The Complexity of the Separable Hamiltonian Problem

André Chailloux* Or Sattath †

November 11, 2011

Abstract

In this paper, we study variants of the canonical LOCAL HAMILTONIAN problem where, in addition, the witness is promised to be separable. We define two variants of the LOCAL HAMILTONIAN problem. The input for the SEPARABLE LOCAL HAMILTONIAN problem is the same as the LOCAL HAMILTONIAN problem, i.e. a local Hamiltonian and two energies a and b, but the question is somewhat different: the answer is YES if there is a *separable* quantum state with energy at most a, and the answer is NO if *all separable* quantum states have energy at least b. The SEPARABLE SPARSE HAMILTONIAN problem is defined similarly, but the Hamiltonian is not necessarily local, but rather sparse. We show that the SEPARABLE SPARSE HAMILTONIAN problem is QMA(2)-complete, while SEPARABLE LOCAL HAMILTONIAN is in QMA. This should be compared to the LOCAL HAMILTONIAN problem, and the SPARSE HAMILTONIAN problem which are both QMA-complete. To the best of our knowledge, SEPARABLE SPARSE HAMILTONIAN is the first non-trivial problem shown to be QMA(2)-complete.

1 Introduction and Results

1.1 Introduction

The class QMA is the the quantum analogue of the class NP (or more precisely, MA). The class was first studied by Kitaev [KSV02], and has been in the focus since: see [AN02] for a survey, and [Osb11] for a more recent physics-motivated review.

One of the striking results in proof systems is that sometimes, *limiting* the prover can *increase* the power of the proof system. For example IP = PSPACE [LFKN92, Sha92], while MIP = NEXP [BFL91]. This means that two classical provers can prove more languages to a verifier if he has the guarantee that the provers cannot communicate with each other. However, these classical examples require interaction between the prover and the verifier. The class QMA(k), introduced by Kobayashi *et al.* [KMY03], deals with quantum non-interactive proofs and limits the prover to send k non-entangled proofs, or equivalently consider k-unentangled provers that cannot communicate with each other. The question whether QMA(k) = QMA(2) was answered in the affirmative by Harrow and Montanaro [HM10]. The question whether QMA(2) $\subseteq$ QMA is still open. Note that in the classical case, MA(k) = MA(2) = MA.

*LIAFA - Université Paris 7 and UC Berkeley

†School of Computer Science and Engineering, The Hebrew University, Jerusalem, Israel. Supported by the Clore Fellowship program, Julia Kempe's Individual Research Grant of the Israeli Science Foundation and by Julia Kempe's European Research Council (ERC) Starting Grant.

To show the power of unentangled quantum proofs, Blier and Tapp [BT09] first presented a QMA(2) protocol for an NP-complete problem with two quantum witnesses of size $O(\log(n))$. The drawback of this protocol is that the soundness parameter is somewhat disappointing (1 - $\Omega(1/n^6)$). This was first improved by Beigi [Bei10] who showed that the soundness can be reduced to $1 - 1/n^{3+\varepsilon}$ for any $\varepsilon > 0$. Very recently, Le Gall improved this soundness to $1 - \Omega(\frac{1}{n\log(n)})$ [LNN11]. Aaronson *et al.* showed that there exists a short proof for SAT in $\mathsf{QMA}(\tilde{O}(\sqrt{n}))$ [ABD+08], where each unentangled witness has logarithmic size, but where the soundness can be exponentially small. In [HM10] it was shown that SAT $\in \mathsf{QMA}(2)$, where the size of each proof is $\tilde{O}(\sqrt{n})$. These results tend to show that quantum unentangled proofs are very powerful, since they can solve NP-complete problems in a seemingly more efficient way than in QMA.

On the other hand, Brandão *et al.* [BCY11] showed that if the verifier is restricted to performing a Bell measurement, then the resulting class BELL-QMA(2) is equal to QMA. Trying to understand the relationship between QMA and QMA(2) is a fundamental open problem from the point of view of quantum complexity as well as for the understanding of the power of quantum unentangled proofs.

1.2 Contribution

In this paper, we study the relationship between QMA and QMA(2) from a different perspective. We study the LOCAL HAMILTONIAN problem with unentangled witnesses. The k-LOCAL HAMILTONIAN problem is the quantum analog of MAX-k-SAT, and is the canonical QMA-complete problem. The first proof that k-LOCAL HAMILTONIAN is QMA-complete is by Kitaev. Our first result is to extend this construction to separable witnesses in order to find a complete problem for QMA(2). The main ingredient in showing that the k-LOCAL HAMILTONIAN problem is QMA-complete, is Kitaev's Hamiltonian, a Hamiltonian which penalizes states that are not history states. History states are states of the form $|\eta_\psi\rangle \equiv \frac{1}{\sqrt{T+1}}\sum_{t=0}^{T}|t\rangle \otimes |\psi_t\rangle$, where $|\psi_t\rangle$ is the state at the t-th step of the verification process when starting with $|\psi\rangle$ and the the m ancilla qubits in 0 state, i.e. $|\psi_t\rangle = U_t U_{t-1} \dots U_0(|0^m\rangle \otimes |\psi\rangle)$, and U_i is the i-th gate used in the QMA verification circuit, and we set as a convention $U_0 = I$.

It is natural to try to adapt this idea to a QMA(2) verification circuit by constructing a SEPARABLE LOCAL HAMILTONIAN problem: the input for the SEPARABLE LOCAL HAMILTONIAN problem is the same as the LOCAL HAMILTONIAN problem, i.e. a collection of local Hamiltonians $\{H_1, \dots, H_m\}$, the answer is YES if there is a *separable* quantum state with energy at most a, and the answer is NO if *all separable* quantum states have energy at least b for some energies $a < b$. But there is a flaw in this idea: even if $|\psi\rangle = |\chi_A\rangle \otimes |\chi_B\rangle$, the history state $|\eta_\psi\rangle$ might not be separable.

In order to resolve the entanglement issue in $|\eta_\psi\rangle$, we use the construction of Harrow and Montanaro [HM10]. They show that every $\mathsf{QMA}(k)$ verification circuit can be transformed into a QMA(2) circuit with the following structure: The first and second witnesses(which are promised to be non-entangled) have the same length, where each witness contains r registers, where each register size in the first and second witnesses is the same. The first r steps of the verification procedure are swap-tests between the i-th register of the first and second witnesses, and from that point, the verification circuit acts non-trivially only on the first witness. In a YES instance, there exists a non-entangled proof, where $|\chi_A\rangle = |\chi_B\rangle = |\chi_1\rangle \otimes |\chi_2\rangle \otimes \dots \otimes |\chi_r\rangle$. Notice that $C - SWAP(|+\rangle \otimes |\phi\rangle \otimes |\phi\rangle) = |+\rangle \otimes |\phi\rangle \otimes |\phi\rangle$, therefore, applying the swap-tests to the above witnesses does not change the state. Since there are no other operations on the second witness, the second witness remains fixed during the entire verification process. If we treat the clock, ancilla

qubits and the first witness as the A system, and the second witness as the B system, we get that the history state $|\eta\rangle$ is indeed separable with respect to this division. This is only true if the controlled swap operation is applied on *all* the qubits in the i-th register of the first and second witnesses. This will make the propagation terms in Kitaev's Hamiltonian non-local. But, on the other hand, a controlled swap operation on arbitrary number of qubits is always sparse: each row has one non-zero entry. This makes each propagation term sparse.

Given a sparse Hamiltonian H, the unitary $U = exp(-iHt)$ can be implemented efficiently, which eventually leads to SEPARABLE SPARSE HAMILTONIAN $\in$ QMA(2). Together with the idea above, it can be shown that:

Theorem 1. SEPARABLE SPARSE HAMILTONIAN *is QMA(2)-complete.*

The only reason why, this construction does not lead to a SEPARABLE LOCAL HAMILTONIAN instance, is that the controlled swap gate must be performed in one step; otherwise, $|\eta\rangle$ would become entangled. At first glance, this might seem as a technicality, but we surprisingly show that:

Theorem 2. SEPARABLE LOCAL HAMILTONIAN *is QMA-complete.*

Since the SEPARABLE LOCAL HAMILTONIAN problem is at least as hard as the LOCAL HAMILTONIAN problem, and LOCAL HAMILTONIAN is QMA-complete, therefore SEPARABLE LOCAL HAMILTONIAN is QMA-hard. To show that SEPARABLE LOCAL HAMILTONIAN $\in$ QMA, we use the CONSISTENCY OF LOCAL DENSITY MATRICES problem [Liu06] as a subroutine. Informally, the CONSISTENCY OF LOCAL DENSITY MATRICES promise problem asks the following question: given a collection of local density matrices ρ_i over a constant set of qubits C_i, is there a quantum state ρ such that for each i, the reduced density matrix of ρ over the qubits C_i is equal to ρ_i? Liu showed that this problem is QMA-complete.

To show that SEPARABLE LOCAL HAMILTONIAN is QMA-complete, we do as follows. Assume that there exists a state $\sigma = \sigma_A \otimes \sigma_B$ of total length $2n$, with energy below the threshold a. Let $\mathcal{A}, \mathcal{B}$ the two spaces of qubits considered, each of size n. The energy is $\mathrm{tr}(H(\sigma_A \otimes \sigma_B))$ where $H = \sum_i H_i$. Let C_i the subset of qubits each H_i act on. We have $\mathrm{tr}(H(\sigma_A \otimes \sigma_B)) = \sum_{i=1}^{m} \mathrm{tr}(H_i \sigma^{C_i})$, where σ^{C_i} corresponds to the reduced state of σ on the qubits of C_i. Again, we can decompose σ^{C_i} into the A part and the B part. We can write $\sigma^{C_i} = \sigma^{A_i} \otimes \sigma^{B_i}$. This is because the state σ is a product state between $\mathcal{A}$ and $\mathcal{B}$, hence, the state σ^{C_i} is also a product state between $\mathcal{A}$ and $\mathcal{B}$.

The proof will consist of a classical part: the classical description of the reduced density matrices $\sigma^{A_i}, \sigma^{B_i}$. This information is sufficient to calculate the energy classically, using $\mathrm{tr}(H(\sigma_A \otimes \sigma_B)) = \sum_{i=1}^{m} \mathrm{tr}(H_i(\sigma^{A_i} \otimes \sigma^{B_i}))$. The proof also consists of a quantum part: the prover tries to convince the verifier that there exists a quantum mixed state ρ_A and similarly for ρ_B that are consistent with the reduced density matrices σ^{A_i} and σ^{B_i}. Since CONSISTENCY OF LOCAL DENSITY MATRICES is known to be in QMA, the prover can convince the verifier if there exists such a state, but cannot fool the verifier if there is no such state.

Discussion In the setting of QMA, both the LOCAL HAMILTONIAN and the SPARSE HAMILTONIAN are natural QMA-complete problems. When we consider separable witnesses, SEPARABLE LOCAL HAMILTONIAN and SEPARABLE SPARSE HAMILTONIAN seem to be natural QMA(2)-complete problem. Theorem 1 proves that SEPARABLE SPARSE HAMILTONIAN is indeed QMA(2)-complete, in sharp contrast to the SEPARABLE LOCAL HAMILTONIAN problem, which is shown to be in QMA, by Theorem 2.

Acknowledgments

We thank Fernando Brandão for his contribution to the soundness proof of Thm. 1.

References

[ABD+08] S. Aaronson, S. Beigi, A. Drucker, B. Fefferman, and P.W. Shor. The power of unentanglement. *Electronic Colloquium on Computational Complexity (ECCC)*, 15(051), 2008.

[AN02] D. Aharonov and T. Naveh. Quantum NP-A Survey. *Arxiv preprint quant-ph/0210077*, 2002.

[BCY11] F.G.S.L. Brandão, M. Christandl, and J. Yard. A quasipolynomial-time algorithm for the quantum separability problem. In *Proceedings of the 43rd annual ACM symposium on Theory of computing*, STOC '11, pages 343–352, New York, NY, USA, 2011. ACM.

[Bei10] S. Beigi. NP vs QMA_log(2). *Quantum Info. Comput.*, 10:141–151, January 2010.

[BFL91] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational complexity*, 1(1):3–40, 1991.

[BT09] 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*, pages 34–37, Washington, DC, USA, 2009. IEEE Computer Society.

[HM10] A.W. Harrow and A. Montanaro. An efficient test for product states with applications to quantum merlin-arthur games. In *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, pages 633–642. IEEE, 2010.

[KMY03] H. Kobayashi, K. Matsumoto, and T. Yamakami. Quantum merlin-arthur proof systems: Are multiple merlins more helpful to arthur? *Algorithms and Computation*, pages 189–198, 2003.

[KSV02] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, Boston, MA, USA, 2002.

[LFKN92] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM (JACM)*, 39(4):859–868, 1992.

[Liu06] Y.K. Liu. Consistency of local density matrices is QMA-Complete. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 438–449. Springer Berlin, 2006.

[LNN11] F. Le Gall, S. Nakagawa, and H. Nishimura. On QMA Protocols with Two Short Quantum Proofs. *Arxiv preprint arXiv:1108.4306*, August 2011.

[Osb11] T.J. Osborne. Hamiltonian complexity. *Arxiv preprint arXiv:1106.5875*, 2011.

[Sha92] A. Shamir. IP= PSPACE. *Journal of the ACM (JACM)*, 39(4):869–877, 1992.