A complexity theory for synthesizing quantum states: stateQMA and beyond

Yupan Liu

Nagoya University

Mostly based on the joint work with Hugo Delavenne, François Le Gall, and Masayuki Miyamoto (available at arXiv:2303.01877)

Nov 20, 2023

1. State-synthesizing complexity classes: Definitions

2. Which results can be “translated” into state-synthesizing classes?

3. Which results currently do not have state-synthesizing counterparts?

Definitions: Boolean functions vs. state families

Definition 1.1 (QMA). A promise problem $\mathcal{L} = (\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}})$ is in $\text{QMA}[c, s]$ if there is a family of $\text{poly}(n)$-size quantum verification circuits $\{V_x\}_{x \in \mathcal{L}}$ where $n := |x|$, that can be computed by a deterministic $\text{poly}(n)$-time Turing machine, satisfies the following:

Completeness. If $x \in \mathcal{L}_{\text{yes}}$, there is a witness $|w\rangle$ s.t. $\Pr[V_x \text{ accepts } w] \geq c(n)$.

Soundness. If $x \in \mathcal{L}_{\text{no}}$, for any witness $|w\rangle$, $\Pr[V_x \text{ accepts } w] \leq s(n)$.

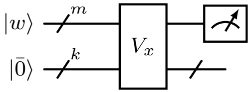


Figure: QMA verification circuit

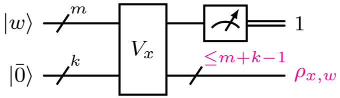


Figure: stateQMA verification circuit

Definition 1.2 (stateQMA). A state family $\{|\psi_x\rangle\}_{x \in \mathcal{L}}$ where $\mathcal{L} \subseteq \{0,1\}^*$ is in $\text{stateQMA}_\delta[c, s]$, if there is a family of $\text{poly}(n)$-size quantum verification circuits $\{V_x\}_{x \in \mathcal{L}}$ where $n := |x|$, that can be computed by a deterministic $\text{poly}(n)$-time TM and output a resulting state $\rho_{x,w}$ when V_x accepts, satisfies the following:

Completeness. If $x \in \mathcal{L}$, there is a state $|w\rangle$ s.t. $\Pr[V_x \text{ accepts } w] \geq c(n)$.

Soundness. For any $|w\rangle$ s.t. $\text{td}(\rho_{x,w}, \psi_x) \geq \delta(n)$, $\Pr[V_x \text{ accepts } w] \leq s(n)$.

* Definition 1.2 is inspired by [Rosenthal-Yuen'22].

Subtleties in the definitions of state-synthesizing complexity classes

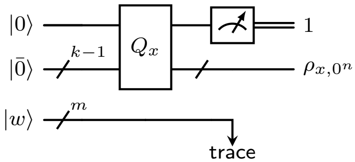
Definition 1.3 (stateBQP). A state family $\{|\psi_x\rangle\}_{x\in\mathcal{L}}$ where $\mathcal{L} \subseteq \{0,1\}^*$ is in stateBQP$_\delta[\gamma]$ if there is a family of $\mathrm{poly}(n)$-size quantum circuits $\{Q_x\}_{x\in\mathcal{L}}$ where $n := |x|$, that can be computed by a deterministic $\mathrm{poly}(n)$-time TM and output a resulting state $\rho_{x,w}$ when Q_x accepts, satisfies the following:

- The probability that Q_x accepts is at least $\gamma(n)$.
- The resulting state ρ_x of the circuit Q_x satisfying $\mathrm{td}(\rho_x, \psi_x) \leq \delta(n)$.

It is not hard to see that stateBQP$_\delta[\gamma] \subseteq$ stateBQP$_{\delta'}[1]$ where $\delta' := \gamma\delta + 1 - \gamma$.

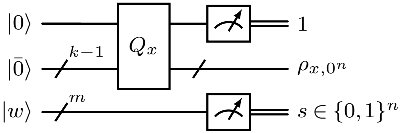
Proposition 1.4 (stateBQP $\subseteq$ stateQMA). stateBQP$_\delta[\gamma] \subseteq$ stateQMA$_\delta[\gamma, \gamma']$ for some $\gamma' > 0$ such that $\gamma(n) - \gamma'(n) \geq 1/\mathrm{poly}(n)$.

First attempt:



There is no promise gap!

Actual solution:



Accept if $s = 0^n$. Then $\gamma(n) - \gamma'(n) \geq 1/\mathrm{poly}(n)$ where $\Pr[V_x \text{ accepts } w] \geq \gamma |\langle w|0^n\rangle|^2 := \gamma' > 0$.

1. State-synthesizing complexity classes: Definitions

2. Which results can be “translated” into state-synthesizing classes?

3. Which results currently do not have state-synthesizing counterparts?

Which results can be “translated” into state-synthesizing classes: stateQIP

Definition 2.1 (stateQIP, informally adapted from [Rosenthal-Yuen’22]). A state family $\{|\psi_n\rangle\}_{n\in\mathbb{N}}$ is in $\mathsf{stateQIP}_{\delta}[c,s]$ if for any $\mathrm{poly}(n)$-time verifier V, there is a *computationally unbounded (and untrusted)* prover P such that V will produce ρ_n when V accepts this interactive protocol $P \rightleftharpoons V$ and all protocols $P \rightleftharpoons V$ satisfy:

Completeness. There is a protocol $P \rightleftharpoons V$ s.t. $\Pr[V \text{ accepts } P \rightleftharpoons V] \geq c(n)$.

Soundness. For any protocol $P \rightleftharpoons V$, if $\mathrm{Tr}(\rho_n, \psi_n) \geq \delta(n)$, then $\Pr[V \text{ accepts } P \rightleftharpoons V] \leq s(n)$.

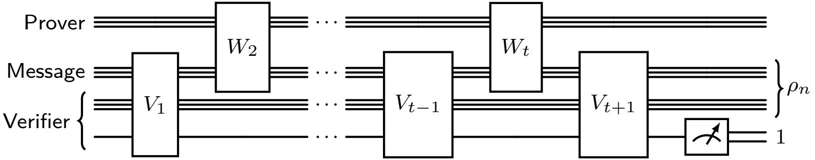


Figure: t-message stateQIP protocol

Which results can be "translated" into state-synthesizing classes: stateQIP (Cont.)

Summary of known results on stateQIP:

Inclusion	Reference	State-synthesizing counterpart
PSPACE $\subseteq$ QIP	PSPACE $\subseteq$ IP $\subseteq$ QIP [Lund-Fortnow-Karloff-Nisan'90, Shamir'90]	statePSPACE$_\delta$ $\subseteq$ stateQIP$_{\delta+1/\mathrm{poly}}$ [Rosenthal-Yuen'22]
QIP(3) $\subseteq$ PSPACE	QIP(3) $\subseteq$ QMAM $\subseteq$ NC(poly) $\subseteq$ PSPACE [Jain-Ji-Upadhyay-Watrous'09] Depth-bounded SDP solver	stateQIP$_\delta$ $\subseteq$ statePSPACE$_{\delta+1/\mathrm{poly}}$ [Metger-Yuen'23] Space-bounded quantum SDP solver
QIP $\subseteq$ QIP(3) "*parallelization*"	[Kitaev-Watrous'03] (also [Kempe-Kobayashi-Matsumoto-Vidick'07])	statePSPACE$_\delta$ $\subseteq$ stateQIP$(6)_{\delta+1/\mathrm{poly}}$ [Rosenthal'23]

Proof Strategies: statePSPACE $\subseteq$ stateQIP

Main techniques: Preparing a state w/ the help of a *trusted* classical oracle

- [Aaronson'16]: $\mathrm{poly}(n)$ adaptive queries protocol.
- [Rosenthal'23]: $\mathrm{poly}(n)$ *non-adaptive* queries protocol $\Rightarrow$ a single query suffices!
- [Lombardi-Ma-Wright'23]: Synthesizing unitary requires *more than one query*.

Bonus: New phenomenon in stateQIP

Question: What is the computational power required to implement the optimal prover strategies? Could we make the implementation computationally bounded?

- [LFKN90, Shamir'90]: $\mathsf{PSPACE} \subseteq \mathsf{IP}[\mathsf{PSPACE}, \mathsf{BPP}]$.
- There is no known quantum analog in the *model of promise problems*!
- [MY23]: $\mathsf{statePSPACE} \subseteq \mathsf{stateQIP}[\mathsf{unitaryPSPACE}, \mathsf{unitaryBQP}]$.

Algorithmic Uhlmann transformation

Uhlmann theorem (1976). Let $|\psi\rangle_{\mathsf{AB}}$ and $|\phi\rangle_{\mathsf{AB}}$ be pure states on registers A, B and denote their reduced states on register A by ρ_A and σ_A, respectively. Then there is a unitary U_B such that $\mathrm{F}(\rho_A, \sigma_A) = |\langle\phi|_{\mathsf{AB}}(I_A \otimes U_B)|\psi\rangle_{\mathsf{AB}}|$.

Implementing the Uhlmann transformation U_{B} is in unitaryPSPACE [MY23].

This techniques is further explored in [Bostanci-Efron-Metger-Poremba-Qian-Yuen'23].

Which results can be "translated" into state-synthesizing classes: stateQMA

① Witness-preserving error reduction for QMA-like classes:

Class	Implication	State-synthesizing counterpart
QMA [Marriott-Watrous'05]	$\mathsf{QMA}_{\log} \subseteq \mathsf{BQP}$ Log-size witness is useless	$\mathsf{stateQMA}_{\log} \subseteq \mathsf{stateBQP}$ [Delavenne-Le Gall-**L.**-Miyamoto'23]
$\mathsf{QMA_UPSPACE}$	$\mathsf{PreciseQMA} \subseteq \mathsf{BQ_UPSPACE}$ [Fefferman-Lin'18]	$\mathsf{statePreciseQMA} \subseteq \mathsf{state_UPSPACE}$ [Delavenne-Le Gall-**L.**-Miyamoto'23]
$\mathsf{QMA_UL}^\dagger$	$\mathsf{QMA_UL} \subseteq \mathsf{BQ_UL}$ [Fefferman-Kobayashi-Lin-Morimae-Nishimura'16]	$\mathsf{stateQMA_UL}^{\mathsf{off}} \subseteq \mathsf{stateBQ_UL}$ Corollary of [Le Gall-**L.**-Wang'23]

†$\mathsf{QMA_UL}$ only allows off-line log-size witness accesses.

② QCMA achieves perfect completeness:

- [Jordan-Kobayashi-Nagaj-Nishimura'11]: $\mathsf{QCMA} \subseteq \mathsf{QCMA}_1$.
- [Delavenne-Le Gall-**L.**-Miyamoto'23]: $\mathsf{stateQCMA} \subseteq \mathsf{stateQCMA}[1, 1-1/\mathrm{poly}]$.

③ How QMA witness states relate to stateQMA?

Theorem 2.2 (UQMA witness is in stateQMA, [Delavenne-Le Gall-**L.**-Miyamoto'23]).

(1) For any $(\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}}) \in \mathsf{UQMA}$, unique-witness state family $\{|w_x\rangle\}_{x\in\mathcal{L}_{\text{yes}}}$ corresponding to *yes* instances is in $\mathsf{stateQMA}_{1/\mathrm{poly}}$.

(2) For any $(\mathcal{L}_{\text{yes}}, \mathcal{L}_{\text{no}}) \in \mathsf{PreciseUQMA}[1-1/\exp, \cdot]$, the unique-witness state family $\{|w_x\rangle\}_{x\in\mathcal{L}_{\text{yes}}}$ corresponding to *yes* instances is in $\mathsf{statePreciseQMA}_{1/\exp}$.

1. State-synthesizing complexity classes: Definitions
2. Which results can be “translated” into state-synthesizing classes?
3. Which results currently do not have state-synthesizing counterparts?

Which results currently do not have state-synthesizing counterparts?

Generally lacking of the notion of hardness for state-synthesizing classes! Only *some variant of unitary-synthesizing classes* admit the notions of reduction and hardness [Bostanci-Efron-Metger-Poremba-Qian-Yuen'23].

There are several results that relies on the notion of hardness:

- [Fefferman-Lin'18] PSPACE is in PreciseQMA.
- [Deshpande-Gorshkov-Fefferman'22] Local Hamiltonian Problem with *exponentially small spectral gap* (and promise gap) is PSPACE-hard.
- [Jeronimo-Wu'23] NEXP is in $\mathsf{QMA}^{+}(2)$, where "$+$" indicates that witness states are entrywise non-negative states in both *yes* and *no* instances.

  See also the follow-up work [Bassirian-Fefferman-Marwaha'23], which shows that NEXP is in QMA^{+} with certain regime.

Question: Is there any new phenomenon in state-synthesizing complexity classess?

Thanks!