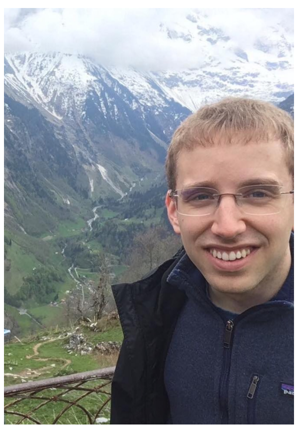
Interactive Proofs for Synthesizing Quantum States & Unitaries



Greg Rosenthal
University of Toronto

Henry Yuen
Columbia University

Motivating Task

Suppose you're given a succinct description of an n-qubit circuit C that has exp(n) many gates.

Ex: $C = e^{-iHt}$ for some local Hamiltonian H, and $t = \exp(n)$.

Your goal is to synthesize

$$|\psi\rangle = C|0^n\rangle.$$

Motivating Task : State Synthesis

Obvious Solution: spend exp(n) time, poly(n) space running C to construct the state.

Cannot synthesize this state in polynomial time unless PSPACE ⊆ BQP.

What if you could interact with an all-powerful prover?

Model

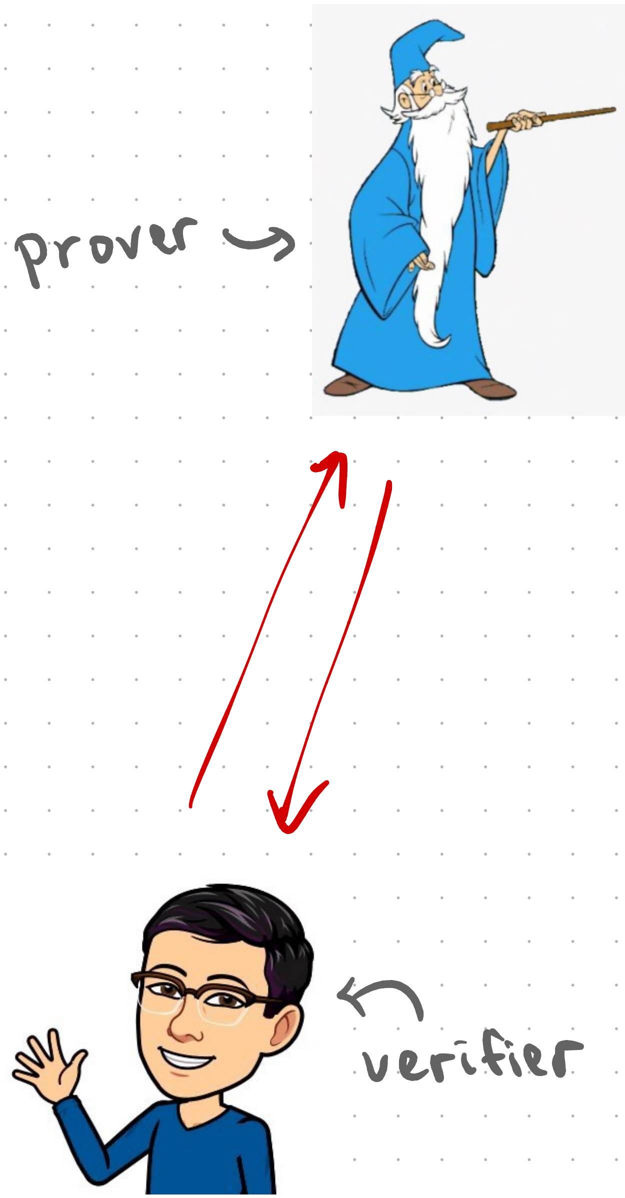
All-powerful quantum prover.

Quantum communication.

Quantum polynomial-time verifier

Goal: By interacting with an omniscient, but untrusted prover, the verifier wants to verifiably synthesize $|\psi\rangle$ in polynomial time.

Model



An **interactive state synthesis** protocol for $|\psi\rangle$ satisfies:

- **completeness:** $\exists$ prover strategy such that verifier accepts with prob $\geq c$ and outputs $\approx |\psi\rangle$.

- **soundness:** $\forall$ prover strategies, if verifier accepts with prob $\geq s$ then output state **conditioned on accepting** is $\approx |\psi\rangle$.

Wait a minute! Doesn't QIP = PSPACE by Jain, Ji, Uppadhyay, Watrous imply there is an interactive proof for synthesizing $|\psi\rangle$?

After all, $|\psi\rangle$ is the result of a quantum polynomial space, exponential time computation

And QPSPACE = PSPACE by a result of Watrous...

Search vs Decision in the Quantum World

QIP = PSPACE is about decision problems.

- verifier wants to decide $x \overset{?}{\in} L$.

State synthesis can be thought of as a "quantum search problem." verifier wants to get its hands on an entire n-qubit state.

Relationship between search and decision problems in quantum setting is much more mysterious!

Search vs Decision in the Quantum World

In classical world, search problems and decision problems often have same complexity.

Ex: If you can efficiently decide 3SAT, you can efficiently find satisfying assignments.

But: unknown if QMA = BQP implies that ground states of local Hamiltonians can be constructed in polynomial time!

In fact, no efficient search-to-decision reduction for QMA relative to a quantum oracle [Y.].

Search vs Decision in the Quantum World

Ex: "classical interactive state synthesis" has a straightforward solution.

Goal: given polynomial space TM M, output final state s of M after $\exp(n)$ steps.

Sol'n: each bit of s is the answer to a PSPACE decision problem ("is the j^{th} bit of $s = 1$?")

Use $IP = PSPACE$ for each bit.

Search vs Decision in the Quantum World

In contrast, quantum state synthesis seems more difficult: verifier is trying to verify the construction of a fragile object

- whose classical description has 2^n complex amplitudes, and

- it should not be entangled with anything else.

Main result (Rosenthal, Y.)

$$\text{statePSPACE} \subseteq \text{stateQIP}$$

"quantum state complexity result"

Theorem: for all space-uniform families of quantum states $\Psi = \{|\psi_n\rangle\}$, there exists an interactive state synthesis protocol for Ψ satisfying, on input $n \in \mathbb{N}$,

- **completeness:** honest prover accepted w.p. 1, output state is $\exp(-n)$ close to $|\psi_n\rangle$.
- **soundness:** if a prover is accepted with prob $\geq \exp(-n)$, output state conditioned on accepting is $\frac{1}{\text{poly}(n)}$-close to $|\psi_n\rangle$.

State complexity classes

Def: a family $\{|\psi_n\rangle\}_{n\in\mathbb{N}}$ of quantum states is space-uniform if $\exists$ a uniform family of circuits $\{C_n\}$ s.t.

- Each C_n uses poly(n) space, exp(n) time
- $C_n |0^{\mathrm{poly}(n)}\rangle = |\psi_n\rangle$.

Def: statePSPACE = class of space-uniform families of quantum states.

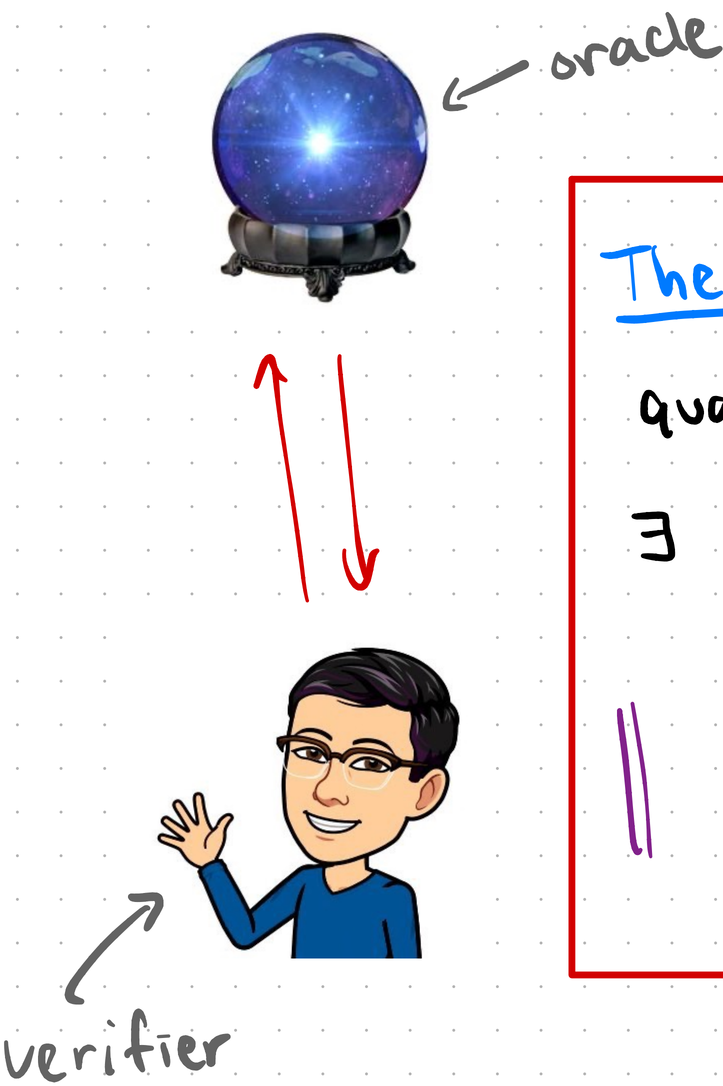
Def: stateQIP = class of state families that admit interactive state synthesis protocols

statePSPACE and stateQIP are state complexity classes. They are classes of state families, rather than languages (i.e. sets of strings).

What does landscape of state complexity theory look like?

How to interactively synthesize a state.

Warmup: interactive state synthesis with a *trusted* prover, i.e., an oracle.



Theorem (Aaronson): $\exists$ poly-size quantum circuit V, $\forall$ n-qubit $|\psi\rangle$ $\exists$ classical oracle A, s.t.

$$\left\| V^A(|0\cdots0\rangle) - |\psi\rangle \right\| \leq \exp(-n).$$

Basic idea: algorithm V builds $|\psi\rangle$ qubit-by-qubit, using classical oracle to compute conditional amplitudes of $|\psi\rangle$ in superposition.

Write

$$|\psi\rangle = \alpha_0 |0\rangle |\psi_0\rangle + \alpha_1 |1\rangle |\psi_1\rangle$$

for complex α_0, α_1 and $|\psi_0\rangle, |\psi_1\rangle$ are $(n-1)$-qubit states.

Then, expand, for $b \in \{0,1\}$,

$$|\psi_b\rangle = \alpha_{b0}|0\rangle|\psi_{b0}\rangle + \alpha_{b1}|1\rangle|\psi_{b1}\rangle$$

for complex α_{b0}, α_{b1} and $(n-2)$-qubit $|\psi_{b0}\rangle, |\psi_{b1}\rangle$.

Continue in this fashion.

The numbers $\{\alpha_y\}$ where $y \in \{0,1\}^{\leq n}$ are conditional amplitudes.

Recursive description of verifier

- verifier asks oracle to compute (α_0, α_1).
- verifier prepares $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
- verifier uncomputes (α_0, α_1).
- controlled on $|b\rangle$, verifier coherently synthesizes $(n-1)$-qubit state $|\psi_b\rangle$ to get

$$\alpha_0 |0\rangle|\psi_0\rangle + \alpha_1 |1\rangle|\psi_1\rangle = |\psi\rangle.$$

---

unrolling the recursion, verifier is using oracle to compute the conditional amplitudes.

Intermediate Result:

Theorem: Let $\Psi = \{|\psi_n\rangle\}$ be state uniform.

Then the conditional amplitudes of $|\psi_n\rangle$ for all n are computable to within $\exp(-\mathrm{poly}(n))$ error in PSPACE.

i.e. $\exists$ poly-space TM M s.t. $\forall n$, $y \in \{0,1\}^{\leq n}$,

$$|M(1^n, y) - \alpha_y| \leq \exp(-\mathrm{poly}(n)).$$

Recursive description of verifier

- verifier asks oracle to compute (α_0, α_1).
- verifier prepares $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
- verifier uncomputes (α_0, α_1).
- controlled on $|b\rangle$, verifier coherently synthesizes $(n-1)$-qubit state $|\psi_b\rangle$ to get

$$\alpha_0 |0\rangle|\psi_0\rangle + \alpha_1 |1\rangle|\psi_1\rangle = |\psi\rangle.$$

If oracle is untrusted, then try to run (Q)IP = PSPACE protocol to verifiably compute (α_0, α_1).

Recursive description of verifier (w/ untrusted prover)

new!

- verifier performs QIP = PSPACE protocol to compute (α_0, α_1). If subprotocol rejects, then reject.
- verifier prepares $\alpha_0 |0\rangle + \alpha_1 |1\rangle$
- verifier uncomputes (α_0, α_1). ← i.e. run QIP=PSPACE in reverse
- Controlled on $|b\rangle$, verifier coherently runs synthesis protocol for $|\psi_b\rangle$ to get

$$\alpha_0 |0\rangle|\psi_0\rangle + \alpha_1 |1\rangle|\psi_1\rangle = |\psi\rangle.$$

If subprotocol rejects, then reject.

Problem: Quantum Attacks

- Soundness of the QIP = PSPACE protocol implies that prover cannot cheat the computation of conditional amplitudes without getting caught.

QIP = PSPACE protocol defends against "classical attacks."

- A malicious prover can undetectably cheat the protocol by mounting "quantum attacks."

Problem: Quantum Attacks

- Entanglement Attacks: during QIP = PSPACE portion of the protocol, prover can entangle its private workspace with the messages. Final state of verifier and prover could be

$$\underbrace{\sum_{x \in \{0,1\}^n} \alpha_x |x\rangle}_{\text{verifier's workspace}} \otimes \underbrace{|\phi_x\rangle}_{\text{prover's workspace}}$$

instead of $|\psi\rangle = \sum \alpha_x |x\rangle$.

Problem: Quantum Attacks

- Phase Attack (a more subtle version of the entanglement attack): prover can undetectably add spurious phases while keeping the synthesized state pure:

$$\sum_x \underbrace{e^{i\theta_x}} \alpha_x |x\rangle$$

↑ spurious phase introduced by prover.

Solution: Quantum tests.

Our state synthesis protocol

Invariant: assume have $\underbrace{|\psi^{(j)}\rangle}_{\text{register } A} \otimes \underbrace{|\psi^{(j)}\rangle}_{\text{register } B}$

$|\psi^{(j)}\rangle$ = j-qubit "in progress" state

- controlled on $|y\rangle$ of register A, run $QIP = PSPACE$ to compute conditional amplitudes $(\alpha_{y0}, \alpha_{y1})$.
- Flip coin $b \in_R \{\text{GROW}, \text{TEST}\}$.
- If $b =$ GROW, then controlled on $|y\rangle_A$, prepare

$$\alpha_{y0}|0\rangle + \alpha_{y1}|1\rangle$$

- Reverse $QIP = PSPACE$ protocol.

- If b = TEST
  - perform SWAP test between registers A, B.
    (check prover didn't do anything fishy in QIP = PSPACE, and reverse steps).
- If b = GROW
  - exchange $|\psi^{(j)}\rangle$ in register B with $|\psi^{(j+1)}\rangle$ provided by prover.
  - perform SWAP test between registers A.B
    (check prover did provide $|\psi^{(j+1)}\rangle$)
- repeat until all n-qubits constructed.

Open Problems

1. stateQIP $\overset{?}{\subseteq}$ statePSPACE

2. improve soundness guarantees of our protocol?

   We prove that if $\Pr[\text{verifier acc.}] \geq \exp(-n)$, then output state (cond. on acc) is $\frac{1}{\text{poly}(n)}$-close to ideal.

   Can we improve $\frac{1}{\text{poly}(n)}$ to $\frac{1}{\exp(n)}$?

3. What are crypto applications of interactive state synthesis?

4. Is there an interesting and achievable notion of zero-knowledge state synthesis?

5. What kinds of states can we construct with <u>multiple provers</u>?

$$\ldots \overset{?}{\subseteq} \text{stateQMIP} \overset{?}{\subseteq} \cdots$$

6. More generally, what does quantum state complexity theory look like?

Summary

- Defined a model of interactive state synthesis, where verifier can use help of untrusted prover to construct complex quantum states.

- <u>Main result:</u> statePSPACE $\subseteq$ stateQIP

- Many open problems and new questions to ask

- Didn't get to in this talk: interactive unitary synthesis!

Interactive Unitary Synthesis

- Motivating task: suppose you are now given a succinct description of n-qubit, exp(n)-time circuit C, and an input state $|\phi\rangle$ in quantum form.

Goal: synthesize $|\psi\rangle = C|\phi\rangle$ (unitary synthesis task)

- Even harder task because you don't even have an implicit classical description of the output state!

- Again, should not be solvable in polynomial time.
- What if you can enlist help of prover?
- Can define a model of interactive unitary synthesis and associated unitary complexity class

  unitary QIP

- Open question: Unitary PSPACE $\overset{?}{\subseteq}$ unitary QIP
- (another) main result: space-uniform unitary families with polynomial action admit unitary QIP protocols.

- **Def:** A family of unitaries $\{U_n\}$ where U_n acts on n-qubits has polynomial action if U_n only acts nontrivially on a subspace of dimension $\text{poly}(n)$.

Ex: Let $\{|\psi_n\rangle\}$ be space-uniform. Then $\{U_n\}$ is space-uniform and has polynomial action where $U_n = I - 2|\psi_n\rangle\langle\psi_n|$.

- our result about unitary QIP uses our result about state QIP as a subprotocol.