A More Direct Proof of $\mathrm{QMA}_{\mathrm{EXP}}$ = PSPACE

Yulong Li
Columbia University

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 better understand the power of quantum computation models. One particular interesting 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, *SAT*, and the natural QMA-*complete* problem, Local Hamiltonian (*LH*). Surprisingly, Fefferman and Lin show that if we allow the confidence and soundness gap of QMA to be inverse exponentially small, denoted as $\mathrm{QMA}_{\mathrm{exp}}$, we can characterize it precisely by PSPACE [2]. On the other hand, we can upper bound $\mathrm{MA}_{\mathrm{exp}}$ with $\mathrm{NP}^{\mathrm{PP}}$, which is contained in PSPACE.

The result $\mathrm{QMA}_{\mathrm{exp}} \subseteq$ PSPACE is more or less 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 proper amplification [2]. The reverse result PSPACE $\subseteq \mathrm{QMA}_{\mathrm{exp}}$ is more surprising. In Fefferman and Lin's original proof, they first characterize PSPACE with *Gapped Succinct Matrix Singularity*, a problem which they prove to be PSPACE-$hard$, and then they solve it with a $\mathrm{QMA}_{\mathrm{exp}}$ protocol. From a abstract perspective, we can understand *Gapped Succinct Matrix Singularity* as encoding the computation path of a PSPACE Turing Machine. This insight motivates us to directly encode the computation path with Hamiltonians using history state construction by Kitaev, Shen, and Vyalyi in their proof that *LH* is QMA-*complete* [3]. In our opinion, the direct encoding of the computation path and the close relationship between Hamiltonian problems and QMA make the proof PSPACE $\subseteq \mathrm{QMA}_{\mathrm{exp}}$ more intuitive.

Preliminaries

Definition 1. We say a promise problem $L = (L_{yes}, L_{no})$ is in (t,k)-bounded $\mathrm{QMA}_m(c,s)$ if there exists a uniform family of quantum circuits $\{V_x\}_x \in \{0,1\}^n$, each of size at most $t(|x|)$, acting on $k(|x|) + m(|x|)$ qubits, so that: If $x \in L_{yes}$ there exists an m-qubit state $|\psi\rangle$ such that:

$$\left(\langle\psi| \otimes \langle 0^k|\right) V_x^\dagger |1\rangle\langle 1|_{out} V_x \left(|\psi\rangle \otimes |0^k\rangle\right) \geq c$$

Whereas for $x \in L_{no}$, for all m-qubit states $|\psi\rangle$:

$$\left(\langle\psi| \otimes \langle 0^k|\right) V_x^\dagger |1\rangle\langle 1|_{out} V_x \left(|\psi\rangle \otimes |0^k\rangle\right) \leq s$$

Definition 2. $\mathrm{QMA}_{\mathrm{exp}} = (poly, poly)$-bounded $\mathrm{QMA}_{poly}(c, c - 2^{-poly})$
Definition 3. $\mathrm{QMA}_{\mathrm{exp}}^{c=1} = (poly, poly)$-bounded $\mathrm{QMA}_{poly}(1, 1 - 2^{-poly})$
This is $\mathrm{QMA}_{\mathrm{exp}}$ with perfect completeness.

Theorem 4. For any $\varepsilon > 0$, any multitape Turing machine running in time T and space S can be simulated by a reversible input-saving machine using time $O(T^{1+\varepsilon})$ and space $O(S \cdot \log T)$. [1]
Corollary 5. PSPACE = revPSPACE
Corollary 6. If $L \in$ PSPACE, L is recognized by a family of quantum circuits $\{C_n\}$ which run in exponential time and polynomial space in n.

Theorem 7. $\mathrm{QMA}_{\mathrm{exp}} \subseteq$ PSPACE [2]

Proof of $\mathrm{QMA}_{\mathrm{exp}} \supseteq$ PSPACE

Recall that the history state construction consists of a set of input-checking Hamiltonians, output-checking Hamiltonians, and propagation-checking Hamiltonians. A clock register is introduced to check a specific time step of the computation.
Lemma 8. If L is recognized 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 $x \notin L$, $\min_\psi \langle\psi|H_x|\psi\rangle \geq \exp(-\mathrm{poly}(n))$.
Proof. The proof is inspired by the Quantum Cook-Levin theorem (KSV reduction) [3]. The idea is to construct a Hamiltonian to check if the circuit has a valid history of computation. Suppose the quantum circuit C_n that acts on $S(n)$ qubits and consists of $T(n) = e^{poly(n)}$ unitary two-qubit gates, $U_1, \cdots, U_T$. We define

$$H_{in}^i = \Pi_i^{|\neg x_i\rangle} \otimes |0\rangle\langle 0|_C$$
$$H_{out} = \Pi_1^{|0\rangle} \otimes |T\rangle\langle T|_C$$
$$H_{prop}^t = \frac{1}{2}(I \otimes |t\rangle\langle t| + I \otimes |t-1\rangle\langle t-1| - U_t \otimes |t\rangle\langle t-1| - U_t^\dagger \otimes |t-1\rangle\langle t|)$$
$$H_x = \sum_{i=1}^{n} H_{in}^i + H_{out} + \sum_{t=1}^{T} H_{prop}^t$$

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 $x \in L$. If $x \notin L$, we can show that $\langle\psi|H|\psi\rangle \geq \frac{1}{4(T+2)^3}$ for all $|\psi\rangle$ with a similar argument used in [3].

The main challenge of encoding a PSPACE Turing Machine comparing to the proof of [3] is that the number of time steps is possibly exponential in the input length, and the clock register is polynomial in the input length. Thus, we have exponentially many checking Hamiltonians, each acting on polynomial number of qubits. Nevertheless, we are allowed inverse exponentially small completeness and soundness gap.
Algorithm 9. We give a $\mathrm{QMA}_{\mathrm{exp}}$ protocol, which given a polynomial size proof state, check the eigenvalue of H_x defined above in polynomial time such that if $\min_\psi \langle\psi|H_x|\psi\rangle = 0$, always accepts; otherwise, reject with at least inverse exponential probability. Given $|\psi\rangle$,

1. Pick $y \in [T + n + 1]$ uniformly at random.
2. Define
$$H_{test}(y) = \begin{cases} H_{prop}^y, & y \in [T] \\ H_{in}^{y-T}, & y \in [T+1, T+n] \\ H_{out}, & y = T+n+1 \end{cases}$$
3. If $H_{test}(y) = H_{in}^i$ or $H_{test} = H_{out}$, which are projections onto standard basis, measure ψ, reject if the measurement is in the projected space.
4. If $H_{test}(y) = H_{prop}^t$, note that H_{prop}^t is also a projection under a rotation
$$R_t^\dagger H_{prop}^t R_t = \frac{1}{2} I \otimes (|t\rangle - |t-1\rangle)(\langle t| - \langle t-1|)$$
where $R = \sum_{t=0}^{T} U_t U_{t-1} \cdots U_1 \otimes |t\rangle\langle t|$, so we can also rotate and measure; reject if the measurement is in the projected space. The total probability of rejection is
$$\geq \frac{1}{T+n+2} \sum_{y=1}^{T+n+2} \langle\psi|H_{test}(y)|\psi\rangle = \frac{1}{T+n+2}\langle\psi|H|\psi\rangle = \exp(-\mathrm{poly}(n))$$

Implications: $\mathrm{QMA}_{\mathrm{exp}} = \mathrm{QMA}_{\mathrm{exp}}^{c=1}$

Lemma 10. If L is recognized 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 which can be written as a sum of $O(exp(n))$ Hermitian PSD matrices each acting on constant number of qubits such that, if $x \in L$, $\min_\psi \langle\psi|H_x|\psi\rangle = 0$, and if $x \notin L$, $\min_\psi \langle\psi|H_x|\psi\rangle \geq \exp(-\mathrm{poly}(n))$.
Proof. Suppose the quantum circuit C_n that acts on $S(n)$ qubits and consists of $T(n) = e^{poly(n)}$ unitary two-qubit gates, $U_1, \cdots, U_T$. The idea is to directly transform the QMA protocol in 9. to a local Hamiltonian. The local Hamiltonian acts on $R(n) + S'(n) + \mathcal{T}(n)$ qubits, where $R(n) = \log(T+n+1)$, $S'(n) = S(n) + \log T(n+1)$, and $\mathcal{T}(n)$ is the maximum number of circuits used in all different cases in Algorithm 9. We can break down Algorithm 9 into two stages: generating a random string $r \in \{0,1\}^{T+n+1}$ and measuring the state. Given a random string r, we use U_τ^r to denote the unitary used at time step τ, which acts on constant number of qubits. We define

$$H_{in}^r = \Pi_r^{|-\rangle} \otimes I \otimes |0\rangle\langle 0|_C$$
$$H_{out} = I \otimes \Pi_1^{|0\rangle} \otimes |\mathcal{T}\rangle\langle\mathcal{T}|_C$$
$$\mathsf{H}_\tau^r = \tfrac{1}{2}|r\rangle\langle r|_R \otimes (I \otimes |\tau\rangle\langle\tau| + I \otimes |\tau-1\rangle\langle\tau-1| - U_\tau^r \otimes |\tau\rangle\langle\tau-1| - U_\tau^{r\dagger} \otimes |\tau-1\rangle\langle\tau|)$$
$$H_x = H_{out} + \sum_{r=0}^{R-1} \left(H_{in}^r + \sum_{\tau=0}^{\mathcal{T}} H_\tau^r\right)$$

If $x \in L$, the desired proof state will be

$$\frac{1}{2^R}\sum_{r=0}^{R-1}\left(\frac{1}{\mathcal{T}+1}\sum_{\tau=0}^{\mathcal{T}} |r\rangle \otimes U_\tau^r \cdots U_1^r |\eta\rangle \otimes |\tau\rangle\right)$$

where again $|\eta\rangle = \frac{1}{T+1}\sum_{i=1}^{T} U_t \cdots U_1 |\chi\rangle \otimes |t\rangle$ and $|\chi\rangle = |x\rangle \otimes |0\rangle^{\otimes S-n}$.

Theorem 11. $\mathrm{QMA}_{\mathrm{exp}} = \mathrm{QMA}_{\mathrm{exp}}^{c=1}$
Proof. For any $L \in \mathrm{QMA}_{\mathrm{exp}}$, by Corollary 5. and Theorem 7., we have a uniform family of quantum circuits $\{C_n\}$ that recognizes precisely L which run in exponential time and polynomial space in n. Then by Lemma 8. and Algorithm 9., we have a QMA protocal for L with perfect completeness and inverse exponential rejection probability.

Acknowledgements

I'd like to thank Henry Yuen, my advisor, and Adrian She very much for introducing me to the problem and guiding me through major difficulties.

References

[1] Charles H. Bennett. "Time/Space Trade-offs for Reversible computation". In: *Society for Industrial and Applied Mathematics* 18 (1989), pp. 766–776.

[2] Bill Fefferman and Cedric Lin. "Quantum Merlin Arthur with Exponentially Small Gap". In: (2016).

[3] A. Kitaev, A. Shen, and M. N. Vyalyi. "Classical and Quantum Computation". In: *American Mathematical Society* (2002).