A Simple Proof of PreciseQMA = PSPACE

Yulong Li
Columbia University

Abstract

We give an alternative proof of PreciseQMA = PSPACE, first proved by Fefferman and Lin (*Innov. Theor. Comp. Sci. 2018*), where PreciseQMA is the class Quantum Merlin-Arthur with inverse exponential completeness-soundness gap. We adapt the proof of Quantum Cook-Levin Theorem to prove the inclusion PSPACE $\subseteq$ PreciseQMA.

1 Introduction

A crucial focus of quantum complexity theory is to study quantum counterparts of classical complexity classes. By comparing the classical and quantum complexity classes, we may better understand the power of quantum computation models. One particularly important quantum complexity class is Quantum Merlin-Arthur (QMA). It is the quantum analog of Merlin-Arthur (MA), and it can also be seen as the quantum equivalent of NP because of the close relationship between the canonical NP-complete problem, the satisfiability problem, and the natural QMA-complete problem, the local Hamiltonian problem. The formal definition of QMA is as following.

Definition 1. *A promise problem $L = (L_{yes}, L_{no})$ is in $\mathsf{QMA}(c, s)$ if there exists a uniform family of quantum circuits $\{V_x\}_x \in \{0,1\}^{|x|}$, each of size at most poly$(|x|)$ and acting on poly$(|x|)$ qubits, such that: For $x \in L_{yes}$, there exists a poly$(|x|)$-qubit state $|\psi\rangle$ such that $\Pr[V_x \text{ accepts } |\psi\rangle] \geq c$; for $x \in L_{no}$, for all poly$(|x|)$-qubit state $|\psi\rangle$: $\Pr[V_x \text{ accepts } |\psi\rangle] \leq s$. The parameter c and s are known as the completeness and soundness of the problem, respectively, and the quantity $c - s$ is known as the* completeness-soundness gap, *or* gap *for short. QMA is typically defined as $\mathsf{QMA}(c, s)$ for all $c - s$ that is inverse polynomial in n.*

One interesting question to ask is how will the precision of values of c and s change the power of QMA. Kitaev showed that as long as the gap $c - s$ is at least inverse polynomial, we can amplify the gap to a constant [KSV02]. It's then natural to ask what if the promise gap is much smaller. Surprisingly, Fefferman and Lin showed that QMA class with inverse exponentially small gap, denoted as PreciseQMA, is equal to PSPACE [FL16a].

Definition 2. PreciseQMA $= \cup_{c,s\in[0,1],c-s\geq 2^{-poly(n)}} \mathsf{QMA}(c, s)$ *where n is the length of the input.*

Theorem 3 ([FL16a]). PreciseQMA = PSPACE

On the other hand, we can upper bound $\mathsf{MA}_{\mathsf{exp}}$, the classical analogy of PreciseQMA with $\mathsf{NP}^{\mathsf{PP}}$, which is widely believed to be strictly contained in PSPACE. This implies a possible separation between the classical complexity class MA and the quantum analogue QMA, at least in the inverse exponential gap setting.

We give an alternate, arguably simpler, proof that PreciseQMA = PSPACE, specifically the direction PreciseQMA $\supseteq$ PSPACE. The direction PreciseQMA $\subseteq$ PSPACE is fairly intuitive. Given a polynomial size proof state and polynomial time verification algorithm, we can simulate the protocol in polynomial space by guessing the proof and performing amplification even when the gap is inverse exponential [FL16a]. The reverse direction, $\mathsf{PreciseQMA} \supseteq \mathsf{PSPACE}$, is more involved. In Fefferman and Lin's original proof, they define the problem *Gapped Succinct Matrix Singularity (GSMS)*, which, informally speaking, takes in a sparse matrix whose smallest eigenvalue is promised to be either 0 or at least inverse exponential and decides between the two cases. They gave a PreciseQMA protocol for *GSMS* based on Hamiltonian simulation and phase estimation and showed that *GSMS* is PSPACE-hard by encoding the configuration graph of a PSPACE machine into a sparse matrix that satisfies the promise gap of *GSMS*. In a follow-up paper by Fefferman and Lin, they prove a more general result about unitary quantum space, of which $\mathsf{PreciseQMA} = \mathsf{PSPACE}$ is a corollary. But their main result still requires a nontrivial reduction to a general linear algebra problem [FL16b].

The proof inspired us to encode the computation of a PSPACE machine *directly* using the Feynman-Kitaev circuit-to-Hamiltonian construction [KSV02]. This proof technique was used to show the QMA-completeness of the Local Hamiltonian problem. In our opinion, the direct encoding of the computation history and the close relationship between Hamiltonian problems and QMA make the proof $\mathsf{PSPACE} \subseteq \mathsf{PreciseQMA}$ more intuitive and sidestep the linear algebraic problem of *GSMS*. As an easy corollary of the proof, we show that PreciseQMA with perfect completeness, denoted as $\mathsf{PreciseQMA}^{c=1}$, is equal to PreciseQMA (Corollary 10), which is first shown in [FL16b]. Note that perfect completeness does not change the class MA [ZF87], the classical analogue of QMA, but it is an open problem whether QMA is equal to $\mathsf{QMA}^{c=1}$. In fact, Aaronson showed that $QMA \neq \mathsf{QMA}^{c=1}$ relative to a quantum oracle [Aar08].

2 Reversible space computation

One crucial difference between classical and quantum computation is that for quantum circuits, we often require the operations to be unitaries which are inherently reversible, while we typically do not have reversibility constraints for Turing machines. Thus, we need the following theorem about reversible classical computation.

Definition 4. *We say a promise problem $L = (L_{yes}, L_{no})$ is in* revPSPACE *(reversible polynomial space) if it can be decided by a polynomial space reversible Turing machine, i.e., a machine for which every configuration has at most one immediate predecessor.*

Theorem 5 ([Ben89])**.** $\mathsf{PSPACE} = \mathsf{revPSPACE}$

Theorem 5 shows that without loss of generality a polynomial-space computation can be made reversible, and thus can be simulated by a unitary quantum circuit with perfect completeness and soundness.

Corollary 6. *If $L \in \mathsf{PSPACE}$, L is recognized by a family of unitary quantum circuits $\{C_n\}$ which run in exponential time and polynomial space in n; moreover, if $x \in L$, then the circuit accepts with probability* 1*, otherwise it accepts with probability* 0*.*

3 QMA with exponentially small gap

Our first step of the proof is to construct a Hamiltonian with inverse exponential promise gap given a PSPACE machine (or equivalently a quantum circuit using exponential time and polynomial space) based on history state construction, which is shown in Lemma. 7. The second step is to give a PreciseQMA protocol for the Local Hamiltonian Problem with inverse exponential promise gaps, which is Algorithm 8.

Lemma 7. *If L is recognized with perfect completeness and soundness by a family of quantum circuits $\{C_n\}$ which run in exponential time and polynomial space in n, then for all $x \in \{0,1\}^n$, there exists a Hamiltonian H_x such that, if $x \in L$, $\min_\psi \langle\psi|H_x|\psi\rangle = 0$, and if $x \notin L$, $\min_\psi \langle\psi|H_x|\psi\rangle \geq \frac{1}{2(T+1)^3}$.*

Proof: We adapt the Quantum Cook-Levin Theorem to the setting of exponentially-long quantum computations. The idea is to construct a Hamiltonian to check to check whether a state encodes a valid history state of a circuit.

Construction:

Suppose the quantum circuit C_n that acts on $S(n)$ qubits and consists of $T(n) = \exp^{poly(n)}$ unitary two-qubit gates, $U_1, \cdots, U_T$. For $b \in \{0,1\}, i \in [S(n)]$, we define $\Pi_i^{|b\rangle}$ to be the projection operator that operates on qubit number i and projects on the subspace spanned by $|b\rangle$.

$$H_{in}^i = \Pi_i^{|\neg x_i\rangle} \otimes |0\rangle\langle 0|_C$$

$$H_{out} = \Pi_1^{|0\rangle} \otimes |T\rangle\langle T|_C$$

$$H_{prop}^t = \frac{1}{2}(I \otimes |t\rangle\langle t| + I \otimes |t-1\rangle\langle t-1| - U_t \otimes |t\rangle\langle t-1| - U_t^\dagger \otimes |t-1\rangle\langle t|)$$

$$H_x = \sum_{i=1}^n H_{in}^i + H_{out} + \sum_{t=1}^T H_{prop}^t$$

for $t \in \{0,1,\ldots,T\}$, where $|t\rangle_C$ is the binary representation of t taking $\log T$ qubits. If $x \in L$, we have the history of computation $|\eta\rangle = \frac{1}{T+1}\sum_{i=1}^T U_t \cdots U_1|\chi\rangle \otimes |t\rangle$ where $|\chi\rangle = |x\rangle \otimes |0\rangle^{\otimes S-n}$ is the start state encoding the work space including an input x. It is straightforward to check that $\langle\eta|H|\eta\rangle = 0$ if $x \in L$ using the fact that C_n accepts x with probability 1 if $x \in L$. If $x \notin L$, following the analysis in [AN02], one can show that $\langle\psi|H|\psi\rangle \geq \frac{1}{2(T+1)^3}$ for all $|\psi\rangle$.

Algorithm 8. *We give a* PreciseQMA *protocol, which given a polynomial size proof state, check the eigenvalue of H_x defined in 7 in polynomial time such that if $\min_{|\psi\rangle}\langle\psi|H_x|\psi\rangle = 0$, always accepts; otherwise, reject with at least inverse exponential probability.*

1. *Pick $y \in [T+n+2]$ uniformly at random.*
2. *Define*

$$H_{test}(y) = \begin{cases} H_{prop}^{y-1}, & y \in [T+1] \\ H_{in}^{y-T-1}, & y \in [T+2, T+n+1] \\ H_{out}, & y = T+n+2 \end{cases}$$

3. *If $H_{test}(y) = H_{in}^i$ or $H_{test} = H_{out}$, which are projections onto standard basis, measure $|\psi\rangle$, reject if the measurement is in the projected space.*
4. *If $H_{test}(y) = H_{prop}^t$, we apply several transformations. Note that*

$$R_t^\dagger H_{prop}^t R_t = \frac{1}{2} I \otimes (|t\rangle - |t-1\rangle)(\langle t| - \langle t-1|)$$

where $R = \sum_{t=0}^T U_t U_{t-1} \cdots U_1 \otimes |t\rangle\langle t|$. Thus, we can design a procedure that involves controlled unitaries of U_t and U_{t+1} that results in measurement of 1 with probability $\langle\psi|H_{prop}^t|\psi\rangle$ in which case we reject.

The total probability of rejection is

$$\frac{1}{T+n+2}\sum_{y=1}^{T+n+2}\langle\psi|H_{test}(y)|\psi\rangle = \frac{1}{T+n+2}\langle\psi|H_x|\psi\rangle$$

For $x \in L$, this equals to 0; for $x \notin L$, this is at least $\exp(-\mathrm{poly}(n))$.

Finally, the result immediately implies that we can always boost the completeness of a PreciseQMA protocol to 1, which is first shown in [FL16b].

Definition 9. $\mathsf{PreciseQMA}^{c=1} = \mathsf{QMA}_{poly}(1, 1-2^{-poly})$

Corollary 10. PreciseQMA= $\mathsf{PreciseQMA}^{c=1}$

Proof. For any $L \in$ PreciseQMA, by Theorem 3 and Corollary 6, we have a uniform family of unitary quantum circuits $\{C_n\}$ which run in exponential time and polynomial space in n that accepts a string in L with probability 1 and rejects otherwise. Then by Lemma 7 and Algorithm 8, we have a $\mathsf{PreciseQMA}^{c=1}$ protocol for L. ☐

However, this is an indirect reduction that goes through PSPACE. It is thus interesting to ask whether there is a direct reduction from PreciseQMA to $\mathsf{PreciseQMA}^{c=1}$.

4 Acknowledgements

We are very thankful to Henry Yuen for introducing the problem and his guidance throughout the process. We are also thankful for helpful discussions with Adrian She at various stages of the work.

References

[Aar08] Scott Aaronson. On perfect completeness for QMA. *Quantum Information and Computation*, 2008.

[AN02] Dorit Aharonov and Tomer Naveh. Quantum NP - a survey, 2002.

[Ben89] Charles H. Bennett. Time/space trade-offs for reversible computation. *Society for Industrial and Applied Mathematics*, 18:766–776, 1989.

[FL16a] Bill Fefferman and Cedric Lin. Quantum Merlin Arthur with exponentially small gap. *arXiv preprint arXiv:1601.01975*, 2016.

[FL16b] Bill Fefferman and Cedric Yen-Yu Lin. A complete characterization of unitary quantum space. *arXiv preprint arXiv:1604.01384*, 2016.

[KSV02] A. Kitaev, A. Shen, and M. N. Vyalyi. Classical and quantum computation. *American Mathematical Society*, 2002.

[ZF87] Stathis Zachos and Martin Furer. Probabilistic quantifiers vs. distrustful adversaries. In *International Conference on Foundations of Software Technology and Theoretical Computer Science*, pages 443–455. Springer, 1987.