QMA-hardness of Consistency of Local Density Matrices with Applications to Quantum Zero-Knowledge

Anne Broadbent * Alex B. Grilo †

Abstract

We provide several advances to the understanding of the class of Quantum Merlin-Arthur proof systems (QMA), the quantum analogue of NP. Our central contribution is proving a longstanding conjecture that the *Consistency of Local Density Matrices* (CLDM) problem is QMA-hard under Karp reductions. The input of CLDM consists of local reduced density matrices on sets of at most k qubits, and the problem asks if there is an n-qubit global quantum state that is locally consistent with all of the k-qubit local density matrices. The containment of CLDM in QMA and the QMA-hardness under Turing reductions were proved by Liu [APPROX-RANDOM 2006]. Liu also conjectured that CLDM is QMA-hard under Karp reductions, which is desirable for applications, and we finally prove this conjecture. We establish this result using the techniques of *simulatable codes* of Grilo, Slofstra, and Yuen [FOCS 2019], simplifying their proofs and tailoring them to the context of QMA.

In order to develop applications of CLDM, we propose a framework that we call *locally simulatable proofs* for QMA: this provides QMA proofs that can be efficiently verified by probing only k qubits and, furthermore, the reduced density matrix of any k-qubit subsystem of a *good* witness can be computed in polynomial time, independently of the witness. Within this framework, we show several advances in zero-knowledge in the quantum setting. We show for the first time a commit-and-open computational zero-knowledge proof system for all of QMA, as a quantum analogue of a "sigma" protocol. We then define a *Proof of Quantum Knowledge*, which guarantees that a prover is effectively in possession of a quantum witness in an interactive proof, and show that our zero-knowledge proof system satisfies this definition. Finally, we show that our proof system can be used to establish that QMA has a quantum *non-interactive* zero-knowledge proof system in the secret parameter setting.
Full version available at: arxiv:1911.07782[1]

In a QMA proof system, an all-powerful prover produces a quantum proof that is verified by a quantum polynomially-bounded verifier. Given the probabilistic nature of quantum computation, we require that for true statements, there exists a quantum proof that makes the verifier accept with high probability (this is called *completeness*), whereas all "proofs" for false statements are rejected with high probability (which is called *soundness*). On top of being the generalization of one of the most important complexity classes, the importance of QMA from a physical perspective comes from the fact that Kitaev also proved that a problem very relevant to physics, the local Hamiltonian problem, is QMA-complete. Much follow-up work focused on understanding the complete problems for QMA, mostly by improving the parameters of the QMA-hard Local Hamiltonian problem, or making it closer to models more physically relevant, *e.g.* [7, 14, 16].

Despite the importance of this class, relatively few QMA-complete problems are known. In 2014, a survey of QMA-complete languages [2] contained a list of 21 problems that are known to be QMA-complete[2], and since then, the situation has not drastically changed. This contrasts with the development of NP, where only a few years after the developments surrounding 3–SAT, hundreds of NP-complete problems were known [10, 15].

The *Consistency of Local Density* matrices problem (CLDM), is a related and conceptually interesting problem, and is defined as follows. Given the classical description of local density matrices $\rho_1, ..., \rho_m$, each on a set of at most k qubits and for a global system of n qubits, is there a state τ that is consistent with such reduced states? Liu [18] showed that this problem is in QMA and that it is QMA-hard under Turing reductions, *i.e.*, a deterministic polynomial-time algorithm with access to an oracle that solves CLDM in unit time can solve any problem in QMA; however, Liu left as open problem to determine if CLDM is also QMA-complete under standard Karp reductions, *i.e.*, to show an efficient mapping between yes- and no-instances of any QMA problem to yes- and no-instances of CLDM, respectively. We remark that Turing reductions are rather troublesome for QMA, since the class is not

*University of Ottawa, Department of Mathematics and Statistics abroadbe@uottawa.ca
†Sorbonne Université, CNRS, LIP6 Alex.Bredariol-Grilo@lip6.fr

[1] An extended abstract is to appear in the Proceedings of FOCS (2020).

[2] We remark that these problems can be clustered as variations of a handful of base problems.

known (nor expected) to be closed under complement, *i.e.*, it is widely believed that QMA $\neq$ coQMA. If this is indeed the case, then Turing reductions do not allow a black-box generalization of results regarding the CLDM problem to all problems in QMA, and this highlights the importance of Karp reductions.

The main result of our work is to show that the CLDM problem is QMA-hard under Karp reductions, solving the 14-year-old problem proposed by Liu [18].

Result 1. *The* CLDM *problem is* QMA*-complete under Karp reductions.*

To prove this result, we build on a tool developed in [13] called *locally simulatable codes*. Roughly, a code is s-simulatable if there is a classical algorithm (the *simulator*), that can compute the reduced density matrix of the encoding of some n-qubit state ρ on any set of at most s qubits of the encoding. Moreover, we also require that we can compute the density matrices of the *computation* on encoded state.[3] Importantly, the simulator must run in time $poly(n, 2^s)$.[4]

In [13], the authors show that the concatenated Steane code is a locally simulatable code, using extensive calculations with the stabilizers of such a code. A conceptual contribution of our work is to provide a simpler proof of this fact, using solely the connections between quantum error correcting codes and secret sharing protocols [5].

We first recall the quantum Cook-Levin theorem proved by Kitaev [17]. In his proof, Kitaev uses the circuit-to-Hamiltonian construction [8], mapping an arbitrary QMA verification circuit $V = U_T ... U_1$ to a local Hamiltonian H_V that enforces that low energy states are *history states* of the computation, *i.e.*, a *superposition* of the snapshots of V for every timestep $0 \leq t \leq T$:

$$|\Phi\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0...T+1} |t\rangle \otimes U_t \dots U_1 |\psi_{init}\rangle. \tag{1}$$

In the above, the first register is called the *clock* register, and it encodes the timestep of the computation, while the second register contains the snapshot of the computation at time t, *i.e.*, the quantum gates $U_1, ..., U_t$ applied to the initial state $|\psi_{init}\rangle = |\phi\rangle|0\rangle^{\otimes A}$, that consists of the quantum witness and auxiliary qubits. The Hamiltonian H_V also guarantees that $|\psi_{init}\rangle$ has the correct form at $t = 0$, and that the final step *accepts*, *i.e.*, the output qubit is close to $|1\rangle$.

The solution is to consider a different verification algorithm V' that implements V on *encoded data*, much like in the theory of fault-tolerant quantum computing. In more details, for a fixed locally simulatable code, V' expects the encoding of the original witness $\mathsf{Enc}(|\phi\rangle)$ and then, with her raw auxiliary states, she creates encodings of auxiliary states $\mathsf{Enc}(|0\rangle)$ and magic states $\mathsf{Enc}(|\mathsf{MS}\rangle)$, and then performs the computation V through transversal gates and magic state gadgets, and finally decodes the output qubit. This gives rise to a new history state:

$$|\Phi'\rangle = \frac{1}{\sqrt{T'+1}} \sum_{t=0...T'+1} |t\rangle \otimes U'_t \dots U'_1 |\psi'_{init}\rangle, \tag{2}$$

where $|\psi'_{init}\rangle = \mathsf{Enc}(|\phi\rangle)|0\rangle^{\otimes A'}$ and $U'_1, ..., U_{T'}$ are the gates of V' described above. Using the techniques from [13], we can show that from the properties of the locally simulatable codes, the reduced density matrix on every set of 5 qubits of $|\Phi'\rangle$ can be efficiently computed. In this work, we prove that these reduced density matrices are in fact QMA-hard instances of CLDM. More concretely, we show that these reduced density matrices of a hypothetical history state of an accepting QMA-verification can always be computed, and there exists a global state (namely the history state) consistent with these reduced density matrices if and only if the original QMA verification accepts with overwhelming probability (and therefore we are in the case of a yes-instance).

Applications to Zero-Knowledge Protocols

Intuitively, a proof system (such as QMA) is said to be *zero-knowledge* if the verifier *does not learn anything* from interacting with the prover. This property is formalized by showing the existence of an efficient *simulator*, which is

[3] This is reminiscent of the theory of fault-tolerant quantum computation, according to which some quantum error-correcting codes allow computations over *encoded* data by using "transversal" gates and encoded magic states.

[4] Note that a straightforward classical simulation of a computation would lead to a runtime $O(2^n)$ and our simulation exponentially improves on the dependency on n.

able to reproduce (*i.e., simulate*) the output of any given verifier on a *yes* instance (without having direct access to the actual prover or witness). As paradoxical as it sounds, statistical zero-knowledge interactive proof systems are known to be possible for a host of languages; their impact is profound and applicable to multiple areas, including cryptography [11] and complexity theory [20].

Zero-Knowledge Proofs for QMA. There has been a recent effort to devise efficient and simpler zero-knowledge protocols for QMA. We point out that Liu [18] observed very early on that the CLDM problem could admit a simple zero-knowledge proof system following the "commit-and-open" approach, as in the 3-COL protocol (this is called a Σ-*protocol*). Inspired by this observation, recent progress has established the existence of zero-knowledge protocols for all of QMA [3]. We note that although the proof system used there is reminiscent of a Σ-protocol, there are a number of reasons why it is not a "natural" quantum analogue of a Σ protocol (which we call a Ξ protocol). These include: (i) the use of a coin-flipping protocol, increasing the communication cost; (ii) the verifier's message is not a random challenge; and (iii) the final answer is not restricted to the opening of some committed values. In our work, we finally show a simple Ξ protocol for QMA via our hardness result for CLDM.

Result 2. *All problems in* QMA *admit a computational zero-knowledge Ξ-proof system.*

Zero-Knowledge Proofs of Knowledge (PoK). In a zero-knowledge proof, the verifier becomes convinced of the *existence* of a witness, but this a priori has no bearing on the prover actually having in her possession such a witness. In some circumstances, it is important to guarantee that the prover actually has a witness. This is the realm of a *zero-knowledge proof of knowledge (PoK)* [1, 12].

We give an example to depict this subtlety. Let us consider the task of anonymous credentials [4]. In this setting, Alice wants to authenticate into some online service using her private credentials. In order to protect her credentials, she could engage in a zero-knowledge proof; this, however would be unsatisfactory, since the verifier in this scenario would be become convinced of the *existence* of accepting credentials, which does not necessarily translate to Alice actually being in the *possession* of these credentials. To remedy this situation, the PoK property establishes an "if-and-only-if" situation: if the verifier accepts, then we can guarantee that the prover actually *knows* a witness. This notion is formally defined by requiring the existence of an *extractor*, which is a polynomial-time process K that outputs a valid witness when given oracle access to some prover P^* that makes the verifier accept with high enough probability.

In the quantum case, there has been some positive results in terms of the security of classical proofs of knowledge for NP against quantum adversaries [19]. However, in the fully quantum case (that is, proofs of quantum knowledge for QMA), no scheme has been proposed. One of the possible reasons why no such proof of quantum knowledge protocols was proposed is the lack of a *simple* zero-knowledge proof for QMA.

We provide the definition of a *Proof of Quantum Knowledge (PoQ)*.[5] In short, we say that a proof system is a PoQ if there exists a quantum polynomial-time *extractor* K that has oracle access to a quantum prover which makes the verifier accept with high enough probability, and the extractor is able to output a sufficiently good witness for a "QMA-relation". We note that this definition for a PoQ is not a straightforward adaptation of the classical definition; this is because NP has many properties such as perfect completeness, perfect soundness and even that proofs can be copied, that are not expected to hold in the QMA case. We are then able to show that our Ξ protocols for QMA described in Result 2 is a PoQ. This is the first proof of knowledge for QMA.[6]

Result 3. *All problems in* QMA *admit a zero-knowledge proof of quantum knowledge proof system.*

We remark that using techniques for post-hoc delegation of quantum computation [9], our PoQ for QMA may be understood as a *proof-of-work* for quantum computations, since it could be used to convince a verifier that the prover has indeed created the *history state* of some pre-defined computation. This is very relevant in the scenario of testing small-scale quantum computers in the most adversarial model possible: the zero-knowledge property ensures that the verifier learns nothing but the truth of the statement, while the PoQ property means that the prover has indeed prepared a ground state with the given properties.

Remark 1. *We note that in our work, we also present other results concerning the concept of locally simulatable proofs, statistical zero-knowledge arguments and non-interactive zero-knowledge protocols in the secret parameters scenario. Given that these contributions easily follow from the ones presented here, we omit them in this abstract.*

[5] This definition is joint work with Coladangelo, Vidick and Zhang [6].

[6] See also independent and concurrent work by Coladangelo, Vidick and Zhang [6].

References

[1] M. Bellare and O. Goldreich. On defining proofs of knowledge. In *CRYPTO 1992*, pages 390–420, 1993. DOI: 10.1007/3-540-48071-4_28.

[2] A. D. Bookatz. QMA-complete problems. *Quant. Inf. Comp.*, 14(5&6):361–383, 2014.

[3] A. Broadbent, Z. Ji, F. Song, and J. Watrous. Zero-knowledge proof systems for QMA. *SIAM J. Comp.*, 49(2):245–283, 2020. DOI: 10.1137/18M1193530.

[4] D. Chaum. Blind signatures for untraceable payments. In *CRYPTO 1983*, pages 199–203, 1983. DOI: 10.1007/978-1-4757-0602-4_18.

[5] R. Cleve, D. Gottesman, and H.-K. Lo. How to share a quantum secret. *Phys. Rev. Lett.*, 83(3):648–651, 1999. DOI: 10.1103/PhysRevLett.83.648.

[6] A. Coladangelo, T. Vidick, and T. Zhang. Non-interactive zero-knowledge arguments for QMA, with preprocessing. In *CRYPTO 2020*, pages 799–828, 2020. DOI: 10.1007/978-3-030-56877-1_28.

[7] T. S. Cubitt and A. Montanaro. Complexity classification of local Hamiltonian problems. In *FOCS 2014*, pages 120–129, 2014. DOI: 10.1109/FOCS.2014.21.

[8] R. P. Feynman. Simulating physics with computers. *Internat. J. Theoret. Phys.*, 21(6):467–488, 1982. DOI: 10.1007/BF02650179.

[9] J. F. Fitzsimons, M. Hajdušek, and T. Morimae. Post hoc verification of quantum computation. *Phys. Rev. Lett.*, 120(4):040501, 2018. DOI: PhysRevLett.120.040501.

[10] M. R. Garey and D. S. Johnson. *Computers and Intractability; A Guide to the Theory of NP-Completeness*. W. H. Freeman & Co., 1990.

[11] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *STOC 1987*, pages 218–229, 1987. DOI: 10.1145/28395.28420.

[12] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM J. Comp.*, 18(1):186–208, 1989. DOI: 10.1137/0218012.

[13] A. B. Grilo, W. Slofstra, and H. Yuen. Perfect zero knowledge for quantum multiprover interactive proofs. In *FOCS 2019*, pages 611–635, 2019. DOI: 10.1109/FOCS.2019.00044.

[14] S. Hallgren, D. Nagaj, and S. Narayanaswami. The local Hamiltonian problem on a line with eight states is QMA-complete. *Quant. Inf. Comp.*, 13(9&10):721–750, 2013.

[15] R. M. Karp. Reducibility among combinatorial problems. In *Complexity of Computer Computations*, pages 85–103, 1972. DOI: 10.1007/978-1-4684-2001-2_9.

[16] J. Kempe, A. Kitaev, and O. Regev. The complexity of the local Hamiltonian problem. *SIAM J. Comp.*, 35(5):1070–1097, 2006. DOI: 10.1137/S0097539704445226.

[17] A. Y. Kitaev, A. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*. American Mathematical Society, 2002.

[18] Y. Liu. Consistency of local density matrices is QMA-complete. In *APPROX/RANDOM 2006*, pages 438–449, 2006. DOI: 10.1007/11830924_40.

[19] D. Unruh. Quantum proofs of knowledge. In *EUROCRYPT 2012*, pages 135–152, 2012. DOI: 10.1007/978-3-642-29011-4_10.

[20] S. Vadhan. The complexity of zero knowledge. In *FSTTCS 2007*, pages 52–70, 2007. DOI: 10.1007/978-3-540-77050-3_5.