on $m(n)$ input qubits and $a(n)$ ancilla qubits, and y be an $m'(n)$-bit string, such that $n := |x|$, m, a, and m' are bounded by polynomials and $m' \leq m+a$. Given the promise that x satisfies one of the following cases, decide which is true:

- either there exists a subset $S \subseteq [2^{m(n)}]$ such that

$$\left\| (\langle y| \otimes I) Z_x |S\rangle |0\rangle^{\otimes a(n)} \right\|_2^2 \geq 1 - \alpha,$$

- or for all subsets $S \subseteq [2^{m(n)}]$, we have

$$\left\| (\langle y| \otimes I) Z_x |S\rangle |0\rangle^{\otimes a(n)} \right\|_2^2 \leq \alpha.$$

Theorem 5.2. *For any polynomial r, the problem* BSCSS *is* QMA*-complete for* $2^{-r(n)} \leq \alpha \leq \frac{1}{257(m(n)+3)}$.

Before we prove this result, we first motivate why we study this problem. At first glance, it looks very similar to a trivial complete problem for QMA. However, BSCSS only considers subset states in both the yes and no-instances, as opposed to arbitrary states for the version for QMA. Moreover, one may ask what happens to the computational power of SQMA if one were to restrict to only rejecting subset states in the soundness criterion in the definition. The bounds on α in the theorem above give bounds on the completeness-soundness gap required for this modified definition of SQMA to still be equivalent to QMA.

To prove the theorem, we show SQMA-hardness and containment in SQMA separately. The result then follows since SQMA = QMA.

Lemma 5.3. *The problem* BSCSS *is in* SQMA *for* $\alpha \leq \frac{1}{257(m(n)+3)}$.

Proof. The SQMA verification is as follows. First, the verifier receives a state $|\psi\rangle$, applies Z_x to $|\psi\rangle |0\rangle^{\otimes a(n)}$, then measures the whole state in the computational basis to see if the outcome agrees with y on the m' bits.

Suppose we have a yes-instance of BSCSS. Then we know there exists a subset state which accepts with probability $1-\alpha$. Now suppose we have a no-instance of BSCSS. We know that for all subset states $|S\rangle$, $\left\| (\langle y| \otimes I) Z_x |S\rangle |0\rangle^{\otimes a(n)} \right\|_2^2 \leq \alpha$. We now show that there is no state $|\psi\rangle$ such that $\left\| (\langle y| \otimes I) Z_x |\psi\rangle |0\rangle^{\otimes a(n)} \right\|_2^2$ is "large". Fix an arbitrary state $|\psi\rangle$ and let $|S\rangle$ be a subset state with overlap at least $1/(8\sqrt{m(n)+3})$ from the Subset State Approximation Lemma (Lemma 3.3). We start with noticing that

$$\left\| (\langle y| \otimes I) Z_x |\psi\rangle |0\rangle^{\otimes a(n)} \right\|_2^2 = \langle \mathrm{Tr}_A \left((I \otimes |0\rangle \langle 0|_A) Z_x^\dagger (|y\rangle \langle y| \otimes I) Z_x (I \otimes |0\rangle \langle 0|_A) \right), |\psi\rangle \langle \psi| \rangle,$$

where A is the $a(n)$-qubit register the ancilla qubits act on. By a similar analysis as in the proof of Lemma 4.2, we have that

$$\begin{aligned} \langle \mathrm{Tr}_A \left((I \otimes |0\rangle \langle 0|_A) Z_x^\dagger (|y\rangle \langle y| \otimes I) Z_x (I \otimes |0\rangle \langle 0|_A) \right), |\psi\rangle \langle \psi| \rangle &\leq \alpha + \left(1 - \frac{1}{128(m(n)+3)} \right) \\ &= 1 + \alpha - \frac{1}{128(m(n)+3)}. \end{aligned}$$

Therefore, any proof succeeds with probability at most $1+\alpha-\frac{1}{128(m(n)+3)}$. The gap between the completeness and soundness is therefore at least

$$(1-\alpha)-\left(1+\alpha-\frac{1}{128(m(n)+3)}\right)=-2\alpha+\frac{1}{128(m(n)+3)}=\Omega(1/m(n)),$$

using the assumption that $\alpha \leq \frac{1}{257(m(n)+3)}$. We can use standard error reduction techniques to put this protocol into SQMA, as desired. □

Lemma 5.4. *For any polynomial r, the problem* BSCSS *is* QMA*-hard for* $2^{-r(n)} \leq \alpha \leq 1/3$.

Proof. Fix a polynomial r and take any SQMA verification circuit where we assume the following modifications have been made:

- The unitary acts on an $m(n)$-qubit proof and an $a(n)$-qubit ancilla register A.
- All measurements are deferred until the end of the verification. Denote the cumulative unitary the verifier applies as V.
- We assume the verifier has a special register, $\mathcal{O}$, at the end containing the outcome of the verification. He then measures it in the computational basis and accepts on outcome 1 and rejects on outcome 0.
- The completeness of the protocol is least $1-2^{-r(n)}$ and the soundness is at most $2^{-r(n)}$.

Then, we define the string y as the single bit $|1\rangle_{\mathcal{O}}$, i.e., $m'=1$ here. Then, for the SQMA protocol, we see the acceptance probability of a state $|\psi\rangle$ is precisely

$$\left\| (\langle y| \otimes I)V |\psi\rangle |0\rangle^{\otimes a(n)} \right\|_2^2.$$

We now let (V,y) be an instance of BSCSS with $2^{-r(n)} \leq \alpha \leq 1/3$. We see that the size of the descriptions of V and y, as well as m, a, and m', are at most polynomial in the size of the SQMA input. It is clear from the definition of SQMA, that yes-instances of SQMA are mapped to yes-instances of the instance of BSCSS and similarly no-instances are mapped to no-instances. Thus, solving this instance of BSCSS decides the SQMA protocol, as desired. □

6 On the perfectly complete version of SQMA

In this section, we study the version of SQMA with perfect completeness, namely SQMA_1. Even though we do not prove here that SQMA admits perfect completeness (i.e., $\mathrm{SQMA}=\mathrm{SQMA}_1$), we characterise SQMA_1 showing that it is equal to a variant of SQMA where there is an optimal subset state witness.

Definition 6.1 (oSQMA)**.** A promise problem $A=(A_{\mathrm{yes}},A_{\mathrm{no}})$ is in oSQMA if and only if there exist polynomials p, q and a polynomial-time uniform family of quantum circuits $\{Q_n\}$, where Q_n takes as input a string $x\in\Sigma^*$ with $|x|=n$, a $p(n)$-qubit quantum state, and $q(n)$ ancilla qubits in state $|0\rangle^{\otimes q(n)}$, such that:

- (completeness) If $x \in A_{\text{yes}}$, then there exists a subset $S \subseteq [2^{p(n)}]$ such that Q_n accepts $(x, |S\rangle)$ with probability at least $2/3$ and this subset state *maximizes* the acceptance probability over all states.
- (soundness) If $x \in A_{\text{no}}$, then for any $p(n)$-qubit quantum state $|\psi\rangle$, Q_n accepts $(x, |\psi\rangle)$ with probability at most $1/3$.

We remark that the perfectly complete versions of SQMA and oSQMA coincide since in both cases there is an optimal subset state witness for yes-instances which leads to acceptance probability 1. Analogous to the notation for QMA_1 and SQMA_1, we denote the perfectly complete version of oSQMA as oSQMA_1.

We now state a theorem characterizing SQMA_1 which provides a stronger lower bound for QMA_1.

Theorem 6.2. $\text{SQMA}_1 = \text{oSQMA}_1 = \text{oSQMA}$ *and hence,* $\text{oSQMA} \subseteq \text{QMA}_1 \subseteq \text{QMA}$.

This theorem is proven using a framework very similar to the works of Jordan, Kobayashi, Nagaj and Nishimura [12] and also Kobayashi, Le Gall and Nishimura [16].

The idea is to use the Rewinding Technique [22][13][16] in order to achieve perfect completeness. For using this technique we need a quantum circuit that has maximum acceptance probability $\frac{1}{2}$ for yes-instances. In order to construct such a circuit we first show that if the oSQMA verifier uses a specific set of gates, then the maximum acceptance probability for a yes-instance is rational and exactly describable using polynomially many bits.

Lemma 6.3. *If an* oSQMA *verifier uses only Hadamard, Toffoli and NOT gates, the maximum acceptance probability for yes-instances has the form* $\frac{p}{q}$*, for* $p, q \in \mathbb{N}$*, and* $\log p, \log q \leq l(|x|)$ *for some polynomial* l*.*

Proof. As noticed in [12], if we apply a quantum circuit that consists only of Hadamard, Toffoli, and NOT gates on the computational basis state $|i\rangle$, the final superposition will be of the form $\sum_j \frac{k_i^j}{2^{\frac{r}{2}}} |j\rangle$ for some $k_i^j \in \mathbb{Z}$ and $r \in \mathbb{N}$, such that r is polynomially bounded. Thus, for an optimal oSQMA witness $\frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle$ we have that the final state is $\frac{1}{\sqrt{|S|}} \sum_{i \in S} \sum_j \frac{k_i^j}{2^{\frac{r}{2}}} |j\rangle$. Therefore, the maximum acceptance probability is

$$\frac{\sum_{j \in A} \left(\sum_{i \in S} k_i^j \right)^2}{|S| 2^r},$$

where A is the subset of computational basis states such that the output qubit is $|1\rangle$ (the measurement outcome where the verifier accepts). It follows that the acceptance probability is rational and succinct. □

In this case, the prover can send a classical description of the maximum acceptance probability in the original protocol, together with the original (optimal) subset state proof. Let a_x be the maximum acceptance probability of the input x in the original protocol and $\frac{p}{q}$ be the value claimed by the prover to be the maximum acceptance probability. The verifier first checks if $\frac{p}{q} \geq \frac{2}{3}$, and rejects otherwise.

We can create a new Verifier circuit that flips $r+1$ quantum coins, for the smallest r such that $2^r \geq q$, and either

1. accepts with probability $\frac{2^r-p}{2^{r+1}}$,
2. rejects with probability $\frac{2^r-q+p}{2^{r+1}}$, or
3. runs the original protocol with probability $\frac{q}{2^{r+1}}$.

For a yes-instance, the prover is honest and sends the correct value $\frac{p}{q} = a_x$. The maximum success probability of the new Verifier circuit is exactly

$$\frac{2^r-p}{2^{r+1}} + \frac{q}{2^{r+1}} \cdot \frac{p}{q} = \frac{1}{2}.$$

For a no-instance the success probability is at most

$$\frac{2^r-p}{2^{r+1}} + \frac{q}{2^{r+1}} \cdot a_x \leq \frac{2^r-p}{2^{r+1}} + \frac{q}{2^{r+1}} \cdot \frac{1}{3} \leq \frac{2^r}{2^{r+1}} - \frac{q}{3 \cdot 2^{r+1}} \leq \frac{1}{2} - \frac{1}{12} = \frac{5}{12},$$

where we used the fact that the maximum acceptance probability a_x in the original protocol is at most $\frac{1}{3}$, $\frac{p}{q} \geq \frac{2}{3}$ (which can be verified with probability 1) and that $2q \geq 2^r$, by definition.

Then, as we said, we can apply the Rewinding Technique with this new Verifier, and achieve perfect completeness. For this, we change the initial projector to have all zeroes in the coin register and the corresponding acceptance projector as described above. For further and explicit details of why such a protocol attains perfect completeness, we refer the reader to reference [16] (in particular, Propositions 17 and 18).

7 Conclusions

Our results provide a new way of looking at the class QMA and provide some insight on the power of quantum witnesses. It shows that all quantum witnesses can be replaced by the "simpler" subset states, a fact that may prove helpful both in the case of a quantum PCP and for proving that QMA admits perfect completeness, towards which we have provided some more partial results. Of course, the main question remains open: Are quantum witnesses more powerful than classical ones and if so, why? What we know now, are some things that do not make the quantum witnesses more powerful, for example arbitrary amplitudes or relative phases.

We conclude by stating some open problems. First, can we restrict the quantum witnesses even further? In addition, even though we proved $\mathrm{SQMA}(2) = \mathrm{QMA}(2)$, we are unable to use this result to show a better upper bound than NEXP, the best upper bound currently known. Also, can we prove perfect completeness for QMA through our new characterisation? Last, can we obtain other complete problems for QMA, possibly related to finding the energy of subset states of local Hamiltonians?

Acknowledgements

The authors acknowledge support from a Government of Canada NSERC Postdoctoral Fellowship, the French National Research Agency (ANR-09-JCJC-0067-01), and the European Union (ERC project QCC

306537). Research at the Centre for Quantum Technologies at the National University of Singapore is partially funded by the Singapore Ministry of Education and the National Research Foundation, also through the Tier 3 Grant "Random numbers from quantum processes," (MOE2012-T3-1-009).

References

[1] S. AARONSON: On perfect completeness for QMA. *Quantum Info. Comput.*, 9:81–89, 2009. 4

[2] D. AHARONOV, I. ARAD, AND T. VIDICK: Guest column: The quantum PCP conjecture. *SIGACT News*, 44(2):47–79, 2013. 2

[3] S. ARORA, C. LUND, R. MOTWANI, M. SUDAN, AND M. SZEGEDY: Proof verification and the hardness of approximation problems. *J. ACM*, 45(3):501–555, May 1998. [doi:10.1145/278298.278306] 1

[4] S. ARORA AND S. SAFRA: Probabilistic checking of proofs: A new characterization of NP. *J. ACM*, 45(1):70–122, January 1998. 1

[5] H. BLIER AND A. TAPP: All languages in NP have very short quantum proofs. In *Proceedings of the 2009 Third International Conference on Quantum, Nano and Micro Technologies*, ICQNM '09, pp. 34–37, Washington, DC, USA, 2009. IEEE Computer Society. [doi:10.1109/ICQNM.2009.21] 3

[6] S. A. COOK: The complexity of theorem proving procedures. In *Proc. ACM Symposium on Theory of Computing (STOC)*, pp. 151–158, 1971. 1

[7] T. CUBITT AND A. MONTANARO: Complexity classification of local Hamiltonian problems. In *Proc. IEEE Symposium on the Foundations of Computer Science (FOCS)*, pp. 120–129, 2014. 2

[8] S. GHARIBIAN, J. SIKORA, AND S. UPADHYAY: QMA variants with polynomially many provers. *Quantum Info. Comput.*, 13(1-2):135–157, 2013. 5

[9] S. HALLGREN, D. NAGAJ, AND S. NARAYANASWAMI: The local Hamiltonian problem on a line with eight states is QMA-complete. *Quantum Info. Comput.*, 13(9-10):721–750, September 2013. 2

[10] A. W. HARROW AND A. MONTANARO: Testing product states, quantum Merlin-Arthur games and tensor optimization. *J. ACM*, 60(1):3:1–3:43, February 2013. [doi:10.1145/2432622.2432625] 10

[11] R. JAIN, S. UPADHYAY, AND J. WATROUS: Two-message quantum interactive proofs are in PSPACE. In *Proc. IEEE Symposium on Foundations of Computer Science, (FOCS)*, pp. 534–543, 2009. 8

[12] S. P. JORDAN, H. KOBAYASHI, D. NAGAJ, AND H. NISHIMURA: Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. *Quantum Info. Comput.*, 12(5-6):461–471, May 2012. 2, 13

[13] J. KEMPE, H. KOBAYASHI, K. MATSUMOTO, AND T. VIDICK: Using entanglement in quantum multi-prover interactive proofs. In *Proceedings of 23rd IEEE Conference on Computational Complexity (CCC)*, pp. 211–222, 2008. 13

[14] J. KEMPE AND O. REGEV: 3-local Hamiltonian is QMA-complete. *Quantum Info. Comput.*, 3(3):258–264, 2003. 2

[15] A. KITAEV, A. SHEN, AND M. N. VYALYI: *Classical and quantum computation*. Graduate studies in mathematics. American mathematical society, Providence (R.I.), 2002. 1, 2

[16] H. KOBAYASHI, F. LE GALL, AND H. NISHIMURA: Stronger methods of making quantum interactive proofs perfectly complete. In R. D. KLEINBERG, editor, *ITCS*, pp. 329–352. ACM, 2013. 4, 13, 14

[17] L. A. LEVIN: Universal sequential search problems. *Problems of Information Transmission*, 9(3):265–266, 1973. 1

[18] C. MARRIOTT AND J. WATROUS: Quantum Arthur-Merlin games. *Computational Complexity*, 14, 2005. 2

[19] R. OLIVEIRA AND B. M. TERHAL: The complexity of quantum spin systems on a two-dimensional square lattice. *Quantum Info. Comput.*, 8(10):0900–0924, 2008. 2

[20] J. WATROUS: Succinct quantum proofs for properties of finite groups. In *Proc. IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 537–546, 2000. 2

[21] J. WATROUS: Quantum computational complexity. In ROBERT A. MEYERS, editor, *Encyclopedia of Complexity and Systems Science*, pp. 7174–7201. Springer, 2009. [doi:10.1007/978-0-387-30440-3-428] 5

[22] J. WATROUS: Zero-knowledge against quantum attacks. *SIAM J. Comput.*, 39(1):25–58, 2009. 13

[23] P. WOCJAN, D. JANZING, AND T. BETH: Two QCMA-complete problems. *Quantum Info. Comput.*, 3(6):635–643, 2003. 3, 5, 6

AUTHORS

Alex Bredariol Grilo
Graduate Student
Université Paris Diderot 7, Paris, France
abgrilo@irif.univ-paris-diderot.fr
http://www.irif.univ-paris-diderot.fr/~abgrilo

Iordanis Kerenidis
Senior Researcher
Université Paris Diderot 7, Paris, France, and
CQT, National University of Singapore, Singapore, Singapore
jkeren@irif.univ-paris-diderot.fr
http://www.irif.univ-paris-diderot.fr/~jkeren

Jamie Sikora
CQT Research Fellow
NSERC Postdoctoral Fellow
CQT, National University of Singapore, Singapore
MajuLab, CNRS-UNS-NUS-NTU International Joint Research Unit, UMI 3654, Singapore
cqtjwjs@nus.edu.sg
https://sites.google.com/site/jamiesikora/