

# QMA with subset state witnesses

Alex B. Grilo<sup>1</sup>, Iordanis Kerenidis<sup>1,2</sup>, and Jamie Sikora<sup>2</sup>

<sup>1</sup> LIAFA, CNRS, Université Paris Diderot, Paris, France

<sup>2</sup>Centre for Quantum Technologies, National University of Singapore, Singapore

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, 13]. 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 [11] and called QMA, has been the subject of extensive study in the last decade. Many important properties of this class are known, including a strong amplification property and an upper bound of PP [14], as well as a number of complete problems related to the ground state energy of different types of Hamiltonians [11, 10, 15, 7, 8]. Nevertheless, there are many questions that remain open about the class QMA, for example 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 [9].

In this paper, we further 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 real-valued 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). 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,  $|S\rangle := \frac{1}{\sqrt{|S|}} \sum_{i \in S} |i\rangle$ .

**Definition 1 (SQMA).** A promise problem  $(L_{\text{yes}}, L_{\text{no}})$  is in SQMA if for every  $x \in L_{\text{yes}} \cup L_{\text{no}}$ , there exists a polynomial time quantum verifier  $V_x$ , such that

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

The only difference with 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 simpler to create.

Notice, nevertheless, that the Group Non-Membership Problem is in SQMA, since the witness in the known QMA protocol is a subset state [16]. 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.

**Result 2.** SQMA = QMA

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 that for any unit vector in  $\mathbb{R}^{2^n}$ , there exists a subset state, such that their inner product is  $\Omega(\frac{1}{\sqrt{n}})$ . 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  $b - a \geq 1/\text{poly}(n)$ . 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.

We provide one new complete problems for QMA related to subset states. This problem is based on the QCMA-complete problem Identity Check on Basis States [17]:

**Result 3.** The following Basis State Check on Subset States problem is a complete problem for QMA.

- *Input:* Let  $x$  be a classical description of a quantum circuit  $Z_x$  on  $n$  qubits and  $y$  be an  $n'$ -bit string (where  $n' \leq n$ ). Decide whether
- *Yes:* there is a subset  $S$  such that  $\|(\langle y | \otimes I)Z_x |S\rangle\|_2^2 \geq 2/3$ ,
- *No:* for all subsets  $S$ , we have  $\|(\langle y | \otimes I)Z_x |S\rangle\|_2^2 \leq 1/3$ .

**Perfect completeness.** Another important open question about QMA is whether it admits perfect completeness. Using our characterisation, this question can be reduced to the question of whether SQMA is equal to SQMA<sub>1</sub>. On one hand, the result of [1] can be used to show that there exists a quantum oracle relative to which these two classes are not equal (SQMA<sup>A</sup> ≠ SQMA<sub>1</sub><sup>A</sup>). 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 of the following closely related class:

**Definition 4** (oSQMA). *A promise problem  $(L_{yes}, L_{no})$  is in oSQMA if for every  $x \in L_{yes} \cup L_{no}$ , there exists a polynomial time quantum verifier  $V_x$ , such that*

- (completeness) for all  $x \in L_{yes}$ , there exists a subset state witness  $|S\rangle$  that maximizes the probability the verifier accepts and this probability is  $\geq \frac{2}{3}$ .
- (soundness) for all  $x \in L_{no}$  and all quantum witnesses  $|\psi\rangle$ , the verifier accepts with probability  $\leq \frac{1}{3}$ .

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<sub>1</sub> than the previously known QCMA bound.

**Result 5.** SQMA<sub>1</sub> = oSQMA<sub>1</sub> = oSQMA and hence, oSQMA ⊆ QMA<sub>1</sub> ⊆ 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 [12] and prove our result.

**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.

*For a full version of the paper please consult arXiv:1410.2882*

## References

- [1] Scott Aaronson. On perfect completeness for QMA. *Quantum Information & Computation*, 9:81–89, 2009.
- [2] Dorit Aharonov, Itai Arad, and Thomas Vidick. Guest column: the quantum pcp conjecture. *SIGACT News*, 44(2):47–79, 2013.
- [3] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *J. ACM*, 45(3):501–555, May 1998.
- [4] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs: A new characterization of NP. *J. ACM*, 45(1):70–122, January 1998.
- [5] Hugue Blier and Alain 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*, pages 34–37, Washington, DC, USA, 2009. IEEE Computer Society.
- [6] S. A. Cook. The complexity of theorem proving procedures. In *Proceedings of the Third Annual ACM Symposium*, pages 151–158, New York, 1971. ACM.
- [7] T. Cubitt and A. Montanaro. Complexity classification of local hamiltonian problems. Available at arXiv.org e-Print quant-ph/1311.3161, 2013.
- [8] Sean Hallgren, Daniel Nagaj, and Sandeep Narayanaswami. The local hamiltonian problem on a line with eight states is QMA-complete. *Quantum Info. Comput.*, 13(9-10):721–750, September 2013.
- [9] S. P. Jordan, H. Kobayashi, D. Nagaj, and H. Nishimura. Achieving perfect completeness in classical-witness quantum Merlin-Arthur proof systems. *Quantum Information & Computation*, 12(5 & 6):461–471, 2012.
- [10] J. Kempe and O. Regev. 3-local Hamiltonian is QMA-complete. 3(3):258–264, 2003.
- [11] A. Kitaev, A. Shen, and M. Vyalıy. *Classical and quantum computation*. Graduate studies in mathematics. American mathematical society, Providence (R.I.), 2002.
- [12] Hirotada Kobayashi, François Le Gall, and Harumichi Nishimura. Stronger methods of making quantum interactive proofs perfectly complete. In Robert D. Kleinberg, editor, *ITCS*, pages 329–352. ACM, 2013.
- [13] L. A. Levin. Universal sequential search problems. *Problems of Information Transmission*, 9(3):265–266, 1973.
- [14] Chris Marriott and John Watrous. Quantum arthur-merlin games. *Computational Complexity*, 14:2005.
- [15] R. Oliveira and B. M. Terhal. The complexity of quantum spin systems on a two-dimensional square lattice. *Quantum Information & Computation*, 8(10):0900–0924, 2008.
- [16] John Watrous. Succinct quantum proofs for properties of finite groups. In *FOCS*, pages 537–546. IEEE Computer Society, 2000.
- [17] Pawel Wocjan, Dominik Janzing, and Thomas Beth. Two qcma-complete problems. *Quantum Information & Computation*, 3(6):635–643, 2003.