

# Interactive Proofs for Synthesizing Quantum States and Unitaries

Gregory Rosenthal   

Department of Computer Science, University of Toronto, Canada

Henry Yuen   

Department of Computer Science, Columbia University, New York, NY, USA

---

## Abstract

Whereas quantum complexity theory has traditionally been concerned with problems arising from *classical* complexity theory (such as computing boolean functions), it also makes sense to study the complexity of inherently *quantum* operations such as constructing quantum states or performing unitary transformations. With this motivation, we define models of *interactive proofs* for synthesizing quantum states and unitaries, where a polynomial-time quantum verifier interacts with an untrusted quantum prover, and a verifier who accepts also outputs an approximation of the target state (for the state synthesis problem) or the result of the target unitary applied to the input state (for the unitary synthesis problem); furthermore there should exist an “honest” prover which the verifier accepts with probability 1.

Our main result is a “state synthesis” analogue of the inclusion  $\text{PSPACE} \subseteq \text{IP}$ : any sequence of states computable by a polynomial-space quantum algorithm (which may run for exponential time) admits an interactive protocol of the form described above. Leveraging this state synthesis protocol, we also give a unitary synthesis protocol for polynomial space-computable unitaries that act nontrivially on only a polynomial-dimensional subspace. We obtain analogous results in the setting with multiple entangled provers as well.

**2012 ACM Subject Classification** Theory of computation  $\rightarrow$  Interactive proof systems; Theory of computation  $\rightarrow$  Quantum complexity theory; Theory of computation  $\rightarrow$  Quantum complexity theory

**Keywords and phrases** interactive proofs, quantum state complexity, quantum unitary complexity

**Digital Object Identifier** 10.4230/LIPIcs.ITCS.2022.112

**Related Version** *Full Version:* <https://arxiv.org/abs/2108.07192>

**Funding** *Gregory Rosenthal:* NSERC (PGS D).

*Henry Yuen:* Supported by an NSERC Discovery Grant, a Google Research Award, and AFOSR award FA9550-21-1-0040.

## 1 Abridged Introduction

In quantum computing and quantum information processing, there are tasks that are “inherently quantum”, meaning that it does not even make sense for a classical computer to perform them. Such tasks include:

- *State synthesis:* given an implicit description of a quantum state, construct the state.
- *State transformations:* given an implicit description of a quantum operation (e.g. a unitary), perform it on a given input state.

Many quantum protocols and algorithms are most naturally viewed as synthesizing a state, performing a state transformation, or both. For example, primitives in quantum cryptography such as quantum money [1] or quantum pseudorandom states [7] revolve around constructing highly entangled, difficult-to-clone states. The class of algorithms known as variational quantum eigensolvers are meant to prepare ground states of physical systems [4]. A decoder for a quantum error-correcting code transforms noise-corrupted states into noise-free states [9].



© Gregory Rosenthal and Henry Yuen;

licensed under Creative Commons License CC-BY 4.0

13th Innovations in Theoretical Computer Science Conference (ITCS 2022).

Editor: Mark Braverman; Article No. 112; pp. 112:1–112:4

Leibniz International Proceedings in Informatics



LIPICs Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

This motivates the study of the complexity of state synthesis and state transformations. The central question is the following: how difficult is it to prepare a given state or perform a given unitary transformation? Unlike how search and decision problems can often be reduced to each other in classical computer science, such “inherently quantum” tasks cannot obviously be reduced to analogous classical decision or search problems. For example, it is unknown whether the ability to decide the local Hamiltonian problem in polynomial time implies the ability to efficiently *construct* ground states of local Hamiltonians on a quantum computer.<sup>1</sup>

We investigate *interactive proofs for synthesizing states and unitaries*. In traditional models of interactive proofs (even the ones associated with quantum complexity classes such as QIP and MIP\*), the goal of the verifier is to solve a decision problem with the help of an all-powerful prover. We propose a model of “inherently quantum” interactive proofs where the verifier’s goal is to synthesize a quantum state or perform a quantum operation. The challenge is for the verifier to use the help of an untrusted prover to perform these tasks in a *verifiable* way. We first discuss interactive state synthesis, and then discuss interactive unitary synthesis.

## 1.1 Interactive state synthesis

We prove the following, which (as we will soon discuss) can be seen as an analogue of the inclusion  $\text{PSPACE} \subseteq \text{IP}$  for state synthesis:

► **Theorem 1.** *Let  $(|\psi_n\rangle)_{n \in \mathbb{N}}$  denote a family of quantum states, where  $|\psi_n\rangle$  is on  $n$  qubits, such that there exists a polynomial-space quantum algorithm<sup>2</sup> that on input  $1^n$  outputs  $|\psi_n\rangle$ . Then there exists an interactive protocol between a polynomial-time quantum verifier and an untrusted quantum prover that, on input  $1^n$ , constructs an approximation of  $|\psi_n\rangle$ . More precisely, the protocol has the following guarantees: for all  $n \in \mathbb{N}$ , when the verifier receives input  $1^n$ ,*

- (Completeness) *There exists an “honest” prover that is accepted by the verifier with probability 1, and for which the verifier outputs a density matrix that is exponentially close to  $|\psi_n\rangle\langle\psi_n|$ .*
- (Soundness) *For all prover strategies, the probability that the verifier accepts and outputs a density matrix that is not even polynomially close to  $|\psi_n\rangle\langle\psi_n|$  is exponentially small.*

For comparison, the celebrated result  $\text{IP} = \text{PSPACE}$  [10, 11] shows that a polynomial-time *classical* verifier can verify membership in any PSPACE language by interacting with an all-powerful but untrusted prover. The  $\text{IP} = \text{PSPACE}$  protocol can straightforwardly be extended to solve *function* problems, where the goal is to produce the first  $n$  (or more generally  $\text{poly}(n)$ ) bits of the output of a polynomial-space Turing machine on an input of length  $n$ . In our state synthesis problem, the goal is not just to produce a string  $s$  on  $n$  bits but an entire *quantum state* on  $n$  qubits.

This goal raises a number of challenges: first, the verifier has to somehow obtain information about exponentially many amplitudes in polynomial time. Second, the verifier has to also check that the prover has not maliciously entangled itself with the  $n$  target qubits at the end of the interaction; for example, if we write the target state as  $\sum_x \alpha_x |x\rangle$ , then the verifier should ensure that it doesn’t have the first  $n$  qubits of the entangled state  $\sum_x \alpha_x |x\rangle |\phi_x\rangle$  where the states  $\{|\phi_x\rangle\}$  are in the possession of the prover.

<sup>1</sup> In fact there is some evidence in the form of an oracle separation that efficient search-to-decision reductions for QMA do not exist [5].

<sup>2</sup> See the introduction of the full paper for a more precise description of what we mean by this.

We note that Theorem 1 is *not* implied by the result  $\text{QIP} = \text{PSPACE}$  [6]. This is because QIP, though defined in terms of quantum verifiers, is still a class of decision problems, and the result does not say anything about the complexity of performing state synthesis. We do, however, use the  $\text{QIP} = \text{PSPACE}$  protocol as a subroutine in our state synthesis protocol.

We also prove a partial converse to Theorem 1, which is analogous to the inclusion  $\text{IP} \subseteq \text{EXP}$ . The uniformity condition makes this converse nontrivial: while *every* quantum state on  $n$  qubits has a  $\exp(\text{poly}(n))$ -size circuit that synthesizes it, it is not necessarily the case that for an arbitrary state family  $(|\psi_n\rangle)_n$  there is a single Turing machine that specifies *all* of the exponential size circuits synthesizing each  $|\psi_n\rangle$ . We also prove an analogue of Theorem 1 with multiple entangled provers, using  $\text{MIP}^* = \text{RE}$  [8].

## 1.2 Interactive unitary synthesis

We prove the following, which can be seen as an analogue of the inclusion  $\text{PSPACE} \subseteq \text{IP}$  for *unitary* synthesis, but only in the special case where each unitary has what we call “polynomial action”; an  $n$ -qubit unitary has polynomial action if it acts nontrivially on a subspace of dimension  $\text{poly}(n)$ .

► **Theorem 2.** *Let  $(C_n)_{n \in \mathbb{N}}$  denote a family of unitaries in “unitary PSPACE” with polynomial action, where  $C_n$  acts on  $n$  qubits. Then there exists an interactive protocol between a polynomial-time quantum verifier and an untrusted quantum prover that, given input an  $n$ -qubit state  $|\phi\rangle$ , constructs an approximation of  $C_n|\phi\rangle$ , with completeness and soundness guarantees analogous to those in Theorem 1.<sup>3</sup>*

A difference between this problem and the state synthesis problem presented in Section 1.1 is that in the latter problem, the input  $C$  provides an implicit classical description of the target state  $|\psi\rangle = C|0^n\rangle$ . In the unitary synthesis problem, however, the input  $|\phi\rangle$  to the circuit  $C$  is provided *in quantum form*. Even if an algorithm were given unlimited time, it would not in general be able to compute a classical description of  $C|\phi\rangle$ ; this is because only one copy of the state  $|\phi\rangle$  is provided. Furthermore, it is not even known how to efficiently perform unitary synthesis with a *trusted* oracle [3], whereas it is known how to efficiently perform state synthesis with a *trusted* oracle [2]. For these reasons, the unitary synthesis problem appears more challenging than the state synthesis problem.

Interesting families of unitaries  $(C_n)_{n \in \mathbb{N}}$  that have polynomial action include *reflections*  $C_n = I - 2|\theta_n\rangle\langle\theta_n|$  where  $(|\theta_n\rangle)_n$  is some family of states. These unitaries act nontrivially on a one-dimensional subspace (namely, the space spanned by  $|\theta_n\rangle$ ). Since the states  $(|\theta_n\rangle)_n$  might be extremely complicated (requiring exponential time to synthesize without the help of a prover, for example), applying the unitaries  $(C_n)_n$  can still be quite nontrivial.

We also show how to generalize Theorem 2 beyond polynomial-action unitary families, provided that the verifier also receives a succinct description of a polynomial-dimensional subspace which is promised to contain the input state  $|\phi\rangle$ .

---

### References

- 1 Scott Aaronson. Quantum copy-protection and quantum money. In *CCC*, pages 229–242, 2009. doi:10.1109/CCC.2009.42.

---

<sup>3</sup> However, here the honest prover can only get the verifier to output a polynomially good approximation of the desired output state, rather than an exponentially good approximation.

- 2 Scott Aaronson. The complexity of quantum states and transformations: from quantum money to black holes, 2016. [arXiv:1607.05256](https://arxiv.org/abs/1607.05256).
- 3 Scott Aaronson. Open problems related to quantum query complexity, 2021. URL: <https://www.scottaaronson.com/papers/open.pdf>.
- 4 Marco Cerezo, Andrew Arrasmith, Ryan Babbush, Simon C. Benjamin, Suguru Endo, Keisuke Fujii, Jarrod R. McClean, Kosuke Mitarai, Xiao Yuan, Lukasz Cincio, and Patrick J. Coles. Variational quantum algorithms, 2020. [arXiv:2012.09265](https://arxiv.org/abs/2012.09265).
- 5 Sandy Irani, Anand Natarajan, Chinmay Nirkhe, Sujit Rao, and Henry Yuen. Quantum search-to-decision reductions and the state synthesis problem, 2021. [arXiv:2111.02999](https://arxiv.org/abs/2111.02999).
- 6 Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. QIP = PSPACE. *J. ACM*, 58(6):1–27, 2011. doi:10.1145/2049697.2049704.
- 7 Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In *CRYPTO*, pages 126–152, 2018. doi:10.1007/978-3-319-96878-0\_5.
- 8 Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP\* = RE, 2020. [arXiv:2001.04383](https://arxiv.org/abs/2001.04383).
- 9 Daniel A. Lidar and Todd A. Brun. *Quantum Error Correction*. Cambridge University Press, 2013. URL: [www.cambridge.org/9780521897877](http://www.cambridge.org/9780521897877).
- 10 Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *J. ACM*, 39(4):859–868, 1992. doi:10.1145/146585.146605.
- 11 Adi Shamir. IP = PSPACE. *J. ACM*, 39(4):869–877, 1992. doi:10.1145/146585.146609.