Quantum Information and Computation, Vol. 24, No. 9&10 (2024) 754–765
© Rinton Press

QUANTUM STATE SYNTHESIS: RELATION WITH DECISION COMPLEXITY CLASSES AND IMPOSSIBILITY OF SYNTHESIS ERROR REDUCTION

HUGO DELAVENNE
Institut Polytechnique de Paris, Ecole Polytechnique, LIX
INRIA
1 rue Honor d'Estienne d'Orves, 91120 Palaiseau, France

FRANOIS LE GALL
Graduate School of Mathematics, Nagoya University
Furocho, Chikusaku, Nagoya Aichi 464-8602, Japan

Received May 20, 2024
Revised August 29, 2024

This work investigates the relationships between quantum state synthesis complexity classes (a recent concept in computational complexity that focuses on the complexity of preparing quantum states) and traditional decision complexity classes. We especially investigate the role of the *synthesis error parameter*, which characterizes the quality of the synthesis in quantum state synthesis complexity classes. We first show that in the high synthesis error regime, collapse of synthesis classes implies collapse of the equivalent decision classes. For more reasonable synthesis error, we then show a similar relationships for BQP and QCMA. Finally, we show that for quantum state synthesis classes it is in general impossible to improve the quality of the synthesis: unlike the completeness and soundness parameters (which can be improved via repetition), the synthesis error cannot be reduced, even with arbitrary computational power.

Keywords: quantum state synthesis, decision complexity classes, error reduction

1 Introduction

While quantum complexity theory traditionally investigates the complexity of decision problems (i.e., Boolean functions), a recent line of research [1, 2, 4, 9, 8, 10] started investigating the complexity of constructing quantum states, a task called *quantum state synthesis*. Those prior works showed that the behavior of quantum state synthesis complexity classes is often similar to the behavior of decision complexity classes: the equality $\mathsf{PSPACE} = \mathsf{QIP}$ [5] has its state synthesis equivalent $\mathsf{statePSPACE} = \mathsf{stateQIP}$ [10, 8], the equality $\mathsf{QCMA} = \mathsf{QCMA}[1, \frac{1}{2}]$ [6] has the equivalent $\mathsf{stateQCMA} = \mathsf{stateQCMA}[1, \frac{1}{2}]$ [4], and the equality $\mathsf{QIP} = \mathsf{QIP}(O(1))$ [11] has the equivalent $\mathsf{stateQIP} = \mathsf{stateQIP}(O(1))$ [9].

In order to further investigate the relationships between quantum state synthesis complexity classes and decision complexity classes, in this paper we introduce a new definition of quantum state synthesis complexity classes in which we allow an arbitrary number of target states per input (prior definitions required exactly one target state per input). Our definition is closer to the definition of classical functional classes like FP or FNP introduced in [7] and thus more closely related to Boolean classes and languages. We stress that this new definition is a generalization of the definitions of prior works: we recover the previous definitions as a special case by requiring one target state per input.

Based on this new definition, we further explore the relationship between quantum state synthesis complexity classes and decision complexity classes. Here are our main contributions:

(1) We investigate the relationship between the class BQP and the corresponding quantum state synthesis complexity class denoted $\mathsf{relationalStateBQP}_\delta$. Here $\delta \in [0,1]$ is a parameter called the *synthesis error parameter* that characterizes the imprecision of the synthesis (the goal is to have δ as small as possible). Theorem 1 shows that if we take δ very close to 1, i.e., if we allow exponentially small fidelity between the ouput and the state we want to synthesize, there exists a tight relationship between BQP and $\mathsf{relationalStateBQP}_\delta$. This relationship remains true for other complexity classes (e.g., QMA and $\mathsf{relationalStateQMA}_\delta$, or QCMA and $\mathsf{relationalStateQCMA}_\delta$).

(2) This above result yields the question of proving relationships between quantum state synthesis complexity classes and decision complexity classes for more reasonable values of the parameter δ. We make a first step in this direction. We especially investigate how proving separations for quantum state synthesis classes relates to proving separations for decision complexity classes. We first observe that $\mathsf{BQP} \neq \mathsf{QMA}$ implies $\mathsf{relationalStateQMA}_\delta \not\subseteq \mathsf{relationalStateBQP}_\delta$ for all δ (Proposition 3) and $\mathsf{BQP} \neq \mathsf{QCMA}$ implies $\mathsf{relationalStateQCMA}_\delta \not\subseteq \mathsf{relationalStateBQP}_\delta$ for all δ (Proposition 4). Our main contribution (in Theorem 2) proves the converse for the case of QCMA (with a small loss in δ): if there exist δ and a polynomial q such that $\mathsf{relationalStateQCMA}_\delta \not\subseteq \mathsf{relationalStateBQP}_{\delta+1/q}$, then $\mathsf{BQP} \neq \mathsf{QCMA}$. These results suggest that progress on understanding decision complexity classes can be done by investigating quantum state synthesis classes.

(3) We finally investigate whether the synthesis error parameter δ can be reduced, i.e., whether the quality of the synthesis can be increased, just like completeness and soundness can be improved via repetition. We show that for quantum state synthesis classes this is in general impossible: we prove (see Corollary 1) that $\mathsf{relationalStateBQP}_\delta \not\subset \mathsf{relationalStateBQP}_{\delta-\epsilon}$ holds for any $\epsilon > 0$. We actually prove in Theorem 3 that reducing δ is impossible even if we allow arbitrary computational power. This result holds for the definitions used in prior works as well and shows the importance of the parameter δ when defining state synthesis complexity classes. This result is closely related to the impossibility of error reduction for unitary synthesis problems of [2, Proposition 3.8], but it is stronger in the sense that there is no gap between the source and target errors.

2 Definition of relational state synthesis complexity classes

We first recall the definition of classical functional classes [7]. In this work, we always use the binary alphabet $\Sigma = \{0,1\}$.

Definition 1 (FP, FNP, TFNP) *A relation $R \subseteq \Sigma^* \times \Sigma^*$ is in FP iff there exists a polynomial-time Turing machine M such that if there exists $y \in \Sigma^*$ such that $(x,y) \in R$ then $M(x)$ outputs such a y, and otherwise $M(x)$ rejects.*

A relation $R \subseteq \Sigma^* \times \Sigma^*$ is in FNP *iff there exists a polynomial-time Turing machine M such that if there exists $y \in \Sigma^*$ such that $(x, y) \in R$ then there exists $w \in \Sigma^*$ such that $M(x, w)$ outputs such a y, and otherwise, for any $w \in \Sigma^*$, $M(x, w)$ rejects.*

A relation $R \in \mathsf{FNP}$ is in TFNP *iff $\forall x \in \Sigma^*, \exists y \in \Sigma^*, (x, y) \in R$.*

The relations for state synthesis are a bit more complex since we have to specify the output space for every input size.

Definition 2 (State synthesis relation) *For $n \in \mathbb{N}$, let $\mathcal{H}_n$ be a Hilbert space and $\mathcal{O}_n$ be the set of density matrices over $\mathcal{H}_n$. A* state synthesis relation *is a triple $(R, L^{\text{yes}}, L^{\text{no}})$ where $(L^{\text{yes}}, L^{\text{no}})$ is a promise language and*

$$R = \{(x, \rho) \mid x \in L^{\text{yes}}, \rho \in S_x\}$$

for non-empty subsets $S_x \subseteq \mathcal{O}_{|x|}$. We often omit the language. We simply use R to denote the state synthesis relation, we write $L_R^{\text{yes}} = L^{\text{yes}}$, $L_R^{\text{no}} = L^{\text{no}}$ and $L_R = L^{\text{yes}} \cup L^{\text{no}}$ and define

$$xR := \{\rho \in \mathcal{O}_{|x|} \mid (x, \rho) \in R\}$$

for any $x \in L_R$ (note that $xR \notin \emptyset$ for any $x \in L_R^{\text{yes}}$ and $xR = \emptyset$ for any $x \in L_R^{\text{no}}$). We also define a function $k_R : \mathbb{N} \to \mathbb{N}$ that gives the number of qubits of $\mathcal{H}_n$.

The quantum circuits considered in this paper are bounded in size and uniform. We give formal definition of these notions.

Definition 3 (Polynomial-size family of circuits) *A family of quantum circuits $(C_n)_{n\in\mathbb{N}}$ is said to be polynomial-size if there exists a polynomial p such that for any $n \in \mathbb{N}$, C_n contains at most $p(n)$ gates.*

Definition 4 (Uniform family of circuits) *A family of quantum circuits $(C_n)_{n\in\mathbb{N}}$ is said to be polynomial-time-uniform, or simply uniform, if there exists a Turing machine M working in polynomial-time such that for any $n \in \mathbb{N}$, $M(n)$ outputs a description of C_n.*

Due to the continuity of the space of quantum states, we need a measure and a threshold to quantify the tolerated error on the state synthesis. We use the trace distance between density matrices, and extend it to a distance between a density matrix and a set of density matrices.

Definition 5 (Trace distance) *Let ρ and σ be two density matrices on the same space. Define*

$$\operatorname{td}(\rho, \sigma) := \frac{1}{2}\operatorname{Tr}\left(\sqrt{(\rho - \sigma)^\dagger(\rho - \sigma)}\right).$$

For a density matrix ρ and a set S of density matrices over the same space, define

$$\operatorname{td}(\rho, S) := \min_{\sigma\in S} \operatorname{td}(\rho, \sigma).$$

In this work we consider families of circuits C_n taking some classical input x and possibly some other input ψ (for a witness). We denote by $C_x(\psi)$ the circuit $C_{|x|}(x\psi)$. The circuit has a specific qubit that is measured at the end of the computation. The measurement outcome is called the acceptance bit and denoted by $C_x^{\text{acc}}(\psi)$. When there is an output channel, we denote by $C_x^{\text{out}}(\psi)$ the quantum state outputted on this channel. Note that this state depends on the value of the acceptance bit. We denote by $C_x^{\text{out}|\text{acc}}(\psi)$ the quantum state outputted on this channel when $C_x^{\mathrm{acc}}(\psi) = 1$. When there is no witness we remove ψ from all these notations, e.g., we use write the acceptance bit simply as C_x^{acc}.

We are now ready to introduce relational state synthesis complexity classes.

Definition 6 ($\mathsf{relationalStateBQP}$) *Let $c, s, \delta \colon \mathbb{N} \to [0,1]$ be completeness, soundness and synthesis error functions. A state synthesis relation R is in $\mathsf{relationalStateBQP}_\delta[c,s]$ if there exists a uniform family of polynomial-size quantum circuits $(C_n)_{n\in\mathbb{N}}$ such that for $x \in L_R$:*

- *completeness: if $xR \neq \emptyset$ then $\Pr\left(C_x^{\mathrm{acc}} = 1\right) \geq c(|x|)$ and $\mathrm{td}(C_x^{\mathrm{out}|\mathrm{acc}}, xR) \leq \delta(k_R(|x|))$.*
- *soundness: if $xR = \emptyset$ then $\Pr\left(C_x^{\mathrm{acc}} = 1\right) \leq s(|x|)$.*

Definition 7 ($\mathsf{relationalStateQMA}$) *Let $c, s, \delta \colon \mathbb{N} \to [0,1]$ be functions. A state synthesis relation R is in $\mathsf{relationalStateQMA}_\delta[c,s]$ if there exists a uniform family of polynomial-size quantum circuits $(C_n)_{n\in\mathbb{N}}$ such that for $x \in L_R$:*

- *completeness: if $xR \neq \emptyset$ then there exists a quantum witness ψ such that $\Pr\left(C_x^{\mathrm{acc}}(\psi) = 1\right) \geq c(|x|)$.*
- *soundness: for any ψ, if both $xR \neq \emptyset$ and $\mathrm{td}(C_x^{\mathrm{out}|\mathrm{acc}}(\psi), xR) > \delta(k_R(|x|))$ hold then $\Pr\left(C_x^{\mathrm{acc}}(\psi) = 1\right) \leq s(|x|)$; and if $xR = \emptyset$ then $\Pr\left(C_x^{\mathrm{acc}}(\psi) = 1\right) \leq s(|x|)$.*

The definitions used in the previous papers [10, 8, 9, 2, 4] do not involve relations since exactly one output is expected per input. We rephrase the definition of $\mathsf{stateBQP}$ and $\mathsf{stateQMA}$ from [4] by using our definitions of $\mathsf{relationalStateBQP}$ and $\mathsf{relationalStateQMA}$.

Definition 8 ($\mathsf{stateBQP}$, $\mathsf{stateQMA}$) *For any $c, s, \delta \colon \mathbb{N} \to [0,1]$,* $\mathsf{stateBQP}_\delta[c] = \{R \in \mathsf{relationalStateBQP}_\delta[c,0]$
$\forall x \in L_R, |xR| = 1\}$,
$\mathsf{stateQMA}_\delta[c,s] = \{R \in \mathsf{relationalStateQMA}_\delta[c,s] \mid \forall x \in L_R, |xR| = 1\}$.

We define the class $\mathsf{relationalStateQCMA}$ similarly to $\mathsf{relationalStateQMA}$ but with a restriction to witnesses being states in the computational basis (i.e., classical strings). We also define a class $\mathsf{relationalStateR}$ corresponding to states synthesized by arbitrary (uniform) quantum circuits (this class can be seen as the equivalent of the class R of recursive languages in decision complexity theory):

Definition 9 ($\mathsf{relationalStateR}$) *Let $c, s, \delta \colon \mathbb{N} \to [0,1]$ be completeness, soundness and synthesis error functions. A state synthesis relation R is in $\mathsf{relationalStateR}_\delta[c,s]$ if there exists an unboundedly powerful Turing machine such that for any $n \in \mathbb{N}$, $M(1^n)$ halts and outputs the description of a quantum circuit C_n such that for $x \in L_R$:*

- *completeness: if $xR \neq \emptyset$ then $\Pr\left(C_x^{\mathrm{acc}} = 1\right) \geq c(|x|)$ and $\mathrm{td}(C_x^{\mathrm{out}|\mathrm{acc}}, xR) \leq \delta(k_R(|x|))$.*
- *soundness: if $xR = \emptyset$ then $\Pr\left(C_x^{\mathrm{acc}} = 1\right) \leq s(|x|)$.*

Finally, we show that the gap between the completeness and the soundness can be amplified for these classes. For $\mathsf{relationalStateBQP}$, $\mathsf{relationalStateQCMA}$ and $\mathsf{relationalStateQMA}$, the proof of gap amplification of [4] applies directly since it amplifies the completeness and soundness while preserving the target state:

Proposition 1 (Gap amplification) *Let $0 \leq c(n), s(n), \delta(n) \leq 1$ be poly-time computable functions such that $c(n) - s(n) \geq 1/\mathrm{poly}(n)$. For any polynomial p,* $\mathsf{relationalStateBQP}_\delta[c,s] \subseteq \mathsf{relationalStateBQP}_\delta[1-2^{-p}, 2^{-p}]$
$\mathsf{relationalStateQCMA}_\delta[c,s] \subseteq \mathsf{relationalStateQCMA}_\delta[1-2^{-p}, 2^{-p}]$
$\mathsf{relationalStateQMA}_\delta[c,s] \subseteq \mathsf{relationalStateQMA}_\delta[1-2^{-p}, 2^{-p}]$.

Since we have an amplification for completeness and soundness, having completeness $2/3$ and soundness $1/3$ is equivalent to having completeness $c(n)$ and soundness $s(n)$ with $c(n) - s(n) \geq 1/\mathrm{poly}(n)$. We thus define $\mathsf{relationalStateBQP}_\delta = \mathsf{relationalStateBQP}_\delta[2/3, 1/3]$, $\mathsf{relationalStateQCMA}_\delta = \mathsf{relationalStateQCMA}_\delta[2/3, 1/3]$, $\mathsf{relationalStateQMA}_\delta = \mathsf{relationalStateQMA}_\delta[2/3, 1/3]$.

A gap amplification result for the class $\mathsf{relationalStateR}$ is also easy to show:

Proposition 2 (Gap amplification) *Let $0 \leq c(n), s(n), \delta(n) \leq 1$ be computable functions such that $c(n) > s(n)$. For any computable function $\gamma(n) > 0$,*

$$\mathsf{relationalStateR}_\delta[c,s] \subseteq \mathsf{relationalStateR}_\delta[1-\gamma, \gamma].$$

Proof. The amplification is very similar to the standard amplification for decision circuits by repetition: We repeatedly apply the synthesis circuit until we get $C_x^{\mathrm{acc}} = 1$. As soon at this happens, we stop and output the output state of the last repetition. If we do not get $C_x^{\mathrm{acc}} = 1$ after a specified number of interactions (depending on c, s and γ), we decide that $xR = \emptyset$ (note that there is no need to output a quantum state in this case). □

3 High synthesis error regime

State synthesis classes defined in Section 2 are closely related to decision languages. In Theorem 1 below we show a basic relationship between these two notions when the synthesis error is close to 1. While for concreteness we focus on the relationship between the classes BQP and $\mathsf{relationalStateBQP}_\delta$, the results proved in this section remains true for other complexity classes (e.g., QMA and $\mathsf{relationalStateQMA}_\delta$, QCMA and $\mathsf{relationalStateQCMA}_\delta$, or QIP and $\mathsf{relationalStateQIP}_\delta$) as well.

We start with the following lemma, which holds for any δ.

Lemma 1 *For any $\delta : \mathbb{N} \to [0,1]$ and any state synthesis relation R, if $R \in \mathsf{relationalStateBQP}_\delta$ then $L_R \in \mathsf{BQP}$.*

Proof. Take $R \in \mathsf{relationalStateBQP}_\delta$. Let $(C_n)_{n\in\mathbb{N}}$ denote the family of circuits from Definition 6. By ignoring the output state of the circuits and considering only their acceptance qubit, they become decision circuits that have acceptance probability $\Pr(C_x^{\mathrm{acc}} = 1)$. If $x \in L_R^{\mathrm{yes}}$ then $\Pr(C_x^{\mathrm{acc}} = 1) \geq 2/3$ by completeness as a state synthesis circuit. If $x \in L_R^{\mathrm{no}}$, which means that $xR = \emptyset$, then $\Pr(C_x^{\mathrm{acc}} = 1) \leq 1/3$ by soundness as a state synthesis circuit. Thus $L_R \in \mathsf{BQP}$. □

Next, we show a tight relationship between quantum state synthesis classes and decision complexity classes when $\delta = 1 - 2^{-n}$, i.e., when we allow exponentially small fidelity between the output and the state we want to synthesize. The idea is to generate the same maximally mixed state on any input.

Theorem 1 *Consider the function $\delta_0 \colon n \mapsto 1 - 2^{-n}$. Then for any state synthesis relation R, $R \in \mathsf{relationalStateBQP}_{\delta_0}$ iff $L_R \in \mathsf{BQP}$.*

Proof. From Lemma 1 we immediately get that $R \in \mathsf{relationalStateBQP}_{\delta_0}$ implies $L_R \in \mathsf{BQP}$.

Now suppose that $L_R \in \mathsf{BQP}$ and let $(C_n)_{n\in\mathbb{N}}$ be a uniform family of circuits recognizing L_R with completeness $2/3$ and soundness $1/3$. A maximally mixed state ρ_n on $k_R(n)$ qubits can be synthesized by a uniform family of polynomial-size circuits because $k_R \in \text{poly}$. Since ρ_n is at distance at most $1 - 2^{-k_R(n)}$ from any other density matrix, the circuit C'_n that outputs $C'^{\text{acc}}_n = C^{\text{acc}}_n$ and $C'^{\text{out}}_n = \rho_n$ synthesizes R with completeness $2/3$, soundness $1/3$ and error δ_0. Thus $R \in \mathsf{relationalStateBQP}_{\delta_0}$. □

4 Relationship between decision and state synthesis classes

In this section we investigate the relationship between proving separations for quantum state synthesis classes and proving separations for decision complexity classes. The results of this section hold for any value of the synthesis error parameter δ. Our main result is Theorem 2, which shows that a separation for quantum state synthesis classes can be used to prove a separation for decision complexity classes.

First, as a consequence of Lemma 1, we show the following result:

Proposition 3 *If* $\mathsf{BQP} \neq \mathsf{QMA}$ *then*

$$\mathsf{relationalStateQMA}_{\delta} \not\subseteq \mathsf{relationalStateBQP}_{\delta'}$$

holds for any $\delta, \delta' \in [0,1]$.

Proof. Suppose that there exist δ, δ' such that the inclusion $\mathsf{relationalStateQMA}_{\delta} \subseteq \mathsf{relationalStateBQP}_{\delta'}$ holds. For $L = (L^{\text{yes}}, L^{\text{no}}) \in \mathsf{QMA}$, there exists a family of circuits $(C_n)_{n\in\mathbb{N}}$ that takes a quantum witness and recognizes L with completeness $2/3$ and soundness $1/3$. For each $n \in \mathbb{N}$ we can build a circuit C'_n that introduces a 1-qubit output channel and "copies" the contents of the acceptance qubit to the output channel using a CNOT gate:

[2,nwires=2,bundle=1]C$_n$[$wires = 3, steps = 3, style =$
$innersep = 2mm, dashed, linewidth = 0.2mm, roundedcorners]circuitC'_n$ [alternate]
[alternate] [alternate]
1 acc
0 out

Define the relation R by $xR = \{\mathbb{1}\}$ if $x \in L^{\text{yes}}$ and $xR = \emptyset$ if $x \in L^{\text{no}}$. Since $(C'_n)_{n\in\mathbb{N}}$ synthesizes R, we get

$$R \in \mathsf{relationalStateQMA}_0 \subseteq \mathsf{relationalStateQMA}_{\delta} \subseteq \mathsf{relationalStateBQP}_{\delta'}.$$

By Lemma 1, we get $L \in \mathsf{BQP}$ and thus $\mathsf{QMA} \subseteq \mathsf{BQP}$. □

By replacing the quantum witness by a classical witness in Proposition 3 we similarly obtain the following result:

Proposition 4 *If* $\mathsf{BQP} \neq \mathsf{QCMA}$ *then*

$$\mathsf{relationalStateQCMA}_{\delta} \not\subseteq \mathsf{relationalStateBQP}_{\delta'}.$$

holds for any $\delta, \delta' \in [0,1]$.

Now using a technique similar to the proof that $\mathsf{P} = \mathsf{NP}$ iff $\mathsf{FP} = \mathsf{FNP}$ [3] we are able to show the following converse statement, which is the main result of this section.

Theorem 2 *If there exist some $\delta \in [0,1]$ and some polynomial q such that*

$$\mathsf{relationalStateQCMA}_\delta \not\subseteq \mathsf{relationalStateBQP}_{\delta+1/q},$$

then $\mathsf{BQP} \neq \mathsf{QCMA}$.

The proof of Theorem 2 will show the contrapositive: we will show that $\mathsf{BQP} = \mathsf{QCMA}$ implies that $\mathsf{relationalStateQCMA}_\delta \subseteq \mathsf{relationalStateBQP}_{\delta+1/q}$ holds for any $\delta \in [0,1]$ and any polynomial q. In order to prove this statement, we first show (in Proposition 5 below) that if $\mathsf{BQP} = \mathsf{QCMA}$ then we can efficiently "guess" the witness of the circuit synthesizing a relation in $\mathsf{relationalStateQCMA}$. For conciseness, we will write

$$f_p(\ell, n) = 1 - 2^{-n} - \frac{\ell}{p(n)^2}.$$

for a polynomial $p : \mathbb{N} \to \mathbb{N}$ and any integers ℓ, n.

Proposition 5 (Guessing a classical witness) *Let R be a relation in the complexity class $\mathsf{relationalStateQCMA}_\delta[1-2^{-n}, 2^{-n}]$ for some $\delta > 0$, and $(C_n)_{n\in\mathbb{N}}$ be the corresponding family of quantum circuits synthesizing R. Let p be a polynomial such that the circuit C_n acts on less than $p(n)$ qubits, and $\ell(n)$ be the length of the classical witness it receives. If* $\mathsf{BQP} = \mathsf{QCMA}$*, then there exists a polynomial-time quantum algorithm that receives as input a string $x \in L_R^{\mathrm{yes}}$ and outputs with probability at least $(1-2^{-n})^{\ell(n)}$ a string $w \in \{0,1\}^{\ell(n)}$ such that*

$$\Pr(C_x^{\mathrm{acc}}(w) = 1) \geq f_p(\ell(n)+1, n)$$

holds.

We use the following lemma to prove Proposition 5.

Lemma 2 *For any polynomial $p : \mathbb{N} \to \mathbb{N}$, the promise language $\mathbf{GW}_p := (\mathbf{GW}_p^{\mathrm{yes}}, \mathbf{GW}_p^{\mathrm{no}})$ defined below is in* QCMA. $\mathbf{GW}_p^{\mathrm{yes}} := \{(C, x, w_0) \mid \{\, C\ \mathit{describesaquantumcircuittaking} \leq p(|x|)\mathit{qubitsasinput}$
$\mathbf{GW}_p^{\mathrm{no}} := \{(C, x, w_0) \mid \{\, C\ \mathit{describesaquantumcircuittaking} \leq p(|x|)\mathit{qubitsasinput}|x| + |w_0| < p(|x|)\forall w, \Pr(C^{\mathrm{a}}$

Proof. For any $n \in \mathbb{N}$, consider the following verification circuit. The circuit receives as input (C, x, w_0) and w as classical witness. It simulates $C(xw_01w)$ and accepts iff this simulation accepts.

Completeness. If $(C, x, w_0) \in \mathbf{GW}_p^{\mathrm{yes}}$ then there exists w such that

$$\Pr(C^{\mathrm{acc}}(xw_01w) = 1) \geq f_p(|w_0|, |x|)$$

holds.

Soundness. If $(C, x, w_0) \in \mathbf{GW}_p^{\mathrm{no}}$, then for any w, the inequality

$$\Pr(C^{\mathrm{acc}}(xw_01w) = 1) \leq f_p(|w_0|+1, |x|)$$

holds.

Since $f_p(|w_0|, |x|) - f_p(|w_0|+1, |x|)$ is lower bounded by an inverse-polynomial function of the input length, we conclude that $\mathbf{GW}_p \in \mathsf{QCMA}$. □

We are now ready to give the proof of Proposition 5. **Proof of Proposition 5.** Assume that $\mathsf{BQP} = \mathsf{QCMA}$. Let $\mathcal{A}$ be a polynomial-time quantum algorithm deciding $\mathbf{GW}_p \in$

$\mathsf{BQP}[1-2^{-n}, 2^{-n}]$, where $\mathbf{GW}_p$ is defined in Lemma 2. Consider the following quantum algorithm that receives $x \in L_R^{\text{yes}}$ as input. The algorithm constructs bit by bit a classical witness $w = w_1...w_{\ell(n)}$ by defining the bit w_i as follows: if $\mathcal{A}$ on input $(C_n, x, w_1...w_{i-1})$ accepts then set $w_i = 1$, otherwise set $w_i = 0$.

This running time of this algorithm is polynomial. We now show its correctness. Consider a string $x \in L_R^{\text{yes}}$. In the analysis below, we assume that V does not make any error (i.e., always decides correctly membership in $\mathbf{GW}_p$ during the $\ell(n)$ iterations), which happens with probability at least $(1-2^{-n})^{\ell(n)}$.

For conciseness, for any $q \in [0,1]$ we say that a string $\bar{w} \in \{0,1\}^{\ell(n)}$ is a q-witness if

$$\Pr(C_x^{\text{acc}}(\bar{w})) \geq q$$

holds. For conciseness again, we write below $f(i)$ instead of $f_p(i,n)$.

We show by induction on i that for each $i \in \{0, \ldots, \ell(n)\}$ the following property $\mathcal{P}_i$ holds at the end of the ith iteration (or at the very beginning of the algorithm for $i = 0$): there exists an $f(i+1)$-witness starting with $w_1 \ldots w_i$. Property $P_{\ell(n)}$ then implies the correctness of our algorithm.

Property P_0 is obviously true: from the completeness of C_n we know that there exists at least one $f(0)$-witness.

Assume now that the property P_{i-1} is true for some $i \in \{1, \ldots, \ell(n)\}$, i.e., there exists an $f(i)$-witness starting with $w_1 \ldots w_{i-1}$. If there exists an $f(i)$-witness starting with $w_1 \ldots w_{i-1}1$ then $(C_n, x, w_1...w_{i-1}) \in \mathbf{GW}_p^{\text{yes}}$, which means that $\mathcal{A}$ on input $(C_n, x, w_1...w_{i-1})$ accepts and we correctly set $w_i = 1$. Otherwise there exists an $f(i)$-witness starting with $w_1 \ldots w_{i-1}0$. If there is no $f(i+1)$-witness starting with $w_1 \ldots w_{i-1}1$ then $(C_n, x, w_1...w_{i-1}) \in \mathbf{GW}_p^{\text{no}}$, which means that Algorithm $\mathcal{A}$ rejects and we correctly set $w_i = 0$; otherwise the output of $\mathcal{A}$ (and the value of w_i) can be arbitrary, which is fine since in this case there exist both an $f(i+1)$-witness starting with $w_1 \ldots w_{i-1}1$ and an $f(i)$-witness starting with $w_1 \ldots w_{i-1}0$. Since $f(i+1) \geq f(i)$, an $f(i)$-witness is an $f(i+1)$-witness. In all cases Property P_i is thus satisfied. □

We can now apply Proposition 5 to prove Theorem 2.

Proof of Theorem 2. We show the contrapositive: we show that $\mathsf{BQP} = \mathsf{QCMA}$ implies that for any $\delta \in [0,1]$ and any polynomial q, the class $\mathsf{relationalStateQCMA}_\delta$ is included in $\mathsf{relationalStateBQP}_{\delta+1/q}$.

Assume that $\mathsf{BQP} = \mathsf{QCMA}$ and take any relation $R \in \mathsf{relationalStateQCMA}_\delta[c,s]$ with $c(n) = 1-2^{-n}$ and $s(n) = 2^{-n}$. Let $(C_n)_{n\in\mathbb{N}}$ denote the circuit synthesizing R with completeness c, soundness s and synthesis error δ, let $\ell(n)$ be the length of the classical witness C_n receives and let $p_1(n)$ be the number of qubits that C_n takes as input. Let p be a polynomial such that $p(n) \geq \sqrt{2q(n)(\ell(n)+1)}$ and $p(n) \geq p_1(n)$ hold. Let C'_n be the circuit obtained by first applying the circuit corresponding to the algorithm of Proposition 5 to guess a witness w and then simulating $C_n(xw)$. In the following, let X be the random variable that gives the witness w guessed by C'_x, and for conciseness let $d = \operatorname{td}(C_x'^{\text{out}|\text{acc}}, xR)$, $d_w = \operatorname{td}(C_x^{\text{out}|\text{acc}}(w), xR)$ and $\delta = \delta(k_R(n))$.

Completeness. Suppose that $xR \neq \emptyset$, i.e., $x \in L_R^{\text{yes}}$. Then by Proposition 5 we obtain $\Pr(C_x'^{\text{acc}} = 1) \geq (1-2^{-n})^{\ell(n)} \cdot f_p(\ell(n)+1, n)$

$= \geq 1 - \ell(n)2^{-n}\underbrace{(1-2^{-n})^{\ell(n)}}\left(1 - 2^{-n} - \frac{\ell(n)+1}{p(n)^2}\right)$
$\geq 1 - (\ell(n)+1)2^{-n} - \frac{\ell(n)+1}{p(n)^2}$
$\geq 1 - 2^{\log(\ell(n)+1)-n} - \frac{1}{2q(n)} =: c'(n)$, where the last inequality holds since we chose a polynomial p satisfying $p(n) \geq \sqrt{2q(n)(\ell(n)+1)}$.

Denote $p_\delta = \Pr(d_w \leq \delta) = \sum_{d_w \leq \delta} \Pr(X = w)$. Since c'(n) $\leq \Pr(C'^{\text{acc}}_x = 1)$
$= \sum_{d_w > \delta} \Pr(X = w) \leq s(n) \underbrace{\Pr(C^{\text{acc}}_x(w) = 1)} + \sum_{d_w \leq \delta} \Pr(X = w) \leq 1 \underbrace{\Pr(C^{\text{acc}}_x(w) = 1)}$
$\leq s(n) + p_\delta$, we have d $\leq \sum_w \Pr(X = w) d_w$
$\leq \sum_{d_w \leq \delta} \Pr(X = w) \leq \delta \underbrace{d_w} + \sum_{d_w > \delta} \Pr(X = w) \leq 1 \underbrace{d_w}$
$\leq \delta \leq 1 \underbrace{p_\delta} + 1 - \geq c'(n) - s(n) \underbrace{p_\delta}$
$\leq \delta + 1 - c'(n) + s(n)$
$\leq \delta + 2^{\log(\ell(n)+1)-n} + \frac{1}{2q(n)} + 2^{-n}$
$\leq \delta + \frac{1}{q(n)}$ when $2^{\log(\ell(n)+1)-n} + 2^{-n} \leq \frac{1}{2q(n)}$, which holds when n is large enough.

Soundness. Suppose that $xR = \emptyset$, i.e., $x \in L^{\text{no}}$. Then by soundness of C_n, whatever the witness w guessed, the acceptance probability is small:

$$\Pr\left(C'^{\text{acc}}_x = 1\right) = \sum_w \Pr(X = w) \leq s(n) \underbrace{\Pr(C^{\text{acc}}_x(w) = 1)} \leq s(|x|).$$

Since $c'(n) - s(n) \geq 1/\text{poly}(n)$, we obtain the inclusion $R \in \mathsf{relationalStateBQP}_{\delta+1/q}$. □

Theorem 2 yields the question of achieving the same result with a quantum witness (i.e., the converse of Proposition 3).

Open question 1 *Does* $\mathsf{relationalStateQMA}_\delta \not\subseteq \mathsf{relationalStateBQP}_{\delta+1/p}$ *for some* $\delta : \mathbb{N} \to [0,1]$ *and polynomial* $p : \mathbb{N} \to \mathbb{N}$ *imply* $\mathsf{BQP} \neq \mathsf{QMA}$*?*

The technique of guessing a quantum witness by using the assumption $\mathsf{BQP} = \mathsf{QMA}$ could not be used here (except if $\mathsf{QCMA} = \mathsf{QMA}$) because using this technique would mean that there is a way to create a valid QMA witness by using classical information and with a polynomial-size circuit.

5 Impossibility to reduce the synthesis error

In this section we prove that it is impossible to reduce the synthesis error for the class $\mathsf{relationalStateBQP}$. Here is the main result:

Theorem 3 *For any* $0 < \epsilon(n) \leq \delta(n) \leq 1 - 2^{-n}$ *and* $0 \leq s(n) < c(n) \leq 1$,

$$\mathsf{relationalStateBQP}_\delta[1,0] \not\subseteq \mathsf{relationalStateR}_{\delta-\epsilon}[c,s].$$

Theorem 3 shows the impossibility to reduce δ even when arbitrary computational power is available and even without a gap between c and s. The following is a straightforward corollary:

Corollary 1 *For any* $0 < \epsilon(n) \leq \delta(n) \leq 1 - 2^{-n}$,

$$\mathsf{relationalStateBQP}_\delta \not\subseteq \mathsf{relationalStateBQP}_{\delta-\epsilon}.$$

Procedure $\mathcal{P}$

1. Apply the circuit C_r^r on the initial state $0^{\otimes r}$.
2. Measure the qubit corresponding to the acceptance bit. Let $b \in \{0, 1\}$ denote the outcome.
3. Measure the output channel in the computational basis. Let $z \in \{0, 1\}^{k(r)}$ denote the outcome.

Fig. 1. Procedure $\mathcal{P}$

This result holds for any class, as long as it is possible to synthesize the maximally mixed state. It holds for the definitions used in prior works as well, even when considering only the inputs in unary [10, 8, 4] as we actually do in the proof of Theorem 3.

Proof of Theorem 3.

We use a diagonal argument to construct a family of strings that cannot be generated with non-trivial probability, and then use it to construct quantum states that can be approximated by a mixed state with error δ but such that generating it with error strictly smaller than δ implies that the family of strings can be generated with non-trivial probability.

Constructing strings from a diagonal argument. Since we are considering uniform families of quantum circuits (i.e., families of quantum circuits generated by Turing machines) we can enumerate them. Let $\mathcal{C}^1$, $\mathcal{C}^2$, $\ldots$ be such an enumeration and for each $r \in \mathbb{N}$, let $\mathcal{C}^r = \{C_n^r\}_{n \in \mathbb{N}}$ denote the circuits in the family.

For any $r \in \mathbb{N}$, we focus on the circuit C_r^r, i.e., we take $n = r$ (as usual in diagonal arguments). Let $k(r)$ denote the number of qubits of the output channel of the circuit C_r^r. Consider the procedure of Figure 1, which we call Procedure $\mathcal{P}$.

For any string $z \in \{0, 1\}^{k(r)}$, let $p(z)$ denote the probability of obtaining z at Step 3 conditioned on getting $b = 1$ at Step 2. From a straightforward counting argument, there is at least one z such that

$$p(z) \leq 2^{-k(r)}.$$

We denote this string (or one of them, chosen arbitrarily, if there are more than one) by u_r.

Constructing the relation. For each $n \in \mathbb{N}$, define the quantum state

$$\rho_n^\delta = \sum_{z \in \{0,1\}^{k(n)}} \alpha_z \mathbb{z},$$

where

$$\alpha_z = \{\, 2^{-k(n)} + \delta(n) if z = u_n, 2^{-k(n)} - \frac{1}{2^{-k(n)} - 1}\delta(n) otherwise.$$

Define the relation $R^\delta = \{(0^n, \rho_n^\delta) \mid n \in \mathbb{N}\}$. Note that the maximally mixed state on $k(n)$ qubits is at distance $\delta(n)$ from ρ_n^δ. Since the maximally mixed state can be generated by a polynomial-size circuit with probability 1, we get

$$R^\delta \in \mathsf{relationalStateBQP}_\delta[1, 0].$$

Impossibility to generate the relation with error $< \delta$. Suppose that there exists a uniform circuit family that synthesizes R^δ with error $\delta - \epsilon < \delta$ and completeness and soundness $c > s$. From Proposition 2 we can assume without loss of generality that $c(n) \geq 1 - \gamma(n)$ for some (computable) function γ such that

$$0 < \gamma(n) < 1 - \frac{2^{-k(n)}}{2^{-k(n)} + \epsilon(n)}.$$

Let $\mathcal{C}^r = \{C_n^r\}_{n \in \mathbb{N}}$ be this family, for some $r \in \mathbb{N}$. Apply Procedure $\mathcal{P}$ described above on the circuit C_r^r.

Consider $p(u_r)$, the probability of obtaining the string u_r at Step 3 of the procedure conditioned on getting $b = 1$ at Step 2. Observe that measuring the state ρ_r^δ in the computational basis gives outcome u_r with probability

$$2^{-k(r)} + \delta(r).$$

By completeness, the probability that C_r^r accepts and generates a state at distance at most $\delta(r) - \epsilon(r)$ from ρ_r^δ is greater than $1 - \gamma(r)$. We thus have $\mathrm{p}(\mathrm{u}_r) \geq (1 - \gamma(r)) \left(2^{-k(r)} + \delta(r) - \left(\delta(r) - \epsilon(r)\right)\right)$ $= (1 - \gamma(r)) \left(2^{-k(r)} + \epsilon(r)\right) > 2^{-k(r)}$, which is impossible by the construction of u_r. □

Acknowledgement

Most of this work was done while HD was in visit at Nagoya University and financed by ENS Paris-Saclay, Universit Paris-Saclay. The authors thank Yupan Liu and Masayuki Miyamoto for the fruitful discussions that happened there. FLG was supported by JSPS KAKENHI Grants Nos. JP20H00579, JP20H05966, JP20H04139, JP24H00071 and MEXT Quantum Leap Flagship Program (MEXT Q-LEAP) Grant No. JPMXS0120319794.

References

1. Scott Aaronson (2016), *The complexity of quantum states and transformations: from quantum money to black holes*, ArXiv:1607.05256.
2. John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen (2023), *Unitary Complexity and the Uhlmann Transformation Problem*, ArXiv:2306.13073.
3. Mihir Bellare and Shafi Goldwasser (1994), *The complexity of decision versus search*, SIAM Journal on Computing, 23(1):97119.
4. Hugo Delavenne, Franois Le Gall, Yupan Liu, and Masayuki Miyamoto (2023), *Quantum Merlin-Arthur proof systems for synthesizing quantum states*, ArXiv:2303.01877.
5. Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous (2011), *QIP = PSPACE*, Journal of the ACM, 58(6):30:130:27.
6. Stephen P. Jordan, Hirotada Kobayashi, Daniel Nagaj, and Harumichi Nishimura (2012), *Achieving Perfect Completeness in Classical-Witness Quantum Merlin-Arthur Proof Systems*, Quantum Information and Computation, 12(56):461471.
7. Nimrod Meggido and Christos H. Papadimitriou (1989), *A note on total functions, existence theorems, and computational complexity*, Technical report, IBM.
8. Tony Metger and Henry Yuen (2023), *stateQIP = statePSPACE*, Proceedings of the 64th IEEE Symposium on Foundations of Computer Science (FOCS 2023), pages 13491356.
9. Gregory Rosenthal (2024), Proceedings of the 35th ACM-SIAM Symposium on Discrete Algorithms (SODA 2024), page 25082534. Gregory Rosenthal (2024), *Efficient quantum state synthesis with one query*, In Proceedings of the 2024 Annual ACM-SIAM Symposium on Discrete Algorithms, pages 25082534. SIAM.

10. Gregory Rosenthal and Henry Yuen (2022), *Interactive proofs for synthesizing quantum states and unitaries*, Proceedings of the 13th Innovations in Theoretical Computer Science Conference (ITCS 2022), pages 112:1112:4.
11. John Watrous (2003), *PSPACE has constant-round quantum interactive proof systems*, Theoretical Computer Science, 292(3):575588.