Unitary Complexity and the Uhlmann Transformation Problem

John Bostanci[1], Yuval Efron[1], Tony Metger[2],
Alexander Poremba[3], Luowen Qian[4], and Henry Yuen[1]

[1]Columbia University
[2]ETH Zurich
[3]MIT/Boston University
[4]Boston University/NTT Research/Northeastern University

Abstract

State transformation problems such as compressing quantum information or breaking quantum commitments are fundamental quantum tasks. However, their computational difficulty cannot easily be characterized using traditional complexity theory, which focuses on tasks with classical inputs and outputs.

To study the complexity of such state transformation tasks, we introduce a framework for *unitary synthesis problems*, including notions of reductions and unitary complexity classes. We use this framework to study the complexity of transforming one entangled state into another via local operations. We formalize this as the *Uhlmann Transformation Problem*, an algorithmic version of Uhlmann's theorem. Then, we prove structural results relating the complexity of the Uhlmann Transformation Problem, polynomial space quantum computation, and zero knowledge protocols.

The Uhlmann Transformation Problem allows us to characterize the complexity of a variety of tasks in quantum information processing, including decoding noisy quantum channels, breaking falsifiable quantum cryptographic assumptions, implementing optimal prover strategies in quantum interactive proofs, and decoding the Hawking radiation of black holes. Our framework for unitary complexity thus provides new avenues for studying the computational complexity of many natural quantum information processing tasks.

Contents

1 Introduction

Complexity theory studies the resources required to solve computational problems. Quantum complexity has traditionally studied the quantum resources required to solve *classical* computational problems, i.e., problems that have classical inputs and outputs. However, quantum mechanics also introduces a new kind of computational problem: preparing and transforming quantum states. The goal of this paper is to initiate the formal complexity-theoretic study of such *quantum state transformation problems*. To this end, we extend the language of traditional complexity theory to encompass state transformation problems – we call the resulting framework *unitary complexity theory*.

The idea that the complexity of inherently quantum problems cannot easily be reduced to the complexity of classical problems has already been explored in prior works [KA04, Aar16, ACQ22]. In recent years, oracle separations [Kre21, KQST23, LMW23] have demonstrated that the complexity of breaking certain quantum cryptographic primitives is independent of the complexity of the decisional complexity classes NP or QMA; in other words, even if $\mathsf{P} = \mathsf{NP}$, certain quantum cryptographic primitives could still remain secure. In fact, [LMW23] gives preliminary evidence that the ability to solve *any* decision problem (even undecidable ones!) would not help with breaking quantum cryptography. Unitary complexity theory allows us to re-establish the link between complexity theory and cryptography in the quantum world.

Beyond this cryptographic motivation, unitary complexity allows us to relate the computational resources required for seemingly unrelated state transformation tasks. In this paper, we focus on tasks involving *Uhlmann transformations*. The name stems from Uhlmann's theorem, [Uhl76] a fundamental result in quantum information theory that quantifies how well a bipartite pure state $|C\rangle$ can be mapped to another bipartite pure state $|D\rangle$ by only acting on a subsystem: letting ρ and σ denote the reduced density matrices on the first subsystem of $|C\rangle$ and $|D\rangle$, respectively, Uhlmann's theorem states that

$$\mathrm{F}(\rho,\sigma) = \max_U \left| \langle D| \, \mathrm{id} \otimes U \, |C\rangle \right|^2 , \tag{1.1}$$

where $\mathrm{F}(\rho,\sigma)$ denotes the fidelity function and the maximization is over all unitary transformations acting on the second subsystem. We call a unitary U achieving equality in Equation (1.1) an *Uhlmann transformation*.[1]

Uhlmann transformations are ubiquitous in quantum information processing. Some examples include:

Quantum Shannon theory. Quantum Shannon theory is the study of the fundamental limits of quantum communication over noisy and noiseless channels. Protocols for a myriad of tasks such as state redistribution, entanglement distillation, and quantum communication over a noisy quantum channel all require performing Uhlmann transformations [HHWY08, ADHW09, BCR11, AJW18].

Quantum cryptography. While it is known that quantum commitment schemes with information-theoretic security are impossible [May97, LC98], they are possible under computational assumptions. Recent oracle separations suggest that their security can be based on weaker assumptions than what is needed classically and that the existence of inherently quantum cryptographic primitives may be independent from assumptions in traditional complexity [Kre21, AQY22, MY22, KQST23, LMW23]. It can be seen from the impossibility results of Mayers–Lo–Chau [May97, LC98] that the security of a quantum commitment scheme relies on the hardness of performing certain Uhlmann transformations.

Quantum gravity. Attempts to unite quantum mechanics with general relativity have given rise to apparent paradoxes of whether black holes preserve information or not [Haw76]. Recently, physicists have provided intriguing arguments based on *computational complexity* as possible resolutions to these

[1] Such Uhlmann transformations are unique only if $|C\rangle, |D\rangle$ have full Schmidt rank.

paradoxes [HH13]. These arguments claim that distilling entanglement from the emitted Hawking radiation of a black hole is computationally infeasible — this can be equivalently phrased as a statement about the hardness of an Uhlmann transformation [HH13, Bra23].

Quantum complexity theory. The $\mathsf{QIP} = \mathsf{PSPACE}$ theorem [JJUW11] gives a characterization of the power of (single-prover) quantum interactive proofs. Kitaev and Watrous [KW00] showed that optimal prover strategies in these interactive proofs boil down to applying Uhlmann transformations at each round.

The fact that Uhlmann transformations appear in these various quantum tasks suggests that they might be related. Can we formalize these relationships and show precise reductions, similarly to how e.g. the theory of NP completeness relates disparate classical computational problems? Can we formalize Uhlmann transformations as a computational problem that is, in some sense, *complete* for these various tasks, similarly to how 3-SAT provides a simple complete problem that elegantly captures the hardness of NP-complete problems? Can we provide complexity-theoretic evidence for the hardness of Uhlmann transformations? What computational restrictions does this place on our ability to e.g. achieve optimal communication rates in quantum Shannon theory?

The goal of this paper is to study such questions formally. Our first main contribution is to provide a general formal framework for reasoning about unitary complexity (Part I). This involves extending many of the traditional notions of complexity theory, such as reductions, complexity classes, complete problems, etc. to quantum state transformations and requires us to deal with many subtleties that arise in the unitary setting. Our second main contribution is to analyze the complexity of the Uhlmann Transformation Problem within this framework (Part II). This in turn allows us to show relationships between unitary complexity classes such as showing that (average case versions of) the classes $\mathsf{unitaryPSPACE}$ and $\mathsf{unitaryQIP}$ are equal. Finally, we show how the Uhlmann transformation problem plays a central role in connecting the complexity of many natural tasks in quantum information processing (Part III). For example, we establish reductions and equivalences between Uhlmann transformation problem and the security of quantum commitment schemes, falsifiable quantum cryptographic assumptions, quantum state compression, and more.

1.1 A fully quantum complexity theory

In [RY22] Rosenthal and Yuen initiated the study of complexity classes for *state synthesis* and *unitary synthesis* problems. A state synthesis problem is a sequence $(\rho_x)_{x\in\{0,1\}^*}$ of quantum states. A *state complexity class* is a collection of state synthesis problems that captures the computational resources needed to synthesize (i.e., generate) the states. For example, [RY22] defined the class $\mathsf{statePSPACE}$ as the set of all state sequences $(\rho_x)_{x\in\{0,1\}^*}$ for which there is a polynomial-space (but possibly exponential-time) quantum algorithm A that, on input x, outputs an approximation to the state ρ_x.

Unitary complexity classes, which are the focus of this work, describe the computational resources needed to perform state *transformations*, formalized as *unitary synthesis problems*. A unitary synthesis problem is a sequence of unitary[2] operators $(U_x)_{x\in\{0,1\}^*}$ and a unitary complexity class is a collection of unitary synthesis problems. For example the class $\mathsf{unitaryBQP}$ is the set of all sequences of unitary operators $(U_x)_{x\in\{0,1\}^*}$ where there is a polynomial-time quantum algorithm A that, given an *instance* $x \in \{0,1\}^*$ and a quantum system B as input, (approximately) applies U_x to system B. As a simple example, any sequence of unitaries (U_x) where x is simply (an explicit encoding of) a sequence of quantum gates that implement the unitary is obviously in $\mathsf{unitaryBQP}$, since given x, the algorithm A can just execute the circuit specified

[2] In our formal definition of unitary synthesis problems (see Section 3), the U_x's are technically partial isometries, which is a promise version of unitaries, but we gloss over the distinction for now.

by x in time polynomial in the length of x. On the other hand, x could also specify a unitary in a sequence in a more implicit way (e.g. by circuits for two quantum states between which U_x is meant to be the Uhlmann transformation), in which case the sequence $(U_x)_x$ could be harder to implement.

The reason we say that the algorithm A is given a *system* instead of a *state* is to emphasize that the state of the system is not known to the algorithm ahead of time, and in fact the system may be part of a larger entangled state. Thus the algorithm has to coherently apply the transformation U_x to the given system, maintaining any entanglement with an external system. This makes unitary synthesis problems fundamentally different, and in many cases harder to analyse, than state synthesis problems.

Traditional complexity classes like P, NP, and BQP have proven to be powerful ways of organizing and comparing the difficulty of different decision problems. In a similar way, state and unitary complexity classes are useful for studying the complexity of quantum states and of quantum state transformations. We can then ask about the existence of complete problems, reductions, inclusions, separations, closure properties, and more. Importantly, state and unitary complexity classes provide a useful language to articulate questions and conjectures about the computational hardness of inherently quantum problems. For example, we can ask whether unitaryPSPACE is contained in $\mathsf{unitaryBQP}^{\mathsf{PSPACE}}$ — in other words, can polynomial-space-computable unitary transformations be also computed by a polynomial-time quantum computer that is given oracle access to a PSPACE decision oracle?[3]

Unitary synthesis problems, classes, and reductions. We begin by giving general definitions for unitary synthesis problems and a number of useful unitary complexity classes, e.g. unitaryBQP and unitaryPSPACE. We then define a notion of *reductions* between unitary synthesis problems. Roughly speaking, we say that a unitary synthesis problem $\mathscr{U} = (U_x)_x$ polynomial-time reduces to $\mathscr{V} = (V_x)_x$ if an efficient algorithm for implementing $\mathscr{V}$ implies an efficient algorithm for implementing $\mathscr{U}$.

Next, we define *distributional* unitary complexity classes that capture the *average case complexity* of solving a unitary synthesis problem. Here, the unitary only needs to be implemented on an input state *randomly chosen* from some distribution $\mathcal{D}$ which is known ahead of time. This is a natural generalisation of traditional average-case complexity statements to the unitary setting. This notion turns out to be particularly natural in the context of entanglement transformation problems because it is closely related to implementing the unitary on part of an entangled state $|\psi\rangle$.

The notion of average case complexity turns out to be central to our paper: nearly all of our results are about average-case unitary complexity classes and the average-case complexity of the Uhlmann Transformation Problem. Thus the unitary complexity classes we mainly deal with will be avgUnitaryBQP and avgUnitaryPSPACE, which informally mean sequences of unitaries that can be implemented by time-efficient and space-efficient quantum algorithms, respectively, and where the implementation error is measured with respect to inputs drawn from a fixed distribution over quantum states.

See Section 3 for details as well as more discussion regarding the choices we made for our definitions.

Interactive proofs for unitary synthesis. We then explore models of *interactive proofs* for unitary synthesis problems. Roughly speaking, in an interactive proof for a unitary synthesis problem $\mathscr{U} = (U_x)_x$, a polynomial-time verifier receives an instance x and a quantum system B as input, and interacts with an all-powerful but untrusted prover to try to apply U_x to system B. As usual in interactive proofs, the main challenge is that the verifier does not trust the prover, so the protocol has to test whether the prover actually behaves as intended. We formalize this with the complexity classes unitaryQIP and avgUnitaryQIP, which capture unitary synthesis problem that can be verifiably implemented in this interactive model. This gener-

[3] This is an open question, and is related to the "Unitary Synthesis Problem" raised by Aaronson and Kuperberg [AK07].

alizes the interactive state synthesis model studied by [RY22, MY23].[4] The primary difference between the state synthesis and unitary synthesis models is that in the former, the verifier starts with a fixed input state (say, the all zeroes state), while in the latter the verifier receives a quantum system B in an unknown state that has to be transformed by U_x. See Section 4 for more details.

Zero-knowledge unitary synthesis. In the context of interactive protocols, we also introduce a notion of *zero-knowledge protocols* for unitary synthesis problems. Roughly speaking, a protocol is zero-knowledge if the interaction between the verifier and prover can be efficiently reproduced by an algorithm (called the *simulator*) that does not interact with the prover at all. This way, the verifier can be thought of as having learned no additional knowledge from the interaction aside from the fact that the task was solved [GMR89]. The counterintuitive concept of zero-knowledge proofs has been one of the most consequential discoveries in complexity theory and cryptography.

Motivated by this, we introduce the unitary complexity class avgUnitaryHVSZK,[5] which is a unitary synthesis analogue of the decision class HVQSZK in traditional complexity theory [Wat06], which captures the concept of *honest-verifier quantum zero-knowledge proofs*. Interestingly, for reasons that we explain in more detail in Section 4.3, the average-case aspect of avgUnitaryHVSZK appears to be necessary to obtain a nontrivial definition of zero-knowledge in the unitary synthesis setting.

Just like there is a zoo of traditional complexity classes [Aar23], we expect that many unitary complexity classes can also be meaningfully defined and explored. In this paper we focus on the ones that turn out to be tightly related to the Uhlmann Transformation Problem. We discuss these relationships next.

Remark 1.1. For simplicity, in the introduction we present informal statements of our results that gloss over some technical details that would otherwise complicate the result statement. For example, we do not distinguish between unitary synthesis problems and distributional versions of them. After each informal result statement we point the reader to where the formal result is stated and proved.

1.2 Structural results about the Uhlmann Transformation Problem

Equipped with the proper language to talk about unitary synthesis problems, we present the Uhlmann Transformation Problem in Part II of this paper. We define the unitary synthesis problem Uhlmann to be the sequence $(U_x)_{x \in \{0,1\}^*}$ where we interpret an instance x as an explicit encoding (as a list of gates) of a pair of quantum circuits (C, D) such that C and D, on the all-zeroes input, output pure bipartite states $|C\rangle, |D\rangle$ on the same number of qubits, and U_x is an associated Uhlmann transformation mapping $|C\rangle$ to $|D\rangle$ by acting on a local system. Usually, we will assume that C and D output $2n$ qubits (for some n specified as part of x) and the Uhlmann transformation acts on the last n qubits. If x does not specify such a pair, then an algorithm implementing the unitary synthesis problem is allowed to behave arbitrarily on such x; this is formally captured by allowing partial isometries as part of unitary synthesis problems in Definition 3.1.

Furthermore, for a parameter $0 \leq \kappa \leq 1$ we define the problem Uhlmann$_\kappa$, which is the same as Uhlmann, except that it is restricted to instances corresponding to states $|C\rangle, |D\rangle$ where the fidelity between the reduced density matrices ρ, σ of $|C\rangle, |D\rangle$ respectively on the first subsystem is at least κ; recall by Uhlmann's theorem that κ lower bounds how much overlap $|C\rangle$ can achieve with $|D\rangle$ by a local transformation. By definition, Uhlmann$_\kappa$ instances are at least as hard as Uhlmann$_{\kappa'}$ instances when

[4] The class unitaryQIP was also briefly discussed informally by Rosenthal and Yuen [RY22].

[5] The "HV" modifier signifies that the zero-knowledge property is only required to hold with respect to verifiers that honestly follow the protocol, and the "S" in "SZK" signifies that it is *statistical* zero-knowledge.

$\kappa \leq \kappa'$. We provide formal definitions of $\textsc{Uhlmann}$, $\textsc{Uhlmann}_\kappa$, and their distributional versions in Section 5.

Zero-knowledge and the Uhlmann Transformation Problem. We show that the Uhlmann Transformation Problem (with fidelity parameter $\kappa = 1$) *characterizes* the complexity of the unitary complexity class $\mathsf{avgUnitaryHVPZK}$, which is the unitary synthesis version of the decision classes PZK and HVQPZK [Wat02]. Here, PZK stands for "perfect zero knowledge", and refers to the special case of statistical zero-knowledge where the simulator can *perfectly* reproduce the view of the verifier.

Theorem 1.2 (Informal)**.** $\textsc{Uhlmann}_1$ is complete for $\mathsf{avgUnitaryHVPZK}$ under polynomial-time reductions.

This is formally stated and proved in Section 6.1. To show completeness we have to prove two directions. The first direction is to show that every (distributional) unitary synthesis problem in $\mathsf{avgUnitaryHVPZK}$ polynomial-time reduces to (the distributional version of) $\textsc{Uhlmann}_1$. This uses a characterization of quantum interactive protocols due to Kitaev and Watrous [KW00].

The second direction is to show that $\textsc{Uhlmann}_1$ is in $\mathsf{avgUnitaryHVPZK}$ by exhibiting an (honest-verifier) zero-knowledge protocol to solve the Uhlmann Transformation Problem. Our protocol is rather simple: in the average case setting, we assume that the verifier receives the last n qubits of the state $|C\rangle = C\,|0^{2n}\rangle$, and the other half is inaccessible. Its goal is to transform, with the help of a prover, the global state $|C\rangle$ to $|D\rangle$ by only acting on the last n qubits that it received as input. To this end, the verifier generates a "test" copy of $|C\rangle$ on its own, which it can do because C is a polynomial-size circuit. The verifier then sends to the prover two registers of n qubits; one of them is the first half of the test copy and one of them (call it A) holds the "true" input state. The two registers are randomly shuffled. The prover is supposed to apply the Uhlmann transformation U to both registers and send them back. The verifier checks whether the "test" copy of $|C\rangle$ has been transformed to $|D\rangle$ by applying the inverse circuit $D^\dagger$ to the test copy and checking if all qubits are zero. If so, it accepts and outputs the register A, otherwise the verifier rejects.

If the prover is behaving as intended, then both the test copy and the "true" copy of $|C\rangle$ are transformed to $|D\rangle$. Furthermore, the prover cannot tell which of its two registers corresponds to the test copy, and thus if it wants to pass the verification with high probability, it has to apply the correct Uhlmann transformation on both registers. This shows that the protocol satisfies the completeness and soundness properties of an interactive proof. The zero-knowledge property is also straightforward: if both the verifier and prover are acting according to the protocol, then before the verifier's first message to the prover, the reduced state of the verifier is $|C\rangle\!\langle C| \otimes \rho$ (where ρ is the reduced density matrix of $|C\rangle$), and at the end of the protocol, the verifier's state is $|D\rangle\!\langle D| \otimes U\rho U^\dagger$. Both states can be produced in polynomial time.

One may ask: if the simulator can efficiently compute the state $U\rho U^\dagger$ without the help of the prover, does that mean the Uhlmann transformation U can be implemented in polynomial time? The answer is no, since the simulator only has to prepare the appropriate reduced state (i.e. essentially solve a state synthesis task), which is easy since the starting and ending states of the protocol are efficiently computable; in particular, $U\rho U^\dagger$ is (approximately) the reduced state of $|D\rangle$, which is easy to prepare. In contrast, the verifier has to implement the Uhlmann transformation on a *specific* set of qubits that are entangled with a *specific* external register, i.e. it has to perform a state transformation task that preserves coherence with the purifying register. This again highlights the distinction between state and unitary synthesis tasks.

A complete problem for $\mathsf{avgUnitaryHVSZK}$? It is natural to wonder about the complexity of $\textsc{Uhlmann}_\kappa$ for fidelity promise $\kappa < 1$. In other words, the reduced density matrices of the two states $|C\rangle\,, |D\rangle$ are not exactly equal. A reasonable conjecture is that $\textsc{Uhlmann}_\kappa$ (for non-negligible κ, say), is complete for avgUnitaryHVSZK. This would correspond to the famous classical complexity result that the problem of distinguishing between whether two probability distributions (represented via sampling circuits) are close or far in trace distance is a SZK-complete problem [SV03].

In Section 6.3 we argue that this conjecture is true assuming that a unitary version of the *polarization lemma* holds, which was instrumental for the SZK-completeness result of Sahai and Vadhan [SV03]. The unitary polarization lemma, if true, would state that $\textsc{Uhlmann}_\kappa$ polynomial-time reduces to $\textsc{Uhlmann}_{1-2^{-\mathrm{poly}(n)}}$ for all inverse polynomial κ.

The succinct Uhlmann Transformation Problem. We also define a *succinct* version of the Uhlmann Transformation Problem (denoted by $\textsc{SuccinctUhlmann}$), where the string x encodes a pair $(\hat{C}, \hat{D})$ of *succinct descriptions* of quantum circuits C, D. By this we mean that $\hat{C}$ (resp. $\hat{D}$) is a classical circuit that, given a number $i \in \mathbb{N}$ written in binary, outputs the i'th gate in the quantum circuit C (resp. D). Thus the circuits C, D in general can have *exponential* depth (in the length of the instance string x) and generate states $|C\rangle, |D\rangle$ that are unlikely to be synthesizable in polynomial time. Thus the task of synthesizing the Uhlmann transformation U that maps $|C\rangle$ to a state with maximum overlap with $|D\rangle$, intuitively, should be much harder than the non-succinct version. We confirm this intuition with the following result:

Theorem 1.3 (Informal)**.** $\textsc{SuccinctUhlmann}$ is complete for avgUnitaryPSPACE under polynomial-time reductions.

The class avgUnitaryPSPACE corresponds to distributional unitary synthesis problems that can be solved using a polynomial-space (but potentially exponential-depth) quantum algorithm. The fact that $\textsc{SuccinctUhlmann} \in$ avgUnitaryPSPACE was already proved by Metger and Yuen [MY23], who used this to show that optimal prover strategies for quantum interactive proofs can be implemented in avgUnitaryPSPACE.[6] The fact that avgUnitaryPSPACE reduces to $\textsc{SuccinctUhlmann}$ is because solving a distributional unitary synthesis problem $(U_x)_x$ in avgUnitaryPSPACE is equivalent to applying a local unitary that transforms an entangled state $|\psi_x\rangle$ representing the distribution to $(\mathrm{id} \otimes U_x)\,|\psi_x\rangle$. This is nothing but an instance of the $\textsc{SuccinctUhlmann}$ transformation problem. We refer to the proof of Lemma 7.5 for details.

We show another completeness result for $\textsc{SuccinctUhlmann}$:

Theorem 1.4 (Informal)**.** $\textsc{SuccinctUhlmann}$ is complete for avgUnitaryQIP under polynomial-time reductions.

Here, the class avgUnitaryQIP is like avgUnitaryHVPZK except there is no requirement that the protocol between the honest verifier and prover can be efficiently simulated. The proof of Theorem 1.4 starts similarly to the proof of the avgUnitaryHVPZK-completeness of $\textsc{Uhlmann}$, but requires additional ingredients, such as the state synthesis protocol of [RY22, Ros24] and the ability to simulate reflections about a state, given copies of the state [JLS18]. We prove this by showing that $\textsc{SuccinctUhlmann}$ is contained in avgUnitaryQIP (Lemma 7.2), avgUnitaryQIP $\subseteq$ avgUnitaryPSPACE (Lemma 7.8), and then argue that avgUnitaryPSPACE is polynomial-time reducible to $\textsc{SuccinctUhlmann}$ (Lemma 7.5).

Theorems 1.3 and 1.4 imply the following unitary complexity analogue of the QIP $=$ PSPACE theorem [JJUW11] and the stateQIP $=$ statePSPACE theorem [RY22, MY23]:

Theorem 1.5. avgUnitaryQIP $=$ avgUnitaryPSPACE.

This partially answers an open question of [RY22, MY23], who asked whether unitaryQIP $=$ unitaryPSPACE (although they did not formalize this question to the same level as we do here).

[6] This was phrased in a different way in their paper, as avgUnitaryPSPACE was not yet defined.

1.3 Centrality of the Uhlmann Transformation Problem

In Part III of this paper we relate the Uhlmann Transformation Problem to quantum information processing tasks in a variety of areas: quantum cryptography, quantum Shannon theory, and high energy physics. We show that the computational complexity of a number of these tasks is in fact essentially *equivalent* to the hardness of UHLMANN. For some other problems we show that they are efficiently reducible to UHLMANN or SUCCINCTUHLMANN. Although some of these connections have been already observed in prior work, we believe that the framework of unitary complexity theory formalizes and clarifies the relationships between these different problems.

We proceed to give a high level overview of our applications of the Uhlmann Transformation Problem and unitary complexity theory.

1.3.1 Quantum cryptography

We show that the Uhlmann Transformation Problem is deeply intertwined with the security of quantum cryptography. First, we show the security of quantum commitment schemes is *equivalent* to the average-case hardness of the Uhlmann Transformation Problem.

Quantum commitments. A bit commitment scheme is a fundamental cryptographic primitive that allows two parties (called a *sender* and *receiver*) to engage in a two-phase communication protocol: in the first phase (the "commit phase"), the sender sends a commitment (i.e. some string) to a bit b to the receiver; the *hiding* property of a bit commitment scheme ensures that the receiver cannot decide the value of b from this commitment string alone. In the second phase (the "reveal phase"), the sender sends another string to the receiver that allows the receiver to compute the value of b; the *binding* property of commitments ensures that the sender can only reveal the correct value of b, i.e. if the sender sent a reveal string that was meant to convince the receiver it had committed to a different value of b, the receiver would detect this.

Commitment schemes — even quantum ones — require efficiency constraints on the adversary [May97, LC98]; at least one of the hiding or binding properties must be computational. In classical cryptography, commitment schemes can be constructed from one-way functions [Nao03], but recent works suggest the possibility of basing quantum commitment schemes on weaker, inherently quantum assumptions such as the existence of pseudorandom states [Kre21, AQY22, MY22, KQST23] or EFI pairs [BCQ23].

The following theorem shows that the existence of secure quantum commitment schemes is essentially equivalent to UHLMANN being hard on average. Roughly speaking, hardness on average means that there is an efficiently sampleable distribution over pairs of quantum circuits (C, D) such that all polynomial-time algorithms fail to implement the Uhlmann transformation corresponding to $(|C\rangle, |D\rangle)$ with non-negligible probability over the sampling of (C, D).

Theorem 1.6 (Informal)**.** $\textsc{Uhlmann}_{1-\epsilon}$ for some negligible ϵ is hard on average if and only if secure quantum commitments exist.

This theorem is formally stated and proved as Theorem 8.10. This formalizes a connection between Uhlmann transformations and quantum commitments that was suggested by Yan in his in-depth study of properties of quantum bit commitments [Yan22]. The necessity for the hardness of UHLMANN is implicit in the original impossibility proofs of information-theoretic security for commitments [May97, LC98]; the sufficiency is due to the fact that *non-interactive quantum commitments* can be constructed from hard UHLMANN instances.

Given the close connection between zero knowledge protocols for unitary synthesis and the Uhlmann Transformation Problem, we also prove the following:

Theorem 1.7 (Informal)**.** If there is a hard distribution of instances for $\mathsf{avgUnitaryHVSZK}$, then secure quantum commitments exist.

We note that this would follow as an immediate corollary if we were able to prove that $\textsc{Uhlmann}_{1-\epsilon}$ is a complete problem for $\mathsf{avgUnitaryHVSZK}$; however as mentioned previously this remains a conjecture. We instead prove Theorem 1.7 directly by showing that hard-on-average problems in $\mathsf{avgUnitaryHVSZK}$ implies $\textsc{Uhlmann}_{1-\epsilon}$ is hard on average.

This is analogous to the classical result of Ostrovsky [Ost91] who showed that if the classical complexity class SZK is hard on average, then one-way functions (and thus secure bit commitments [Nao91]) exist. This is formally stated and proved as Theorem 8.11.

Minimal assumptions in quantum cryptography. In classical cryptography, the existence of one-way functions is considered a *minimal assumption* in the sense that the security of virtually all (classical) cryptography implies it [IL89, Imp95]. It is a fascinating open question of what is the minimal assumption (if there exists one) in quantum cryptography; as of writing the leading contender for the minimal quantum cryptographic assumption is the existence of quantum commitments, meaning that many quantum cryptographic primitives can be shown to imply the existence of quantum commitments [BCQ23, KT23]. If quantum commitments are indeed minimal (mirroring the setting of classical cryptography), then this would show that the hardness of the Uhlmann Transformation Problem is necessary for computationally secure quantum cryptography.

Breaking falsifiable quantum cryptographic assumptions. While we don't know yet if the hardness of the Uhlmann Transformation Problem is necessary for computational quantum cryptography, we show that the hardness of the *succinct* Uhlmann Transformation Problem is necessary for the security of a wide class of quantum cryptographic primitives. We consider the general notion of a *falsifiable quantum cryptographic assumption*, which can be seen as a quantum analogue of the notion of a falsifiable assumption considered by Naor [Nao03] as well as Gentry and Wichs [GW11]. Our notion of a falsifiable quantum cryptographic assumption captures almost any reasonable definition of security in quantum cryptography which can be phrased in terms of an interactive *security game* between an adversary and a challenger. We show the following generic upper bound on the complexity of breaking falsifiable quantum cryptographic assumptions (see Theorem 8.15 for the formal statement):

Theorem 1.8 (Informal)**.** A falsifiable quantum cryptographic assumption is either information-theoretically secure, or the task of breaking security reduces to $\textsc{SuccinctUhlmann}$.

Since $\textsc{SuccinctUhlmann}$ is complete for $\mathsf{avgUnitaryPSPACE}$ (Theorem 1.3), this means that $\mathsf{avgUnitaryBQP} \neq \mathsf{avgUnitaryPSPACE}$ is a necessary complexity-theoretic assumption for computational quantum cryptography. This suggests that unitary complexity provides the appropriate framework to establish a close link between complexity theory and quantum cryptography, as recent work [Kre21, AQY22, MY22, KQST23, LMW23] has shown that traditional complexity theoretic assumptions are not always linked to quantum cryptography in the way one would expect.

1.3.2 Quantum Shannon theory applications

Quantum Shannon theory studies the achievability and limits of quantum communication tasks (see [Wil17, KW20, Ren22] for a comprehensive overview). While the information-theoretic aspects of quantum communication tasks are well-understood, the complexity of implementing these protocols has received remarkably little attention. Here, we study the computational complexity of some fundamental tasks in quantum

Shannon theory, namely noisy channel decoding and compression of quantum states using our framework for unitary complexity and our results on the Uhlmann transformation problem.[7]

Decodable channel problem. Consider a quantum channel $\mathcal{N}$ that maps a register A to a register B. Suppose that the channel $\mathcal{N}$ is *decodable*, meaning that it is possible to information-theoretically (approximately) recover the information sent through the channel; i.e., there exists a decoding channel $\mathcal{D}$ mapping register B back to register A such that $\mathcal{D}_{\mathsf{B}\to\mathsf{A}'}\Big(\mathcal{N}_{\mathsf{A}\to\mathsf{B}}(\Phi_{\mathsf{AR}})\Big) \approx \Phi_{\mathsf{A}'\mathsf{R}}$, where $|\Phi\rangle_{\mathsf{AR}}$ is the maximally entangled state. Note that the register R is not touched.

Important examples of decodable channels come from coding schemes for noisy quantum channels: suppose $\mathcal{K}$ is a noisy quantum channel that has capacity C (meaning it is possible to (asymptotically) transmit C qubits through $\mathcal{K}$). Let $\mathcal{E}$ denote a channel that takes C qubits and maps it to an input to $\mathcal{K}$. For example, we can think of $\mathcal{E}$ as an encoder for a quantum error-correcting code. If $\mathcal{E}$ is a good encoding map, the composite channel $\mathcal{N} : \rho \mapsto \mathcal{K}(\mathcal{E}(\rho))$ is decodable.

We define the *Decodable Channel Problem*: given as input a circuit description of a channel $\mathcal{N}$ that maps register A to register B and furthermore is promised to be decodable, and given the register B of the state $(\mathcal{N} \otimes \mathrm{id})(\Phi_{\mathsf{AR}})$, decode and output a register $\mathsf{A}' \equiv A$ such that the final joint state of $\mathsf{A}'\mathsf{R}$ is close to $|\Phi\rangle$. Although it is information-theoretically possible to decode the output of $\mathcal{N}$, it may be computationally intractable to do so. In fact, we can characterize the complexity of the Decodable Channel Problem:

Theorem 1.9 (Informal)**.** The Decodable Channel Problem can be solved in polynomial-time up to inverse polynomial error if and only if UHLMANN can be solved in polynomial-time up to inverse polynomial error.

This theorem is formally stated and proved as Theorem 9.6; since we do not expect that UHLMANN is solvable in polynomial-time, this suggests that the Decodable Channel Problem is computationally hard in general. The main idea behind the upper bound (Decodable Channel Problem is easy if UHLMANN is easy) is that a channel $\mathcal{N}$ is decodable if and only if the output of the *complementary channel*[8] $\mathcal{N}^c$, when given register A of the maximally entangled state $|\Phi\rangle_{\mathsf{AR}}$, is approximately unentangled with register R. Thus by Uhlmann's theorem there exists an Uhlmann transformation acting on the output of the channel $\mathcal{N}$ that recovers the maximally entangled state. If UHLMANN $\in$ avgUnitaryBQP, then this transformation can be performed efficiently.

The proof of the lower bound (Decodable Channel Problem is hard if UHLMANN is hard) draws inspiration from quantum commitments. As discussed earlier, the hardness of UHLMANN essentially implies the existence of secure quantum commitments, and in particular one where the hiding property is computational. From this, we can construct a hard instance of the Decodable Channel Problem: consider a channel $\mathcal{N}$ that takes as input a single bit $|b\rangle$, and then outputs the commitment register of the commitment to bit b (and discards the reveal register). The ability to decode this "commitment channel" implies the ability to break the hiding property of the underlying commitment scheme, and therefore decoding must be computationally hard.

Compression of quantum information. Another fundamental task in information theory — both classical and quantum — is compression of data. Shannon's source coding theorem shows that the Shannon

[7] We also note that in independent work after the publication of our results, Arnon-Friedman, Brakerski, and Vidick have investigated the computational aspects of entanglement distillation [ABV23], showing that in general entanglement distillation is computationally infeasible assuming quantum commitments exist. It would be interesting to connect their results to our framework for unitary complexity to build up a more rigorous theory of the complexity of quantum Shannon tasks.

[8] The output of the complementary channel can be thought of as the qubits that a purification (formally, a Stinespring dilation) of the channel $\mathcal{N}$ discards to the environment.

entropy of a random variable X characterizes the rate at which many independent copies of X can be compressed [Sha48]. Similarly, Schumacher proved that the von Neumann entropy of a density matrix ρ characterizes the rate at which many independent copies of ρ can be (coherently) compressed [Sch95].

We consider the *one-shot* version of the information compression task, where one is given just one copy of a density matrix ρ (rather than many copies) and the goal is to compress it to as few qubits as possible while being able to recover the original state within some error. In the one-shot setting the von Neumann entropy no longer characterizes the optimal compression of ρ; instead this is given by a one-shot entropic quantity known as the *smoothed max-entropy* [Tom13]. What is the computational effort required to perform near-optimal one-shot compression of quantum states? Our next result gives upper and lower bounds for the computational complexity of this task:

Theorem 1.10 (Informal)**.** Quantum states can be optimally compressed to their smoothed max entropy in polynomial-time if $\textsc{Uhlmann}_{1-\epsilon} \in \mathsf{avgUnitaryBQP}$ for some negligible ϵ. Furthermore, if stretch pseudorandom state generators exist, then optimal compression of quantum states cannot be done in polynomial time.

This theorem is formally stated and proved as Theorems 9.11 and 9.13. The upper bound (i.e., compression is easy if $\textsc{Uhlmann}$ is easy) is proved using a powerful technique in quantum information theory known as *decoupling* [Dup09]. The hardness result for compression is proved using a variant of *pseudorandom states*, a cryptographic primitive that is a quantum analogue of pseudorandom generators [JLS18].

1.3.3 Black-hole radiation decoding

In recent years, quantum information and quantum complexity have provided a new lens on long-standing questions surrounding the quantum-mechanical description of black holes. [Pre92, AMPS13, HH13, BRS⁺16, Sus16, BFV20, YE23]. We consider applications of the Uhlmann Transformation Problem to computational tasks arising from this research.

In particular, we consider the Harlow-Hayden *black hole radiation decoding task* [HH13], which is defined as follows. We are given as input a circuit description of a tripartite state $|\psi\rangle_{\mathsf{BHR}}$ that represents the global pure state of a single qubit (register B), the interior of a black hole (register H), and the Hawking radiation that has been emitted by the black hole (register R). Moreover, we are promised that it is possible to *decode* from the emitted radiation R a single qubit A that forms a maximally entangled state $|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with register B. The task is to perform this decoding when given register R of a system in the state $|\psi\rangle$.

Harlow and Hayden [HH13] showed that the decoding task is computationally intractable assuming that $\mathsf{SZK} \not\subseteq \mathsf{BQP}$. However, precisely characterizing the task's complexity (i.e., providing an equivalence rather than a one-way implication) appears to require the notions of a fully quantum complexity theory. Brakerski recently showed that this task is equivalent to breaking the security of a quantum cryptographic primitive known as EFI pairs [Bra23]. We reformulate this equivalence in our unitary complexity framework to show that black hole radiation decoding (as formalised above) can be solved in polynomial-time if and only if $\textsc{Uhlmann} \in \mathsf{avgUnitaryBQP}$.

1.4 Summary and future directions

Computational tasks with quantum inputs and/or outputs are ubiquitous throughout quantum information processing. The traditional framework of complexity theory, which is focused on computational tasks with classical inputs and outputs, cannot naturally capture the complexity of these "fully quantum" tasks.

In this paper we introduce a framework to reason about the computational complexity of unitary synthesis problems. We then use this framework to study Uhlmann's theorem through an algorithmic lens, i.e. to study the complexity of Uhlmann transformations. We prove that variants of the Uhlmann Transformation Problem are complete for some unitary complexity classes, and then explore relationships between the Uhlmann Transformation Problem and computational tasks in quantum cryptography, quantum Shannon theory, and high energy physics.

The study of the complexity of state transformation tasks is a very new field and we hope that our formal framework of unitary complexity theory and our findings about the Uhlmann Transformation Problem provide a useful starting point for a rich theory of the complexity of "fully quantum" problems. Many questions in this direction have yet to be explored. Throughout this paper, we have included many concrete open problems, which we hope will spark future research in this new direction in complexity theory. Additionally, our work suggests some high-level, open-ended future directions to explore:

Populating the zoo. An important source of the richness of computational complexity theory is the variety of computational problems that are studied. For example, the class NP is so interesting because it contains many complete problems that are naturally studied across the sciences [Pap97], and the theory of NP-completeness gives a unified way to relate them to each other.

Similarly, a fully quantum complexity theory should have its own zoo of problems drawn from a diverse range of areas. We have shown that core computational problems in quantum cryptography, quantum Shannon theory, and high energy physics can be related to each other through the language of unitary complexity theory. What are other natural problems in e.g. quantum error-correction, quantum metrology, quantum chemistry, or condensed matter physics, and what can we say about their computational complexity?

The crypto angle. Complexity and cryptography are intimately intertwined. Operational tasks in cryptography have motivated models and concepts that have proved indispensible in complexity theory (such as pseudorandomness and zero-knowledge proofs), and conversely complexity theory has provided a rigorous theoretical foundation to study cryptographic hardness assumptions.

We believe that there can be a similarly symbiotic relationship between quantum cryptography and a fully quantum complexity theory. Recent quantum cryptographic primitives such as quantum pseudorandom states [JLS18] or one-way state generators [MY22] are unique to the quantum setting, and the relationships between them are barely understood. For example, an outstanding question is whether there is a meaningful *minimal hardness assumption* in quantum cryptography, just like one-way functions are in classical cryptography. Can a fully quantum complexity theory help answer this question about minimal quantum cryptographic assumptions, or at least provide some guidance? For example, there are many beautiful connections between one-way functions, average-case complexity, and Kolomogorov complexity [IL89, Imp95, LP20]. Do analogous results hold in the fully quantum setting?

The learning theory angle. Quantum learning theory has also seen rapid development, particularly on the topic of quantum state learning [Aar07, HKP20, BO21, AA24]. Learning quantum states or quantum processes can most naturally be formulated as tasks with quantum inputs. Traditionally these tasks have been studied in the information-theoretic setting, where sample complexity is usually the main measure of interest. However we can also study the computational difficulty of learning quantum objects. What does a complexity theory of quantum learning look like?

Traditional versus fully quantum complexity theory. While traditional complexity theory appears to have difficulty reasoning about fully quantum tasks, can we obtain *formal* evidence that the two theories are, in a sense, independent of each other? For example, can we show that $\mathsf{P} = \mathsf{PSPACE}$ does not imply $\mathsf{unitaryBQP} = \mathsf{unitaryPSPACE}$? One would likely have to show this in a *relativized* setting, i.e., exhibit an oracle O relative to which $\mathsf{P}^O = \mathsf{PSPACE}^O$ but $\mathsf{unitaryBQP}^O \neq \mathsf{unitaryPSPACE}^O$. Another way would be to settle Aaronson and Kuperberg's "Unitary Synthesis Problem" [AK07] in the negative; see [LMW23] for progress on this. Such results would give compelling evidence that the reasons for the hardness of unitary transformations are intrinsically different than the reasons for the hardness of a Boolean function. More generally, what are other ways of separating traditional from fully quantum complexity theory?

Guide for readers

Although the paper is rather long, the material is organized in a way that supports random-access reading – depending on your interests, it is not necessary to read Section X before reading Section $X + 1$. All sections depend on the basic definitions of unitary complexity theory (Section 3) and the basic definitions of the Uhlmann Transformation Problem (Section 5). From then on, it's choose-your-own-adventure. If you are interested in:

- **Structural results about the complexity of UHLMANN**. Read Sections 4, 6 and 7.
- **Quantum cryptography**. Read Section 8. It may be helpful to review the definitions of quantum interactive protocols (Sections 2 and 4).
- **Quantum Shannon theory**. Read Section 9. It may be helpful to read the section on quantum commitments (Section 8.1).
- **Quantum gravity**. Read Section 10. It may be helpful to read the section on the Decodable Channel Problem (Section 9.1).

Acknowledgments

We thank Anurag Anshu, Lijie Chen, Andrea Coladangelo, Sam Gunn, Yunchao Liu, Joe Renes, Renato Renner, and Mehrdad Tahmasbi for helpful discussions. We thank Fred Dupuis for his help with understanding the decoupling results in his thesis. We are especially grateful to William Kretschmer, Fermi Ma, and John Wright for their thorough discussions on the first draft of the paper. We also thank Tomoyuki Morimae for their helpful comments on a preliminary version of this work. We thank anonymous conference reviewers for their helpful feedback. JB and HY are supported by AFOSR award FA9550-21-1-0040, NSF CAREER award CCF-2144219, and the Sloan Foundation. TM acknowledges support from SNSF Project Grant No. 200021_188541 and AFOSR-Grant No. FA9550-19-1-0202. AP is partially supported by AFOSR YIP (award number FA9550-16-1-0495), the Institute for Quantum Information and Matter (an NSF Physics Frontiers Center; NSF Grant PHY-1733907) and by a grant from the Simons Foundation (828076, TV). LQ is supported by DARPA under Agreement No. HR00112020023. We thank the Simons Institute for the Theory of Computing, where some of this work was conducted.

2 Preliminaries

2.1 Notation

For a bit string $x \in \{0,1\}^*$, we denote by $|x|$ its length (not its Hamming weight). When x describes an instance of a computational problem, we will often use $n = |x|$ to denote its size.

A function $\delta : \mathbb{N} \to [0,1]$ is an *inverse polynomial* if there exists a polynomial p such that $\delta(n) \leq 1/p(n)$ for all sufficiently large n. A function $\epsilon : \mathbb{N} \to [0,1]$ is *negligible* if for every polynomial p, for all sufficiently large n we have $\epsilon(n) \leq 1/p(n)$. **Henry: added (March 31, 2025):** Furthermore for convenience we also assume (unless otherwise stated) all polynomials and error functions are *monotonic*, i.e., for polynomials p we assume that $p(n+1) \geq p(n)$ for all n and for error functions $\epsilon : \mathbb{N} \to [0,1]$ we have $\epsilon(n+1) \leq \epsilon(n)$. When we talk about polynomial or negligible functions with multiple arguments (e.g., $\mathrm{poly}(n,r)$ or $\mathrm{negl}(n,r)$), we mean that it is a polynomial or negligible function in the *sum* of the two arguments (i.e., $\mathrm{poly}(n,r) = \mathrm{poly}(n+r)$ and $\mathrm{negl}(n,r) = \mathrm{negl}(n+r)$). **Tony: not super important, but why the sum rather than just plain multivariate polynomials? Henry: I want the property that keeping either n or r fixed, and letting the other grow, will make the polynomial grow. the multivariate definition doesn't have this property.**

A *register* R is a named finite-dimensional complex Hilbert space. If $\mathsf{A}, \mathsf{B}, \mathsf{C}$ are registers, for example, then the concatenation ABC denotes the tensor product of the associated Hilbert spaces. We abbreviate the tensor product state $|0\rangle^{\otimes n}$ as $|0^n\rangle$. For a linear transformation L and register R, we write L_{R} to indicate that L acts on R, and similarly we write ρ_{R} to indicate that a state ρ is in the register R. We write $\mathrm{Tr}(\cdot)$ to denote trace, and $\mathrm{Tr}_{\mathsf{R}}(\cdot)$ to denote the partial trace over a register R.

We denote the set of linear transformations on R by $\mathrm{L}(\mathsf{R})$, and linear transformations from R to another register S by $\mathrm{L}(\mathsf{R}, \mathsf{S})$. We denote the set of positive semidefinite operators on a register R by $\mathrm{Pos}(\mathsf{R})$. The set of density matrices on R is denoted $\mathrm{S}(\mathsf{R})$. For a pure state $|\varphi\rangle$, we write φ to denote the density matrix $|\varphi\rangle\langle\varphi|$. We denote the identity transformation by id. For an operator $X \in \mathrm{L}(R)$, we define $\|X\|_\infty$ to be its operator norm, and $\|X\|_1 = \mathrm{Tr}(|X|)$ to denote its trace norm, where $|X| = \sqrt{X^\dagger X}$. We write $\mathrm{td}(\rho,\sigma) = \frac{1}{2}\|\rho - \sigma\|_1$ to denote the trace distance between two density matrices ρ, σ, and $\mathrm{F}(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$ for the fidelity between ρ, σ.[9] Throughout the paper we frequently invoke the following relationship between fidelity and trace distance:

Proposition 2.1 (Fuchs-van de Graaf inequalities)**.** For all density matrices ρ, σ acting on the same space, we have that

$$1 - \sqrt{\mathrm{F}(\rho,\sigma)} \leq \mathrm{td}(\rho,\sigma) \leq \sqrt{1 - \mathrm{F}(\rho,\sigma)}\,.$$

A *quantum channel* from register A to B is a completely positive and trace-preserving (CPTP) map from $\mathrm{L}(\mathsf{A})$ to $\mathrm{L}(\mathsf{B})$. For simplicity, we often write $\mathcal{N} : \mathsf{A} \to \mathsf{B}$ instead of $\mathcal{N} : \mathrm{L}(\mathsf{A}) \to \mathrm{L}(\mathsf{B})$ when it is clear that $\mathcal{N}$ is a channel. We denote the set of quantum channels as $\mathsf{CPTP}(\mathsf{A}, \mathsf{B})$. We also call a channel a *superoperator*. For a channel Φ, we write $\mathrm{supp}(\Phi)$ to denote the number of qubits it takes as input. We call a channel unitary (resp. isometric) if it conjugates its input state with a unitary (resp. isometry). The diamond norm of a channel $\Phi \in \mathsf{CPTP}(\mathsf{A}, \mathsf{B})$ is defined as $\|\Phi\|_\diamond = \max_\rho \|(\Phi \otimes \mathrm{id}_{\mathsf{C}})(\rho)\|_1$ where the maximization is over all density matrices $\rho \in \mathsf{S}(\mathsf{A} \otimes \mathsf{C})$ where C is an arbitrary register.

Another important type of quantum operation is a *measurement*. In general a quantum measurement is described by a finite set of positive semidefinite matrices $\mathcal{M} = \{M_i\}_i$ satisfying $\sum_i M_i = \mathrm{id}$. Performing a measurement on a state ρ results in outcome i with probability $\mathrm{Tr}[M_i \rho]$. Conditioned on outcome i, the post-measurement state is

$$\rho|_{M_i} = \frac{\sqrt{M_i}\rho\sqrt{M_i}}{\mathrm{Tr}(M_i \rho)}\,. \tag{2.1}$$

The gentle measurement lemma is an important property about quantum measurements that connects the trace distance between a state and its post-measurement state to the probability that the measurement accepts.

[9] We note that in the literature there are two versions of fidelity that are commonly used; here we use the *squared* version of it.

Proposition 2.2 (Gentle Measurement lemma)**.** Let ρ be a density matrix and Λ be a positive semidefinite Hermitian matrix. If $\mathrm{Tr}[\Lambda\rho] \geq 1-\epsilon$, then $\mathrm{F}(\rho, \rho|_\Lambda) \geq 1-\epsilon$ and $\|\rho - \rho|_\Lambda\|_1 \leq 2\sqrt{\epsilon}$.

A proof of this can be found in, e.g., [Wil17, Lemma 9.4.1].

2.2 Partial isometries and channel completions

Usually, operations on a quantum state can be described by a unitary matrix, an isometry (if new qubits are introduced), or more generally a quantum channel (if one allows incoherent operations such as measuring or discarding qubits). However, we will find it useful to consider operations whose action is only defined on a certain subspace. Outside of this "allowed subspace" of input states, we do not want to make a statement about how the operation changes a quantum state. Such operations can be described by partial isometries.

Definition 2.3 (Partial isometry)**.** A linear map $U \in \mathrm{L}(\mathsf{A}, \mathsf{B})$ is called a partial isometry if there exists a projector $\Pi \in \mathrm{L}(\mathsf{A})$ and an isometry $\tilde{U} \in \mathrm{L}(\mathsf{A}, \mathsf{B})$ such that $U = \tilde{U}\Pi$. We call the image of the projector Π the *support* of the partial isometry U.

Of course in practice we cannot implement a partial isometry because it is not a trace-preserving operation, as states in the orthogonal complement of the support are mapped to the 0-vector. We therefore define a *channel completion* of a partial isometry as any quantum channel that behaves like the partial isometry on its support, and can behave arbitrarily on the orthogonal complement of the support.

Definition 2.4 (Channel completion)**.** Let $U \in \mathrm{L}(\mathsf{A}, \mathsf{B})$ be a partial isometry. A *channel completion of* U is a quantum channel $\Phi \in \mathsf{CPTP}(\mathsf{A}, \mathsf{B})$ such that for any input state $\rho \in \mathrm{S}(\mathsf{A})$,

$$\Phi(\Pi\rho\Pi) = U\rho U^\dagger \,,$$

where $\Pi \in \mathrm{L}(\mathsf{A})$ is the projector onto the support of U. If Φ is a unitary or isometric channel, we also call Φ a *unitary* or *isometric completion* of the partial isometry.

An ϵ*-error channel completion of* U is a quantum channel $\tilde{\Phi}$ that is ϵ-close in diamond norm to a channel completion Φ of U.

2.3 Quantum circuits

For convenience we assume that all quantum circuits use gates from the universal gate set $\{H, \mathit{CNOT}, T\}$ [NC10, Chapter 4] (although our results hold for any universal gate set consisting of gates with algebraic entries). A *unitary quantum circuit* is one that consists only of gates from this gate set. A *general quantum circuit* is a quantum circuit that can additionally have non-unitary gates that (a) introduce new qubits initialized in the zero state, (b) trace them out, or (c) measure them in the standard basis. We say that a general quantum circuit has size s if the total number of gates is at most s. We say that a general quantum circuit uses space s if the number of qubits involved at every time step of the computation is at most s. The description of a general quantum circuit is a sequence of gates (unitary or non-unitary) along with a specification of which qubits they act on. A general quantum circuit C implements a quantum channel; we will abuse notation slightly and also use C to denote the channel. For a unitary quantum circuit C we will write $|C\rangle$ to denote the state $C|0\ldots0\rangle$.

Definition 2.5 (Polynomial-size and polynomial-space circuit families)**.** A family of general quantum circuits $(C_{x,r})_{x\in\{0,1\}^*, r\in\mathbb{N}}$ has *polynomial-size* (resp. *polynomial-space*) if there exists a polynomial p such that $C_{x,r}$ has size (resp. uses space) at most $p(|x|, r)$.

The reason circuit families are indexed by a pair (x, r) is because in our unitary complexity theory framework, algorithms get both an *instance* $x \in \{0,1\}^n$, which is a string that specifies *which* state transformation to implement, and a *precision parameter* $r \in \mathbb{N}$, which specifies *how accurately* to implement the state transformation. The complexity of the circuit family is measured as a function of the length $|x|$ and the precision parameter r. The formal sense in which r is a precision parameter will become clear when we define the notion of unitary synthesis problems in Section 3.

Remark 2.6. Sometimes we work with circuit families $\{C_x\}_{x\in\{0,1\}^*}$ that are *not* indexed by a precision parameter r (e.g., the precision may be fixed). In that case, we say that the family has polynomial size if C_x has size $\mathrm{poly}(|x|)$.

Definition 2.7 (Uniform circuit families)**.** A family of general polynomial-size (resp. polynomial-space) quantum circuits $(C_{x,r})_{x\in\{0,1\}^*, r\in\mathbb{N}}$ is called *time-uniform* (resp. *space-uniform*) if there exists a classical polynomial-time (resp. polynomial-space) Turing machine that on input $(x, 1^r)$ outputs the description of $C_{x,r}$,[10] where 1^r means r written in unary. For brevity, we use *uniform* to mean *time-uniform*. We call a time-uniform (resp. space-uniform) family of quantum circuits a *polynomial-time quantum algorithm* (resp. *polynomial-space quantum algorithm*).

Finally, it is occasionally useful to defer measurements in a circuit and consider its unitary purification:

Definition 2.8 (Unitary purification of a general quantum circuit)**.** A *unitary purification* (or *dilation*) of a general quantum circuit C is a unitary circuit $\tilde{C}$ formed by performing all measurements in C coherently (with the help of additional ancillas) and not tracing out any qubits.

The following proposition relates a general quantum circuit to its unitary purification; it follows directly from the definition of the unitary purification. This proposition also demonstrates that the unitary purification $\tilde{C}$ of a general quantum circuit C is a specific *Stinespring dilation* of the quantum channel corresponding to C.

Proposition 2.9. Let C be a size-m general quantum circuit acting on n qubits, and let $\tilde{C}$ be a unitary purification. Let register R denote all the qubits that are traced out in the original circuit C as well as the ancilla qubits introduced for the purification. Then for all states ρ,

$$C(\rho) = \mathrm{Tr}_{\mathsf{R}}(\tilde{C}\,\rho\tilde{C}^\dagger)\,.$$

Furthermore, $\tilde{C}$ acts on at most $n + m$ qubits and has size at most m.

Remark 2.10. Throughout this paper, whenever we refer to a family of quantum circuits $(C_{x,r})_{x,r}$, we mean a *general* family (i.e., non-unitary operations are allowed).

2.4 Quantum interactive protocols

We present the model of quantum interactive protocols. (For a more in-depth account we refer the reader to the survey of Vidick and Watrous [VW16].) Since in quantum computing the standard model of computation is the quantum circuit model (rather than quantum Turing machines), we model the verifier in a quantum interactive protocol as a sequence of *verifier circuits*, one for each input length. A verifier circuit is itself a

[10] We adopt the convention that the output tape of a Turing machine is write-only, and does not contribute to the space usage of the Turing machine. Thus a polynomial-space Turing machine can output an exponentially-long string.

tuple of quantum circuits that correspond to the operations performed by the verifier in each round of the protocol.

More formally, a *k-round quantum verifier circuit* $C = (C_j)_{j \in [k]}$ is a tuple of general quantum circuits that each act on a pair of registers (V, M). The circuit C_j should be thought of as the verifier's actions in the j-th round of the protocol. The register V is further divided into disjoint sub-registers $(\mathsf{V}_{\mathsf{work}}, \mathsf{V}_{\mathsf{flag}}, \mathsf{V}_{\mathsf{out}})$. The register $\mathsf{V}_{\mathsf{work}}$ is the verifier circuit's "workspace", the register $\mathsf{V}_{\mathsf{flag}}$ is a single qubit indicating whether the verifier accepts or rejects, and the register $\mathsf{V}_{\mathsf{out}}$ holds the verifier's output (if applicable). The register M is the message register. The size of a verifier circuit C is the sum of the circuit sizes of the C_j's.

A *quantum prover P* for a verifier circuit C is a unitary that acts on M as well as a disjoint register P. Note that we could also define the prover to be a collection of unitaries, one for each round, in analogy to the verifier; the two definitions are equivalent since we can always combine the single-round unitaries into a larger unitary that keeps track of which round is being executed and applies the corresponding single-round unitary. Since we will rarely deal with prover unitaries for individual rounds, we will find it more convenient to just treat the prover as one large unitary. Furthermore, since the prover register is of unbounded size, we can assume without loss of generality that the prover applies a unitary (rather than a quantum channel).

Let $|\psi\rangle$ denote a quantum state whose size is at most the number of qubits in $\mathsf{V}_{\mathsf{work}}$. We write $C(|\psi\rangle) \leftrightarrows P$ to denote the interaction between the verifier circuit C and the prover P on input $|\psi\rangle$, which is defined according to the following process. The initial state of the system is $|\phi_0\rangle = |\psi, 0 \cdots 0\rangle_{\mathsf{V}_{\mathsf{work}}} |0 \cdots 0\rangle_{\mathsf{V}_{\mathsf{flag}}\mathsf{V}_{\mathsf{out}}\mathsf{MP}}$. Inductively define $|\phi_i\rangle = P |\phi_{i-1}\rangle$ for odd $i \leq 2k$, and $|\phi_i\rangle = C_{i/2} |\phi_{i-1}\rangle$ for even $i \leq 2k$. We say that $C(|\psi\rangle) \leftrightarrows P$ accepts (resp. rejects) if measuring the register $\mathsf{V}_{\mathsf{flag}}$ in the state $|\phi_{2k}\rangle$ in the standard basis yields the outcome 1 (resp. 0). We say that the *output of $C(|\psi\rangle) \leftrightarrows P$ conditioned on accepting* is the density matrix

$$\frac{\mathrm{Tr}_{\mathsf{VMP} \setminus \mathsf{V}_{\mathsf{out}}} \left(|1\rangle\langle 1|_{\mathsf{V}_{\mathsf{flag}}} \cdot \phi_{2k} \right)}{\mathrm{Tr} \left(|1\rangle\langle 1|_{\mathsf{V}_{\mathsf{flag}}} \cdot \phi_{2k} \right)} \,;$$

in other words, it is the reduced density matrix of $|\phi_{2k}\rangle$ on register $\mathsf{V}_{\mathsf{out}}$, conditioned on $C(|\psi\rangle) \leftrightarrows P$ accepting. (If the probability of accepting is 0, then we leave the output undefined.)

A *quantum verifier* $V = (V_{x,r})_{x \in \{0,1\}^*, r \in \mathbb{N}}$ is a time-uniform sequence of polynomial-size and polynomial-round quantum verifier circuits. As in Definition 2.5, the index x should be thought of as the instance, i.e., which unitary the verifier is trying to implement using the interactive protocol, and $1/r$ is the precision parameter, i.e., to within what error the verifier implements the desired unitary; see e.g. Definition 4.1 for an example of how these parameters are used formally.

2.5 Quantum state complexity classes

Here we present the definitions of some state complexity classes that were introduced in [RY22]. Intuitively, they are classes of sequences of quantum states that require certain resources to be synthesized (e.g., polynomial time or space).

Definition 2.11 (stateBQP, statePSPACE)**.** The class stateBQP (resp. statePSPACE) is the set of all sequences of density matrices $(\rho_x)_{x \in \{0,1\}^*}$ such that there exists a time-uniform polynomial-size (resp. space-uniform polynomial-space) family of general quantum circuits $(C_{x,r})_{x \in \{0,1\}^*, r \in \mathbb{N}}$, where $C_{x,r}$ takes no inputs, and for every $x \in \{0,1\}^*$ and $r \in \mathbb{N}$, the output $\sigma_{x,r}$ of $C_{x,r}$ satisfies

$$\mathrm{td}(\sigma_{x,r}, \rho_x) \leq \frac{1}{r} \,.$$

We also present the class of states that can be synthesized by an efficient verifier interacting with an all-powerful prover:

Definition 2.12 (stateQIP)**.** Let $c, s : \mathbb{N} \times \mathbb{N} \to [0,1]$ be functions. The class $\mathsf{stateQIP}_{c,s}$ is the set of state sequences $(\rho_x)_{x \in \{0,1\}^*}$ where there exists a time-uniform polynomial-time quantum verifier $V = (V_{x,r})_{x \in \{0,1\}^*, r \in \mathbb{N}}$ such that for all $x \in \{0,1\}^*$ and $r \in \mathbb{N}$:

- *Completeness:* There exists a quantum prover P^* (called an *honest prover*) such that

$$\Pr[V_{x,r} \leftrightarrows P^* \text{ accepts}] \geq c(|x|, r) \, .$$

- *Soundness:* For all quantum provers P, it holds that

$$\text{if} \quad \Pr[V_{x,r} \leftrightarrows P \text{ accepts}] \geq s(|x|, r) \qquad \text{then} \qquad \mathrm{td}(\sigma, \rho_x) \leq \frac{1}{r} \, ,$$

  where σ denotes the output of $V_{x,r} \leftrightarrows P$ conditioned on accepting.

Here the probabilities are over the randomness of the interaction, assuming the verifier starts with the all-zero input state.

Finally, define

$$\mathsf{stateQIP} = \bigcup_{\epsilon(n) \text{ negl}} \mathsf{stateQIP}_{1-\epsilon, \frac{1}{2}}$$

where the union is over all negligible functions $\epsilon(n, r)$. The choice of $s = \frac{1}{2}$ is without loss of generality; [RY22, Lemma 4.4] shows that the soundness parameter can made exponentially small.

The main results of [RY22, MY23] combined imply the following state synthesis analogue of the famous $\mathsf{QIP} = \mathsf{IP} = \mathsf{PSPACE}$ theorem in traditional complexity theory [Sha92, LFKN92, JJUW11]:

Theorem 2.13 ([RY22, MY23])**.** $\mathsf{stateQIP} = \mathsf{statePSPACE}$.

This theorem will be used as a "subroutine" in our characterization of avgUnitaryQIP and avgUnitaryPSPACE in Section 7.

Remark 2.14. We discuss two refinements in our definitions of state complexity classes compared to [RY22, MY23]. These modifications do not impact Theorem 2.13 and readers unfamiliar with [RY22, MY23] may safely skip this discussion.

Firstly, the state sequences in [RY22, MY23] are indexed by natural numbers $n \in \mathbb{N}$, rather than strings $x \in \{0,1\}^*$. The results in [RY22, MY23] can be easily adapted to hold for state sequences indexed by strings; complexity measures are then functions of the length of x. Consider the containment $\mathsf{statePSPACE} \subseteq \mathsf{stateQIP}$; instead of the stateQIP verifier receiving n as input to specify the state ρ_n to synthesize as in [RY22], the verifier now receives x to specify the state ρ_x. For the reverse containment $\mathsf{stateQIP} \subseteq \mathsf{statePSPACE}$, instead of the statePSPACE algorithm receiving n as input to specify ρ_n, it instead receives x as input to specify the state ρ_x.

Secondly, the state complexity classes in [RY22, MY23] are all parameterized by an error function δ; for example $\mathsf{stateBQP}_\delta$ was defined, where $\delta(n)$ is a function describing the closeness of the output to the target state. Without the δ subscript, the class stateBQP is defined to be the intersection over $\mathsf{stateBQP}_\delta$ for all inverse polynomials $\delta(n) = 1/p(n)$. (The classes $\mathsf{stateQIP}, \mathsf{statePSPACE}$ in [RY22, MY23] are also defined similarly with respect to some error parameter δ).

In this paper we define state (and unitary) complexity classes slightly differently when it comes to the error parameterization. We now insist that an algorithm or verifier that synthesizes a state family $(\rho_x)_x$ must, in addition to a string $x \in \{0,1\}^*$, also take in a parameter $r \in \mathbb{N}$ as input, which controls how close the output is to ρ_x. That is, the algorithm/verifier must be able to approximate the state family $(\rho_x)_x$ arbitrarily well, potentially at the cost of more running time (or more space). For $\mathsf{stateBQP}$ (resp. $\mathsf{statePSPACE}$) specifically, the running time (resp. space usage) of the algorithm must scale as $\mathrm{poly}(|x|, \frac{1}{\epsilon})$ where ϵ is the desired approximation error.

The definitions given in [RY22, MY23] technically allow a different algorithm for every error function δ, and only require algorithms for inverse polynomial error (but not necessarily for inverse exponential error). In these revised definitions we insist on a *single uniform algorithm* that can handle all error ranges, which is arguably more natural, as we discuss below Definition 3.2.

Part I
Unitary Complexity Theory

3 Unitary Synthesis Problems and Unitary Complexity Classes

To be able to make formal statements about the complexity of quantum tasks, we present a framework for unitary complexity theory: we define unitary synthesis problems, algorithms for implementing them, unitary complexity classes, and reductions between unitary synthesis problems.

Defining these concepts for unitaries is more subtle than in the classical world. First, a unitary synthesis problem requires both a classical *instance* specifying which unitary we are interested in and a quantum input to which that unitary is supposed to be applied. Secondly, we need to allow approximation errors when implementing unitaries. Finally, we will want to consider unitary versions of promise problems, which are most naturally formalized by partial isometries; these are not physical operations, so we will frequently talk about all physical instantiations (formally, channel completions) of these partial isometries.

The definitions presented in this section should be viewed as our current best understanding of conceptually clean yet practically useful definitions, but new results, e.g., on error amplification, may provide reasons to adapt these definitions in the future. In Section 3.6 we provide additional discussion of the choices we made in our definitions.

3.1 Unitary synthesis problems

In traditional complexity theory, decision problems are formalized as *languages*, which are sets of binary strings. The analogue in our framework is the following formalization of unitary synthesis problems.

Definition 3.1 (Unitary synthesis problem)**.** A *unitary synthesis problem* is a sequence $\mathscr{U} = (U_x)_{x\in\{0,1\}^*}$ of partial isometries.[11]

We note that Definition 3.1 considers partial isometries, not only unitaries (which are of course the special case of partial isometries for which the projector in Definition 2.3 is $\Pi = \mathrm{id}$). A partial isometry is essentially a unitary defined on some subspace. This is analogous to the idea of a "promise" on the inputs in traditional complexity theory: the partial isometry only specifies the state transformation task on input states coming from a "promised subspace". For inputs with support on the orthogonal complement to this promised subspace, the behavior of the state transformation is not specified.

One should think of a unitary synthesis problem $\mathscr{U}$ as specifying, for each string $x \in \{0,1\}^*$ (called the *instance*), a state transformation task U_x to be performed on some quantum system (called the *quantum input*). How the instance x specifies such a task varies from problem to problem; we give some examples of unitary synthesis problems below.

1. (*Hamiltonian time evolution*) Consider some natural string encoding of pairs (H,t) where H is a local Hamiltonian and t is a real number: the encoding will specify the number of qubits that H acts on as well as each local term of H. If x is a valid encoding of such a pair (H,t), then define $U_x = e^{-iHt}$. Otherwise, define $U_x = 0$ (i.e., to be the zero map, which is a partial isometry). Then we define $\textsc{TimeEvolution} = (U_x)_{x\in\{0,1\}^*}$.

[11] We note that while unitary synthesis problems are not necessarily sequences of unitaries, we believe that it is a better name than "partial isometry synthesis problem".

2. (*Decision languages*) Let $L \subseteq \{0,1\}^*$ be a decision language. Define $\textsc{UnitaryDecider}_L = (U_x)_{x \in \{0,1\}^*}$ as follows: if $x = 1^n$ (i.e. x is the unary representation of an integer $n \in \mathbb{N}$), then the unitary $U_{1^n} = U_x$ acts on $n+1$ qubits and for all $y \in \{0,1\}^n, b \in \{0,1\}$, we define $U_{1^n} |y\rangle |b\rangle = |y\rangle |b \oplus L(y)\rangle$ where $L(y) = 1$ iff $y \in L$. If x is not a unary encoding of an integer, then we define $U_x = 0$.

3. (*Ground state preparation*) Consider a natural string encoding local Hamiltonians. If x is an encoding of a local Hamiltonian with a unique ground state $|\psi_x\rangle$, then let $U_x = |\psi_x\rangle\langle 0 \cdots 0|$; otherwise let $U_x = 0$. The unitary synthesis problem $\mathscr{U} = (U_x)_{x \in \{0,1\}^*}$ corresponds to the task of preparing (starting with the all zeroes state) the unique ground state of the Hamiltonian encoded by x; the "promised subspace" here consists only of the all zeroes state.

We now define what it means to *implement* a unitary synthesis problem.

Definition 3.2 (Worst-case implementation of unitary synthesis problems)**.** Let $\mathscr{U} = (U_x)_{x \in \{0,1\}^*}$ denote a unitary synthesis problem. Let $C = (C_{x,r})_{x \in \{0,1\}^*, r \in \mathbb{N}}$ denote a family of quantum circuits. We say that C *is a worst-case implementation of* $\mathscr{U}$ if for all $x \in \{0,1\}^*$, for all $r \in \mathbb{N}$, there exists a channel completion $\Phi_{x,r}$ of U_x such that

$$\Big\| C_{x,r} - \Phi_{x,r} \Big\|_\diamond \leq \frac{1}{r} ,$$

where $\| \cdot \|_\diamond$ denotes the diamond norm[12].

This definition also clarifies the sense in which we can think of the subscript r in $C_{x,r}$ as a desired approximation error.

Intuitively, an implementation of a unitary synthesis problem is just a sequence of general quantum circuits that approximately implement the corresponding partial isometries. We call Definition 3.2 a *worst-case implementation* because $C_{x,r}$ has to approximate the partial isometry (more precisely, any channel completion) in diamond distance, which means that $C_{x,r}$ and $\Phi_{x,r}$ have to behave the same *on all quantum inputs*. We note two subtleties:

1. We require that the circuit $C_{x,r}$ is close to *some* channel completion $\Phi_{x,r}$ of U_x because $C_{x,r}$ is only required to behave like U_x on the support of U_x, and can behave arbitrarily on states orthogonal to the support (in a way that may depend arbitrarily on x and r). This is analogous to classical promise problems, where a Turing machine deciding the promise problem is allowed to behave arbitrarily on inputs violating the promise, i.e., the Turing machine is only required to implement *some* function that agrees with the promise problem on inputs fulfilling the promise.

2. This definition provides, for every instance $x \in \{0,1\}^*$ and $\epsilon > 0$, a circuit $C_{x,r}$ that implements U_x with error ϵ, for $r = O(1/\epsilon)$. Thus an algorithm for implementing a unitary synthesis problem has to be able to achieve arbitrarily small error. This captures the notion that the unitary synthesis problem $(U_x)_x$ must be *algorithmically implementable*.

3.2 Distributional unitary synthesis problems

We also define a notion of *distributional (or average-case) unitary synthesis problems*. Here, in addition to a partial isometry, we also specify a state and a register of this state on which the partial isometry is going

[12] Recall that a small diamond distance between two channels means that the channels are difficult to distinguish even if the channels are applied to an entangled state.

to act; note, however, that this is very different from a state synthesis problem, as we discuss in Remark 3.7. We first give the formal definition and then explain why this is a reasonable notion of a distributional unitary synthesis problem.

Definition 3.3 (Distributional unitary synthesis problem)**.** We say that a pair $(\mathscr{U}, \Psi)$ is a *distributional unitary synthesis problem* if $\mathscr{U} = (U_x)_x$ is a unitary synthesis problem with $U_x \in \mathrm{L}(\mathsf{A}_x, \mathsf{B}_x)$ for some registers $\mathsf{A}_x, \mathsf{B}_x$, and $\Psi = (|\psi_x\rangle)_x$ is a family of bipartite pure states on registers $\mathsf{A}_x\mathsf{R}_x$. We call $|\psi_x\rangle$ the *distribution state* with *target register* A_x and *ancilla register* R_x.

Definition 3.4 (Average-case implementation of distributional unitary synthesis problems)**.** Let $(\mathscr{U}, \Psi)$ denote a distributional unitary synthesis problem, where $\mathscr{U} = (U_x)_x$ and $\Psi = (|\psi_x\rangle)_x$. Let $C = (C_{x,r})_{x\in\{0,1\}^*, r\in\mathbb{N}}$ denote a family of quantum circuits, where $C_{x,r}$ implements a channel whose input and output registers are the same as those of U_x for all $r \in \mathbb{N}$. We say that C *is an average-case implementation of* $(\mathscr{U}, \Psi)$ if for all $x \in \{0,1\}^*$ and $r \in \mathbb{N}$, there exists a channel completion $\Phi_{x,r}$ of U_x such that

$$\mathrm{td}\Big((C_{x,r} \otimes \mathrm{id})(\psi_x),\, (\Phi_{x,r} \otimes \mathrm{id})(\psi_x)\Big) \leq \frac{1}{r}\,,$$

where the identity channel acts on the ancilla register of $|\psi_x\rangle$.

Remark 3.5. The term "distributional" may seem a bit odd at first; for example, where is the distribution in Definition 3.3? In classical average-case complexity theory, a distributional problem is one where the inputs are sampled from some probability distribution $\mathcal{D}$. The state family $\Psi = (|\psi_x\rangle)_x$ in a distributional unitary synthesis problem $(\mathscr{U}, \Psi)$ can be viewed as a *purification* of a distribution over pure states: by the Schmidt decomposition, we can always write

$$|\psi_x\rangle = \sum_j \sqrt{p_{x,j}}\, |\phi_{x,j}\rangle \otimes |j\rangle \tag{3.1}$$

for orthonormal states $\{|\phi_{x,j}\rangle\}_j$ on A_x and $\{|j\rangle\}_j$ on R_x. The Schmidt coefficients $\{p_{x,j}\}_j$ form a probability distribution $\mathcal{D}_x$, so $|\psi_x\rangle$ can be viewed as the purification of the distribution $\mathcal{D}_x$ over pure states $\{|\phi_{x,j}\rangle\}_j$. The condition of C implementing $(\mathscr{U}, \Psi)$ with average-case error implies the following: for all $x \in \{0,1\}^*$ and $r \in \mathbb{N}$ there exists a channel completion $\Phi_{x,r}$ of U_x such that

$$\mathop{\mathbb{E}}_{j\sim\mathcal{D}_x} \left[\mathrm{td}(C_{x,r}(\phi_{x,j}),\, \Phi_{x,r}(\phi_{x,j}))\right] \leq \frac{1}{r}\,. \tag{3.2}$$

This can be seen by applying a measurement in the Schmidt basis on the purifying register, which does not increase the trace distance in Definition 3.4. Looking ahead, we will find it more convenient to simply specify (for each x) one pure state $|\psi_x\rangle_{\mathsf{A}_x\mathsf{R}_x}$ instead of a set of pure states on A_x and a distribution over them.

Remark 3.6. Comparing Definition 3.2 and Definition 3.4, we see that we can also define worst-case implementations in terms of average-case implementations: a circuit family $C = (C_{x,r})_{x\in\{0,1\}^*, r\in\mathbb{N}}$ is a worst-case implementation for a unitary synthesis problem $\mathscr{U} = (U_x)_{x\in\{0,1\}^*}$ if and only if it is an average-case implementation of the distributional unitary synthesis problem $(\mathscr{U}, \Psi)$ for all state sequences $\Psi = (|\psi_x\rangle)_x$. This is because the diamond norm distance between two channels is equivalent to the maximum trace distance over all inputs (which can be, without loss of generality, a pure state if we include the purifying system).

Remark 3.7. Since an average-case unitary synthesis problem specifies both an input state $|\psi_x\rangle$ and a unitary U_x to be applied on that state, it may seem like this is equivalent to the state synthesis problem of preparing $U_x |\psi_x\rangle$. This, however, is not the case: the state $|\psi_x\rangle$ can be entangled across registers $\mathsf{A}_x\mathsf{R}_x$, but the unitary U_x is only allowed to act on A_x. Thus even if one could prepare copies of the pure state $(U_x \otimes \mathrm{id}) |\psi_x\rangle$ for free, one cannot necessarily efficiently transform $|\psi_x\rangle$ to $(U_x \otimes \mathrm{id}) |\psi_x\rangle$ by acting locally on a subsystem – there is the additional requirement that the output of the transformation task is correctly entangled with a reference register that the transformation cannot access.

3.3 Unitary complexity classes

A *unitary complexity class* is a collection of unitary synthesis problems. We introduce some natural unitary complexity classes by defining the unitary synthesis analogues of BQP and PSPACE, respectively.

Definition 3.8 ($\mathsf{unitaryBQP}$, $\mathsf{unitaryPSPACE}$)**.** Define the unitary complexity class $\mathsf{unitaryBQP}$ (resp. $\mathsf{unitaryPSPACE}$) to be the set of unitary synthesis problems $\mathscr{U} = (U_x)_x$ for which there exists a time-uniform polynomial-time (resp. polynomial-space) quantum algorithm $C = (C_{x,r})_{x,r}$ that is a worst-case implementation of $\mathscr{U}$.

Next we define classes of distributional unitary synthesis problems, the unitary complexity analogues of classical average case complexity classes.

Definition 3.9 ($\mathsf{avgUnitaryBQP}$, $\mathsf{avgUnitaryPSPACE}$)**.** Define the unitary complexity class $\mathsf{avgUnitaryBQP}$ (resp. $\mathsf{avgUnitaryPSPACE}$) to be the set of distributional unitary synthesis problems $(\mathscr{U}, \Psi)$ where $\Psi \in \mathsf{stateBQP}$ (resp. $\Psi \in \mathsf{statePSPACE}$) and there exists a polynomial-time (resp. polynomial-space) quantum algorithm C that implements $(\mathscr{U}, \Psi)$ with average-case error.

In our definition of $\mathsf{avgUnitaryBQP}$ and $\mathsf{avgUnitaryPSPACE}$, we require that the state sequence with respect to which the average case unitary synthesis problem is defined be in the corresponding state complexity class (i.e. $\mathsf{stateBQP}$ and $\mathsf{statePSPACE}$, respectively). We will follow this general pattern throughout the paper: whenever we define an average case unitary complexity class, we will require that the state sequence is in the corresponding state class (see e.g. Definition 4.5).

3.4 Reductions

Notions of reductions are crucial in complexity theory and theoretical computer science. We introduce a basic notion of reduction that allows us to relate one unitary synthesis problem to another. First, we formalize the notion of circuits that can make queries to a unitary synthesis oracle. Intuitively, a quantum circuit with access to a unitary synthesis oracle is just like a normal quantum circuit, except that it can apply some set of partial isometries (or more precisely arbitrary channel completions of partial isometries) in a single computational step by using the unitary synthesis oracle.

Definition 3.10 (Quantum query circuits)**.** A *quantum query circuit* C^* specifies a sequence of gates like those in a general quantum circuit (defined in Section 2.3), except it may also include special "oracle gates". An oracle gate is specified by a label $(y, s) \in \{0,1\}^* \times \mathbb{N}$; its action on its input qubits will be specified separately, i.e. a quantum query circuit is not actually a quantum circuit, but rather a *template* for a quantum circuit.

The label (y, s) of an oracle gate specifies both which instance y of a unitary synthesis problem will be inserted into the oracle gate and what implementation error $1/s$ we allow for the oracle gate.

Definition 3.11 (Instantiations of quantum query circuits)**.** An *instantiation* of a quantum query circuit $C^* = (C^*_{x,r})_{x,r}$ with a unitary synthesis problem $\mathscr{U}$, denoted by $C^{\mathscr{U}}$, is a sequence of quantum channels obtained by first fixing a worst-case implementation $(D_{y,s})_{y,s}$ of $\mathscr{U}$, and then replacing all the oracle gates in $C^*_{x,r}$ with labels $\ell = (y, s)$ by channels $D_{y,s}$. Whenever we write $C^{\mathscr{U}}$, we implicitly require that $\mathscr{U}$ is such that the input and output registers of U_y match the input and output registers of any oracle gate with label (y, s) in C^*.

Remark 3.12. In Definition 3.11 we leave implicit the dependence on which worst-case implementation of U_y the instantiation uses. This is we because we will always require that an oracle circuit works for all choices of channel completion: whenever we say that a statement holds for $C^{\mathscr{U}}$, we mean that it holds for all possible choices of worst-case implementation $(D_{y,s})_{y,s}$ of $\mathcal{U}$. This is analogous to classical oracle machines that have access to promise problems: in the classical case, such an oracle machine must work no matter how the oracle behaves on inputs outside the promise.

Remark 3.13. We note that our definition of quantum query circuit has the classical instances y "hardcoded" into the description of the circuit. In particular, the query circuit cannot choose which oracles it queries depending on its quantum input.[13] To accommodate situations when the oracle circuit may want to query different oracles $\mathscr{U} = (U_x)_x$ (perhaps even in superposition), one can define a "controlled oracle" $\tilde{U}_n = \sum_{x:|x|=n} |x\rangle\langle x| \otimes U_x$. In other words, $\tilde{U}_n$ applies the oracle U_x conditioned on some n-qubit register being in the state $|x\rangle$. A quantum query circuit with access to this controlled oracle can then apply different U_x coherently depending on its quantum input, i.e. the controlled oracle gives a query circuit more power than the uncontrolled one.

It will also be useful to define instantiations of quantum query circuits with distributional unitary synthesis problems. The only difference to Definition 3.11 is that the channels $D_{y,s}$ are now only required to be average-case implementations of some distributional unitary synthesis problem. We include a formal definition for completeness:

Definition 3.14 (Instantiations of query circuits with distributional unitary synthesis problems)**.** An instantiation of a quantum query circuit $C^* = (C^*_{x,r})_{x,r}$ with an average-case unitary synthesis problem $(\mathscr{U}, \Psi)$, denoted by $C^{(\mathscr{U},\Psi)}$, is a sequence of quantum channels obtained by first fixing an average-case implementation $(D_{y,s})_{y,s}$ of $(\mathscr{U}, \Psi)$, and then replacing all the oracle gates in $C^*_{x,r}$ with labels $\ell = (y, s)$ by channels $D_{y,s}$. Whenever we write $C^{(\mathscr{U},\Psi)}$, we implicitly require that $(\mathscr{U}, \Psi)$ is such that the input and output registers of U_y match the input and output registers of any oracle gate with label (y, s) in C^*.

Basic notions from "normal" circuits, like polynomial-size, naturally extend to query circuits. The one additional requirement is that a query circuit $C^*_{x,r}$ only uses oracle gates with labels y, s that are polynomially related to x, r:

Definition 3.15 (Polynomial-size query circuits)**.** A family $(C^*_{x,r})_{x\in\{0,1\}^*,r\in\mathbb{N}}$ of quantum query circuits has *polynomial-size* if there exists a polynomial p such that $C^*_{x,r}$ contains at most $p(|x|, r)$ gates and each oracle gate in $C^*_{x,r}$ is labelled by a tuple (y, s) satisfying $|y|, s \leq p(|x|, r)$.

Definition 3.16 (Time-uniform quantum query circuits)**.** A family $(C^*_{x,r})_{x\in\{0,1\}^*,r\in\mathbb{N}}$ of polynomial-size quantum query circuits is *time-uniform* (or just *uniform*) if there exists a classical polynomial-time Turing machine that on input $(x, 1^r)$ outputs the description of $C^*_{x,r}$. We call a time-uniform family of quantum query circuits a *polynomial-time quantum query algorithm*.

[13] Of course, for a family of query circuits $(C^*_{x,r})$, the labels (y, s) used by $C^*_{x,r}$ can depend on the index x; the point here is that a given $C^*_{x,r}$ cannot compute y as a function of the quantum input it is given.

Using quantum query circuits, we can define polynomial-time reductions between unitary synthesis problems. Intuitively, "$\mathscr{U}$ polynomial-time reduces to $\mathscr{V}$" means that $\mathscr{U}$ can be implemented efficiently if we have access to oracle gates that (approximately) implement channel completions of instances of $\mathscr{V}$.

Definition 3.17 (Polynomial-time reductions between unitary synthesis problems)**.** Let $\mathscr{U} = (U_x)_x$ and $\mathscr{V} = (V_x)_x$ denote unitary synthesis problems. Then $\mathscr{U}$ *polynomial-time reduces* to $\mathscr{V}$ if there exists a polynomial-time quantum query algorithm $C^* = (C^*_{x,r})_{x,r}$ such that $C^{\mathscr{V}}$ is a worst-case implementation of $\mathscr{U}$.

This notion of reduction readily extends to distributional problems, too. The only thing that changes is whether the oracle gates are instantiated with worst-case or average-case implementations, and whether the instantiated query circuit is required to be a worst-case or an average-case implementation. We spell out the definition for completeness.

Definition 3.18 (Polynomial-time reductions between distributional unitary synthesis problems)**.** Let $(\mathscr{U}, \Psi)$ and $(\mathscr{V}, \Phi)$ denote distributional unitary synthesis problems. Then $(\mathscr{U}, \Psi)$ *polynomial-time reduces* to $(\mathscr{V}, \Phi)$ if there exists a polynomial-time quantum query algorithm $C^* = (C^*_{x,r})_{x,r}$ such that $C^{(\mathscr{V},\Phi)}$ is an average-case implementation of $(\mathscr{U}, \Psi)$.

Note that one can also define reductions between "normal" and distributional unitary synthesis problems in the same way.

Just like one can define oracle complexity classes like $\mathsf{P}^{\mathrm{3SAT}}$ (i.e., polynomial-time computation with oracle access to a 3SAT oracle), we can now also define oracle complexity classes for unitary synthesis problems:

Definition 3.19 (Oracle unitary complexity classes)**.** We define the oracle class $\mathsf{unitaryBQP}^{\mathscr{V}}$ to be the set of all unitary synthesis problems that are polynomial-time reducible to a unitary synthesis problem $\mathscr{V}$.

We can similarly define the oracle class $\mathsf{avgUnitaryBQP}^{(\mathscr{V},\Omega)}$. However, there is a subtlety: we will have to specify a state complexity class which the distributional states are required to be from. For $\mathsf{avgUnitaryBQP}$, we required that the distributional states be from $\mathsf{stateBQP}$. However, if we give the $\mathsf{avgUnitaryBQP}$ oracle access to $(\mathscr{V}, \Omega)$, it is natural to allow the same oracle access for the preparation of the distributional states, too (corresponding to the principle that the complexity of the distributional state should match the complexity of the unitary class). The resulting "oracle state complexity class" $\mathsf{stateBQP}^{(\mathscr{V},\Omega)}$ is defined completely analogously to the unitary setting by allowing oracle gates in the state preparation circuits from Definition 2.11. With this, we can define:

Definition 3.20 (Average-case oracle unitary complexity classes)**.** We define the oracle class $\mathsf{avgUnitaryBQP}^{(\mathscr{V},\Omega)}$ to be the set of all distributional problems $(\mathscr{U}, \Psi)$ that are polynomial-time reducible to the distributional unitary synthesis problem $(\mathscr{V}, \Omega)$ and for which $\Psi \in \mathsf{stateBQP}^{(\mathscr{V},\Omega)}$.

Just like for classical complexity classes, we can use this notion of reduction to define hard and complete problems for (average-case) unitary complexity classes.

Definition 3.21 (Hard and complete problems)**.** We call a unitary synthesis problem $\mathscr{U}$ *hard* (under polynomial-time reductions) for a unitary complexity class $\mathsf{unitaryC}$ if $\mathsf{unitaryC} \subseteq \mathsf{unitaryBQP}^{\mathscr{U}}$. If additionally $\mathscr{U} \in \mathsf{unitaryC}$, we call $\mathscr{U}$ *complete* for the class $\mathsf{unitaryC}$.

Analogously, we call a distributional unitary synthesis problem $(\mathscr{U}, \Psi)$ *hard* (under polynomial-time reductions) for an average-case unitary complexity class $\mathsf{avgUnitaryC}$ if $\mathsf{avgUnitaryC} \subseteq \mathsf{avgUnitaryBQP}^{(\mathscr{U},\Psi)}$. If additionally $(\mathscr{U}, \Psi) \in \mathsf{avgUnitaryC}$, we call $(\mathscr{U}, \Psi)$ *complete* for the class $\mathsf{avgUnitaryC}$.

As would be expected, $\mathsf{unitaryBQP}$ and $\mathsf{avgUnitaryBQP}$ are closed under polynomial-time reductions.

Lemma 3.22. $\mathsf{unitaryBQP}$ is closed under polynomial-time reductions, i.e., for all $\mathscr{V} \in \mathsf{unitaryBQP}$, we have that $\mathsf{unitaryBQP}^{\mathscr{V}} \subseteq \mathsf{unitaryBQP}$. Similarly, $\mathsf{avgUnitaryBQP}$ is closed under polynomial-time reductions, i.e. for all $(\mathscr{V}, \Omega) \in \mathsf{avgUnitaryBQP}$, we have that $\mathsf{avgUnitaryBQP}^{(\mathscr{V},\Omega)} \subseteq \mathsf{avgUnitaryBQP}$.

This follows almost trivially from the definitions, but we spell out the proof to illustrate how to use the definitions.

Proof. Consider a unitary synthesis problem $\mathscr{U} = (U_x)_x \in \mathsf{unitaryBQP}^{\mathscr{V}}$. By definition, there exists a polynomial-time quantum query algorithm $C^* = (C^*_{x,r})_{x,r}$ such that $C^{\mathscr{V}}$ is a worst-case implementation of $\mathscr{U}$. Since $\mathscr{V} \in \mathsf{unitaryBQP}$, there exists a polynomial-time quantum algorithm $(D_{y,s})_{y,s}$ that is a worst-case implementation of $\mathscr{V}$. For every oracle gate in $C^{\mathscr{V}}_{x,r}$ with some label (y, s), we can insert the explicit circuit $D_{y,s}$. This yields a polynomial-time quantum algorithm for $\mathscr{U}$ because $|y|, s \leq \mathrm{poly}(|x|, r)$ by Definition 3.15. □

The same "proof-by-plugging-in-explicit-circuits" also shows that $\mathsf{unitaryPSPACE}$ and $\mathsf{avgUnitaryPSPACE}$ are closed under polynomial-time reductions.

Lemma 3.23. $\mathsf{unitaryPSPACE}$ is closed under polynomial-time reductions, i.e. for all $\mathscr{V} \in \mathsf{unitaryPSPACE}$, we have that $\mathsf{unitaryBQP}^{\mathscr{V}} \subseteq \mathsf{unitaryPSPACE}$. Similarly, $\mathsf{avgUnitaryPSPACE}$ is closed under polynomial-time reductions, i.e. for all $(\mathscr{V}, \Omega) \in \mathsf{avgUnitaryPSPACE}$, we have that $\mathsf{avgUnitaryBQP}^{(\mathscr{V},\Omega)} \subseteq \mathsf{avgUnitaryPSPACE}$.

3.5 Purification of space-bounded unitary synthesis

By definition, unitary synthesis problems in $\mathsf{unitaryPSPACE}$ and $\mathsf{avgUnitaryPSPACE}$ are implementable by *general* circuits using polynomial space. Thus, non-unitary operations such as measurements, tracing out, qubit reset, etc., are allowed. Although one can simulate such non-unitary operations using unitary ones (for example, performing measurements coherently), such direct simulations result in an expensive blow-up in space. For example, applying the principle of deferred measurement to a polynomial-space circuit with exponentially many intermediate measurements would require exponentially many ancilla qubits.

Whether intermediate measurements and other non-unitary operations can be removed in space-bounded quantum computation has been studied by Fefferman and Remscrim [FR21] and Girish and Raz [GR21]. Both works show that, up to a small blow-up in space (but perhaps a large blow-up in time), general circuits and unitary circuits decide the same languages. Girish and Raz prove a stronger result and show that the *channel* computed by a circuit with intermediate measurements can be approximated by a unitary circuit with small blow-up in space:

Theorem 3.24 (Eliminating intermediate measurements [GR21])**.** Let C be a time T, space $S \geq \log T$ general quantum circuit whose output is n qubits. Then for all $\epsilon > 0$ there exists a unitary circuit D using $O((S + \log(1/\epsilon)) \log T)$ space and $T \cdot \mathrm{poly}(S, \log 1/\epsilon)$ time such that

$$\left\| C - B \circ D \circ A \right\|_{\diamond} \leq \epsilon$$

Here, C and D are also used to denote the channels computed by the circuits, A denotes the channel that appends a number of zeroes (so that the input size of A matches the input size of C, and the output size of A matches the input size of D), and B denotes tracing out all but the first n qubits. Furthermore, if the circuit description of C is computable by a Turing machine M, then the circuit description of D is computable by a Turing machine whose space and time usage is polynomial in that of M.

We apply this result to show that, without loss of generality, all unitary synthesis problems in $\mathsf{unitaryPSPACE}$ and $\mathsf{avgUnitaryPSPACE}$ can be implemented by circuits that are entirely unitary except for some initial ancilla initialization, and a final trace out operation.

Lemma 3.25. All unitary synthesis problems $\mathscr{U} \in \mathsf{unitaryPSPACE}$ and $(\mathscr{U}, \Psi) \in \mathsf{avgUnitaryPSPACE}$ have polynomial-space implementations that are entirely unitary except for some initial ancilla initialization, and a final trace out operation.

Proof. We prove this for $\mathsf{unitaryPSPACE}$; the proof for $\mathsf{avgUnitaryPSPACE}$ is essentially the same. Let $\mathscr{U} = (U_x)_x \in \mathsf{unitaryPSPACE}$. Then for all instances x and precision parameter r, there exists a general quantum circuit C on $S = \mathrm{poly}(n, r)$ qubits that implements U_x with error $1/2r$. Furthermore, since the description of C is computable by a $\mathrm{poly}(n, r)$-space Turing machine, it must be that the time complexity of the circuit is at most $T = 2^{\mathrm{poly}(n,r)}$. By Theorem 3.24 and setting $\epsilon = 1/2r$, there exists a unitary circuit D on $(S + \log(1/\epsilon)) \log T = \mathrm{poly}(n, r)$ qubits and $T \cdot \mathrm{poly}(S, \log 1/\epsilon) = 2^{\mathrm{poly}(n,r)}$ time that simulates C with error $1/2r$, and therefore

$$\left\| U_x - B \circ D \circ A \right\|_\diamond \leq \frac{1}{r} \, ,$$

as desired. Since the circuit C is part of a space-uniform family of circuits, so is the circuit D (this follows from the "furthermore" part of Theorem 3.24). □

3.6 Discussion

Compared to the classical setting, the definitions of complexity classes and reductions in the unitary world have additional subtleties. Above, we have presented the definitions that we find most natural and useful for showing interesting reductions. In this subsection, we explain the choices we made in our definitions.

3.6.1 Classical vs quantum inputs

Our definition of unitary synthesis problems distinguishes between the instance specified by a string $x \in \{0, 1\}^*$ and the quantum input. One might wonder about an alternative definition of unitary synthesis problems where the instance x is "folded" into the quantum input; instead of having U_x for every string x, we define a unitary U_n that maps $|x\rangle |\psi\rangle$ to $|x\rangle U_x |\psi\rangle$ for all $x \in \{0, 1\}^n$. That is, the unitaries/partial isometries are indexed by natural numbers indicating the length of the instance x.

Our definition of unitary synthesis problem contains this definition as a special case (e.g. we could only define U_n for $n \in \mathbb{N}$ to be nontrivial, like in the definition of $\textsc{UnitaryDecider}_L$ in Section 3.1). We find our more general definition helpful because it reinforces the conceptual separation between the instance x (which specifies *which* state transformation task we are meant to perform), and the input state to that state transformation task. In the aforementioned alternative definition, the instance x is syntactically treated on equal footing with the quantum input, even though the instance string $|x\rangle$ is not meant to be transformed.

Furthermore, the alternative definition suggests an unnatural requirement where implementing U_n would mean behaving coherently on a superposition of instances, i.e.,

$$\sum_x \alpha_x |x\rangle |\psi_x\rangle \mapsto \sum_x \alpha_x |x\rangle U_x |\psi_x\rangle \ .$$

However, this is usually difficult to achieve as it requires the algorithm implementing U_n to uncompute any junk that depends on x, which may not be efficiently performable (even though each individual map $|\psi\rangle \mapsto U_x |\psi\rangle$ may be efficiently performable).

3.6.2 Classical average-case complexity vs distributional unitary synthesis problems

Distinguishing between the classical instance and the quantum input allows us to consider two different notions of average-case unitary synthesis problems. The first, which we focus on in this paper, are distributional unitary synthesis problems. Here, the input to the unitary is fixed as part of a larger entangled state, and for every instance x, we require the existence of a circuit that approximates the unitary U_x on this fixed entangled input state.

Another notion, which is closer to classical average-case complexity [BT06], are "instance-average-case" unitary synthesis problems: we could consider a distribution over classical instances x of a unitary synthesis problem $\mathscr{U} = (U_x)_x$, and e.g. require that a polynomial-time quantum algorithm $C_{x,r}$ approximates U_x with high probability over the choice of x. This parallels the way in which classical average-case complexity considers distributions over computational problems and demands that an algorithm can solve a randomly sampled instance with high probability. We do not explore this in depth here, but we do introduce some version of this when discussing the complexity of quantum commitment schemes (see Section 8).

3.6.3 On the error dependence

In our definition of (average-case) unitaryBQP, the running time of the algorithm scales polynomially with the instance size, as well as the precision parameter r. Put another way, the algorithm achieves error ϵ by running in time $\mathrm{poly}(n, 1/\epsilon)$. As mentioned earlier, the fact that the algorithm must work for all ϵ ensures that the given unitary synthesis problem is captured by the algorithm.

Some may wonder why we choose the error dependence to be polynomial in $1/\epsilon$ rather than, say, $\log 1/\epsilon$. In traditional complexity theory we are accustomed to the fact that errors can be often reduced to ϵ by simply repeating the algorithm $O(\log 1/\epsilon)$ times and taking a majority vote. Being able to achieve negligible error while maintaining polynomial time complexity is a very convenient property in traditional complexity theory.

This feature is not universal, however. For example, the majority vote approach does not work in settings where the output is randomized and consists of many bits. Furthermore, in the unitary complexity setting it may not be possible to repeat an algorithm, because ithere is only one copy of the input.

The $\mathrm{poly}(1/\epsilon)$-dependence in our definitions is analogous to several other areas in complexity theory:

1. In the theory of approximation algorithms for NP-optimization problems, a *fully polynomial time approximation scheme (FPTAS)* is an algorithm that achieves approximation error ϵ in time $\mathrm{poly}(n, 1/\epsilon)$. A wide variety of optimization problems are known to be NP-hard to solve exactly but admit FPTASes, such as knapsack problems, some subset sum problems, and some restricted shortest path problems [Vaz01].

2. In the theory of average-case complexity [BT06], a (decision) problem is efficiently solvable on average if there is an algorithm that, for all ϵ, decides the problem with error ϵ and runs in time $\mathrm{poly}(n, 1/\epsilon)$.

3. The definitions of relational complexity classes such as FBPP, FBQP as well as the sampling classes SampBPP, SampBQP all have error dependencies that scale as $\mathrm{poly}(1/\epsilon)$ [Aar14, ABK23]. **Tony: we could maybe make a bigger deal about [ABK23] since they also discuss this explicitly? I find it a bit strange that people give us so much trouble for this error dependence and Scott just says "We allow time polynomial in $1/\epsilon$ because, as we'll see, there are natural reductions that need such time." and presumably everyone is just fine with it? Though I'm not sure how to say this**

nicely...Henry: added a comment below. not sure there's much to say... either you want to be ideological about definitions, or you can make definitions in order to say useful things :)

In these settings, the $\mathrm{poly}(1/\epsilon)$ error dependence in the definition of efficient computation is justified in two ways. First, it captures natural classes of algorithms in the setting of interest (e.g., approximation, average-case, heuristic, or sampling algorithms). **Henry: added:** This definitional choice enables one to make useful statements about the various computational phenomena being studied (see, for example, the brief discussion about this choice in [ABK23]).

Second, in certain cases, it is highly implausible to have better error dependence: for example, problems like knapsack have FPTASes (with running time $\mathrm{poly}(n, 1/\epsilon)$), but if there was $\mathrm{poly}(n, \log 1/\epsilon)$-time approximation algorithm, then $\mathsf{P} = \mathsf{NP}$.

As we will see, our definitions of efficient computation (with $\mathrm{poly}(1/\epsilon)$ error dependency) capture the error-dependency of most algorithms and protocols for "fully quantum" tasks. Just to name a few assorted examples: interactive protocols for state synthesis [RY22], tomography algorithms [OW16, HKP20], Uhlmann transformations [MY23], and density matrix exponentiation algorithms [LMR14, KLL$^+$17] all have $\mathrm{poly}(1/\epsilon)$ dependency on accuracy. Furthermore, there is some evidence that this error dependency is necessary in the unitary complexity setting: there is a (black-box) unitary synthesis task that can be solved in time $\mathrm{poly}(n, 1/\epsilon)$ but not $\mathrm{poly}(n, \log 1/\epsilon)$ [CCLY21].[14]

We find that it is a fascinating question of whether there are exponential error reduction techniques in state and unitary synthesis, or whether it is impossible. Finding additional evidence for it one way or another would help us understand "fully quantum" complexity theory better.

Open Problem 1. Is exponential error reduction generically possible for state and unitary synthesis problems, or can we find additional evidence that this is impossible?

Even if generic error reduction is impossible, one can still hope to construct exponentially precise implementations of *specific* unitary synthesis problems by other means. We leave it as an interesting open problem to come up with such exponentially precise algorithms for e.g. the Uhlmann Transformation Problem.

Open Problem 2. Are there interesting examples of unitary synthesis problems, e.g. the Uhlmann Transformation Problem, which can be efficiently implemented with inverse exponential error?

3.6.4 On errors in reductions

In traditional complexity theory, when defining an oracle class like $\mathsf{PSPACE}^{\mathsf{BQP}}$, we mean that the PSPACE query algorithm gets to query an oracle that decides a BQP language *without error*. This is justified by the fact that we can assume without loss of generality that a BQP algorithm has exponentially small error. The lack of exponential error reduction for unitary synthesis problems, however, compels us to take additional care when defining reductions.

In our notion of reduction, the query circuit is required to specify an error bound for each query. This captures the operational idea of a reduction: when running a reduction algorithm in "real life", each query is made to some actual algorithm which will makes errors. Of course, when composing polynomial-time algorithms for unitary synthesis problems, we can assume the queries are made to the *ideal* unitary: the error of each query can be made an arbitrarily small inverse polynomial at the cost of a polynomial blow-up in running time, and the overall error is still only an inverse polynomial.

[14] The task studied is in the context of post-quantum zero-knowledge proofs: given a malicious verifier's code and its auxiliary input as input, output an ϵ-approximation of the verifier's view after its interaction with the honest prover.

On the other hand, if the query algorithm can make a superpolynomial number of queries (for example, when considering unitaryPSPACE query algorithms), it can matter whether we assume the query algorithm gets access to the ideal unitary or an approximate version of it. For example, one can construct examples[15] of unitary synthesis problems $\mathscr{U} \in$ unitaryBQP such that, given the ability to make exponentially many queries to the ideal unitary, one can in polynomial-space implement a unitary that would require exponential space – leading to the puzzling conclusion that $\mathsf{unitaryPSPACE}^{\mathscr{U}}$ requires exponential space to compute. On the other hand, if we insist that an error bound has to be specified for each query (and the space complexity of the query algorithm scales with the desired precision), then we obtain the seemingly more reasonable conclusion that $\mathsf{unitaryPSPACE} = \mathsf{unitaryPSPACE}^{\mathsf{unitaryBQP}}$.

Granted, these peculiarities only manifest themselves when considering reductions that make a superpolynomial number of queries. The rest of this paper only considers polynomial-time reductions, but we believe it is an interesting future direction to explore the nature of inefficient reductions in unitary complexity theory.

3.7 Summary and open problems

In this section, we introduced a formal framework for studying the complexity of unitary synthesis problems. We have already seen the unitary complexity classes unitaryBQP and unitaryPSPACE, as well as their average-case versions. In the next section, we consider interactive proofs for unitary synthesis problems, which will naturally lead us to define the classes unitaryQIP and unitarySZK. This, however, is by no means a full list of all unitary complexity classes that might be of interest — our aim here is to introduce the classes relevant to the Uhlmann transformation problem, not to provide a complete account. As such, it is natural to consider the following question.

Open Problem 3. What are other unitary complexity classes that naturally relate to physically interesting problems? For example, is there a useful notion of unitaryQMA?

The core goal of complexity theory is to organize computational problems into computational classes and understand the relationships between these classes. Later in this paper, we will prove some results relating unitary complexity classes to one another. However, one would naturally conjecture that certain unitary complexity classes are in fact different, e.g. one would expect $\mathsf{unitaryBQP} \neq \mathsf{unitaryPSPACE}$. For decision languages, proving such separations unconditionally is significantly out of reach of current techniques. Intriguingly, it is not clear whether this necessarily constitutes a barrier for proving similar results in the unitary setting, as it might for example be possible that $\mathsf{unitaryBQP} \neq \mathsf{unitaryPSPACE}$, but $\mathsf{BQP} = \mathsf{PSPACE}$. Therefore, another interesting question is the following:

Open Problem 4. Are there barriers from traditional complexity theory to proving unitary complexity class separations? Might it be feasible to prove $\mathsf{unitaryBQP} \neq \mathsf{unitaryPSPACE}$ unconditionally?

Henry: added: Finally, as mentioned at the beginning of this section, the unitary complexity framework presented here (and in the rest of the paper) should not be treated as being set in stone; it is our best attempt at a starting point for a "fully quantum" complexity theory. The definitions and notions were chosen to balance both conceptual clarity as well as practical usefulness for capturing phenomena in "fully quantum" computational tasks. However, we anticipate the framework will evolve in tandem with our understanding of the complexity of quantum input, quantum output tasks.

[15] An example of this would be unitaries of the form $U = V^{1/\exp(n)}$ where V requires exponential time and space to implement. U can be implemented in unitaryBQP because it is exponentially close to the identity and because of the $\mathrm{poly}(n, 1/\epsilon)$ definition of unitaryBQP, but powering it exponentially many times recovers V.

4 Interactive Proofs for Unitary Synthesis

In this section we introduce the notion of interactive proofs for unitary synthesis problems. Intuitively, a unitary synthesis problem $\mathscr{U} = (U_x)_x$ admits an interactive proof if a polynomial-time verifier, who receives an instance x and a quantum register B, can interact with an all-powerful but untrusted prover, and at the end – conditioned on accepting – implements U_x on the register B. This is inspired by the notion of interactive proofs for decision languages, except in addition to accepting/rejecting at the end, the verifier has to implement a unitary transformation on a given register.

We introduce the (worst-case) unitary synthesis class unitaryQIP, and give an example of a unitary synthesis problem in it that is plausibly outside unitaryBQP. We then introduce the average-case interactive proof classes avgUnitaryQIP and avgUnitaryHVSZK; this latter class captures a notion of *zero-knowledge* interactive unitary synthesis. As we will see in Sections 6 and 7, the complexity of such average-case interactive proof classes are deeply related to the Uhlmann Transformation Problem.

4.1 Interactive proofs for unitary synthesis

We present our notion of interactive protocols for unitary synthesis. (For a refresher on how quantum interactive protocols are formalized, we refer the reader to Section 2.4. It is also useful to compare this definition to the anologous one for state complexity in Definition 2.12).

Definition 4.1 (unitaryQIP)**.** Let $c, s : \mathbb{N} \times \mathbb{N} \to [0, 1]$ be functions. The class $\mathsf{unitaryQIP}_{c,s}$ is the set of unitary synthesis problems $\mathscr{U} = (U_x)_x$ where there exists a time-uniform polynomial-time quantum verifier $V = (V_{x,r})_{x\in\{0,1\}^*,r\in\mathbb{N}}$ satisfying, for all $x \in \{0, 1\}^*$ and $r \in \mathbb{N}$:

- *Completeness:* There exists a quantum prover P^* (called an *honest prover*) such that for all input states $|\psi\rangle$ in the support of U_x,

$$\Pr[V_{x,r}(|\psi\rangle)\leftrightarrows P^* \text{ accepts}] \geq c(|x|, r)\,.$$

- *Soundness:* For all input states $|\psi\rangle$ (which consists of an input register A given to the verifier, and a purifying register R not accessed by the verifier or prover), and for all quantum provers P, there exists a channel completion $\Phi_{x,r}$ of U_x such that

$$\text{if} \quad \Pr[V_{x,r}(|\psi\rangle)\leftrightarrows P \text{ accepts}] \geq s(|x|, r) \qquad \text{then} \qquad \mathrm{td}(\sigma_{x,r}, (\Phi_{x,r} \otimes \mathrm{id})(\psi)) \leq \frac{1}{r}\,,$$

  where $\sigma_{x,r}$ denotes the output of $V_{x,r}(|\psi\rangle)\leftrightarrows P$ conditioned on accepting.

Here the probabilities are over the randomness of the interaction.

Remark 4.2. The concept of interactive unitary synthesis and the class unitaryQIP was first introduced by Rosenthal and Yuen [RY22], albeit with a slightly different formulation. Here we have adapted it to be compatible with the framework of unitary synthesis problems established in Section 3.

We note that in the soundness condition, the malicious prover P can depend on the input state $|\psi\rangle$ of the verifier, on which the verifier wants to implement the unitary U_x. This poses a major challenge in designing any unitaryQIP protocol. The prover is untrusted, so it seems dangerous for the verifier to send $|\psi\rangle$ to the prover "in the clear", as the prover could potentially recognize the state and alter it without being detected. But then, how can the verifier enlist the prover's help to implement the desired unitary on the input state?

Rosenthal and Yuen demonstrated that there are nontrivial protocols for interactive unitary synthesis [RY22]; in particular, they showed that a class of unitaries with *polynomial action* – unitary operators that act nontrivially on a subspace of polynomial dimension – can be interactively synthesized. More formally:

Definition 4.3 (Polynomial-action unitary synthesis problems [RY22])**.** A unitary synthesis problem $\mathscr{U} = (U_x)_x$ has *polynomial action* if all U_x are unitary operators, and there exists a polynomial $p(n)$ such that for all x, the unitary U_x acts nontrivially on a subspace of dimension at most $p(|x|)$.

An example of a unitary synthesis problem with polynomial action is a family of reflections $\mathrm{id} - 2\,|\psi\rangle\!\langle\psi|$ for some state $|\psi\rangle$. The reflection only acts nontrivially on a subspace of dimension 1.

Theorem 4.4 (Interactive proofs for unitaries with polynomial action [RY22])**.** Let $\mathscr{U} \in \mathsf{unitaryPSPACE}$ have polynomial action. Then $\mathscr{U} \in \mathsf{unitaryQIP}_{1,\exp(-\mathrm{poly}(n,r))}$.

The high-level ideal behind Theorem 4.4 is as follows: if U is an n-qubit unitary that acts nontrivially only on a $\mathrm{poly}(n)$-dimensional subspace, then there exists an n-qubit density matrix ρ and a parameter $t = \mathrm{poly}(n)$ such that $U = e^{-i\rho t}$. Then, the unitary U can be approximately implemented via the so-called *density matrix exponentiation* algorithm of [LMR14, KLL+17] using only $\mathrm{poly}(n)$-copies of the state ρ. Furthermore, if U can be implemented in $\mathsf{unitaryPSPACE}$, then copies of the corresponding density matrices ρ can be efficiently synthesized via an interactive proof; this utilizes the $\mathsf{statePSPACE} \subseteq \mathsf{stateQIP}$ result of [RY22]. Once these copies have been synthesized, the density matrix exponentiation algorithm is used to apply the Hamiltonian evolution $e^{-i\rho t}$ to the desired register. Note that in this protocol, the prover is just used to synthesize a (potentially) complex state, which in turn helps the verifier apply the desired unitary – the prover never touches the input register given to the verifier.

While unitaries with polynomial action are a rather restrictive class of transformations, they can still be quite complex. For example, suppose $|\psi\rangle$ is a state that requires exponential time (but polynomial space) to synthesize. The reflection operator $\mathrm{id} - 2\,|\psi\rangle\!\langle\psi|$ is unlikely to be efficiently implementable in polynomial time; finding formal evidence for this is an interesting direction that we leave for future work.

Polynomial action unitaries provide evidence of problems in $\mathsf{unitaryQIP}$ that lie beyond $\mathsf{unitaryBQP}$, but it would be even better to find a broader class of unitary synthesis problems in $\mathsf{unitaryQIP}$, perhaps even a complete problem. Next, we define an *average-case* version of $\mathsf{unitaryQIP}$ that ends up capturing a much wider class of (distributional) unitary synthesis problems (as we will see in Section 6).

4.2 Average-case interactive unitary synthesis

Analogously to $\mathsf{avgUnitaryBQP}$, in the average-case complexity version of $\mathsf{unitaryQIP}$, the verifier only has to synthesize the desired unitary accurately on a specified distribution state. We define $\mathsf{avgUnitaryQIP}$ as follows.

Definition 4.5 ($\mathsf{avgUnitaryQIP}$)**.** Let $c, s : \mathbb{N} \times \mathbb{N} \to [0, 1]$ be functions. The class $\mathsf{avgUnitaryQIP}_{c,s}$ is the set of distributional unitary synthesis problems $(\mathscr{U} = (U_x)_x, \Psi = (|\psi_x\rangle)_x)$ such that $\Psi \in \mathsf{stateQIP}$ and there exists a polynomial-time quantum verifier $V = (V_{x,r})_{x\in\{0,1\}^*, r\in\mathbb{N}}$ satisfying, for all $x \in \{0, 1\}^*$ and $r \in \mathbb{N}$,

- *Completeness:* There exists a quantum prover P (called an *honest prover*) such that

$$\Pr[V_{x,r}(|\psi_x\rangle) \leftrightarrows P \text{ accepts}] \geq c(|x|, r)$$

where $V_{x,r}$ does not have access to the ancilla register of $|\psi_x\rangle$.

- *Soundness:* For all quantum provers P, there exists a channel completion $\Phi_{x,r}$ of U_x such that

$$\text{if} \quad \Pr[V_{x,r}(|\psi_x\rangle) \leftrightarrows P \text{ accepts}] \geq s(|x|, r) \qquad \text{then} \qquad \mathrm{td}(\sigma_{x,r}, (\Phi_{x,r} \otimes \mathrm{id})(\psi_x)) \leq \frac{1}{r},$$

  where $\sigma_{x,r}$ denotes the output of $V_{x,r}(|\psi_x\rangle) \leftrightarrows P$ conditioned on accepting and $V_{x,r}$ does not have access to the ancilla register of $|\psi_x\rangle$.

Here the probabilities are over the randomness of the interaction.

Remark 4.6. **Henry: added: July 9, 2025:** The distributional state family Ψ of a problem in avgUnitaryQIP is defined to come from stateQIP (corresponding to the principle that the complexity of the distributional state family should match the complexity of the unitary class). However, the result that stateQIP = statePSPACE [RY22, MY23] implies that the class is equivalently defined with the distributional state family coming from statePSPACE. In fact, this will be the definition we work with in the future sections.

Note the difference between the soundness condition of avgUnitaryQIP and unitaryQIP: in the average-case setting, the verifier V receives half of an an entangled distributional state, and at the beginning of the protocol the prover P is guaranteed to be unentangled with this distributional state. The prover's uncertainty about the verifier's quantum input turns out to be a very useful in designing avgUnitaryQIP protocols, as will be illustrated in Section 7 when we show that the Succinct Uhlmann Transformation Problem is complete for avgUnitaryQIP.

4.3 Zero-knowledge protocols for unitary synthesis

In this section we present a notion of *zero knowledge* for unitary synthesis problems. In traditional complexity theory and cryptography, a zero knowledge proof allows a polynomial-time verifier, interacting with an all-powerful prover, to decide the truth of a statement (e.g., whether a graph is 3-colorable) without learning anything else. This is formalized via the notion of a polynomial-time simulator that can reproduce the view of the verifier without any interaction with the prover [GMR89, Wat99]. We now explore an analogous notion for interactive unitary synthesis.

A priori, it is unclear how to reasonably define zero knowledge in the unitary synthesis setting. First, defining zero-knowledge quantum protocols for decision languages is already challenging, as the notion of "view" in the quantum setting is less straightforward than with classical protocols [Wat02, Wat06]. Second, in the unitary synthesis setting the verifier additionally gets one copy of an unknown state $|\psi\rangle$ for the quantum part of its input.

We first explore several attempts to define zero knowledge for unitary synthesis, and highlight their shortcomings. For simplicity, for this discussion we will ignore the precision parameter r. A first attempt is to require that the view of the verifier, when given instance x and a quantum input $|\psi\rangle$ and interacts with the honest prover, can be efficiently output by the simulator Sim that only receives instance x and state $|\psi\rangle$ as input and does not interact with the prover. However, since the verifier is supposed to end up with $U_x |\psi\rangle$ at the end of the protocol, this means that the simulator can output $U_x |\psi\rangle$ from x and $|\psi\rangle$ in polynomial time, meaning that $\mathscr{U} \in$ unitaryBQP. This would lead to an uninteresting definition of zero knowledge.

A second attempt to define zero knowledge is inspired by simulation-based security, where we allow the simulator to query the ideal Uhlmann transformation U_x once. In particular, the simulator gets as input the honest verifier's input $|\psi\rangle$, and gets a single query to U_x, before being asked to output the verifier's view. This still seems problematic in the honest verifier setting, since the simulator might decide to query U_x on a state other than $|\psi\rangle$. If it does that, it seems tricky to argue that the verifier does not learn anything from the interaction since it could potentially learn the target unitary transformation applied to a state that is completely unrelated to the input.

These difficulties point to the core issue with devising a notion of zero knowledge in the unitary synthesis setting. With the standard definition of zero knowledge for decision problems, the input and outputs of the verifier are fully specified for the simulator: in particular, the simulator only has to reproduce the interaction in the accepting case. In the unitary synthesis setting, the verifier does not have a full classical description of what state it is supposed to output: the classical string x provides the simulator with a complete classical description of the partial isometry U_x, but it only gets the input state $|\psi\rangle$ in quantum form.

This motivates us to define a notion of *honest-verifier, average-case* zero knowledge for unitary synthesis, where we consider verifiers that get a classical input x and a subsystem of a fixed state $|\psi_x\rangle$ (like the fixed distribution state in Definition 3.9). We assume the distribution state $|\psi_x\rangle$ has an efficient classical description (i.e. it comes from a stateBQP state family). Thus, the input/output behavior of the unitary synthesis protocol when both the verifier and prover are honest is completely specified, which then allows for the possibility of a simulator. Although the honest-verifier and average-case conditions may appear restrictive, we believe that this definition captures a reasonable notion of zero-knowledge in the unitary synthesis setting. Furthermore, as we will see in Section 6, it is deeply related to the complexity of the Uhlmann Transformation Problem.

Definition 4.7 (Honest-verifier, zero-knowledge unitary synthesis)**.** Let $c, s, \epsilon : \mathbb{N} \times \mathbb{N} \to [0, 1]$ be functions. The class $\mathsf{avgUnitaryHVSZK}_{c,s,\epsilon}$ is the set of distributional unitary synthesis problems $(\mathscr{U} = (U_x)_x, \Psi = (\psi_x)_x) \in \mathsf{avgUnitaryQIP}_{c,s}$ such that

1. The distributional state family $\Psi \in \mathsf{stateBQP}$.
2. There is an *honest verifier* $V^* = (V_{x,r})_{x,r}$ and an *honest prover* P^* satisfying the $\mathsf{avgUnitaryQIP}_{c,s}$ completeness and soundness conditions for $(\mathscr{U}, \Psi)$, and
3. There exists a polynomial-time quantum algorithm Sim (called the *simulator*) ssuch that on input (x, r, j) (for $j \in \mathbb{N}$), outputs a state ρ satisfying
$$\mathrm{td}(\rho, \sigma_{x,r,j}) \leq \epsilon(|x|, r)$$
where $\sigma_{x,r,j}$ is the joint density matrix of both the honest verifier $V^*_{x,r}$'s private register *and* the ancilla register of the input $|\psi_x\rangle$, immediately after the j'th round of interaction with the honest prover P^*.

Remark 4.8. Note that the distribution state sequence Ψ associated with a distributional unitary synthesis problem in $\mathsf{avgUnitaryHVSZK}$ is required to be in $\mathsf{stateBQP}$, instead of some notion of "zero-knowledge state synthesis". **Henry: Added July 19, 2025**. This may appear to violate our principle that the complexity of the distributional state corresponds to the complexity of the unitary synthesis class, but note that the simulator in a $\mathsf{avgUnitaryHVSZK}$ protocol can synthesize the distributional state (because the simulator can produce the ancilla register of $|\psi_x\rangle$ and the verifier's view at the beginning of the protocol). This implies that the distributional state is in $\mathsf{stateBQP}$.

Perfect zero knowledge unitary synthesis. We also define a special subclass of $\mathsf{avgUnitaryHVSZK}$ where the simulator can *perfectly* reproduce the view of the verifier. We call this class $\mathsf{avgUnitaryHVPZK}$, which is analogous to the decision complexity class *perfect zero knowledge*, or PZK, which is a subclass of SZK.

Definition 4.9 ($\mathsf{avgUnitaryHVPZK}$)**.** The class $\mathsf{avgUnitaryHVPZK}_s$ is defined to be $\mathsf{avgUnitaryHVSZK}_{1,s,0}$, i.e., with completeness 1, soundness s, and zero simulator error. When we don't specify the soundness parameter s, we set it to be $1/2$ by default.

In Section 6 we will show that $\textsc{DistUhlmann}_1$ is a complete problem for avgUnitaryHVPZK.

4.4 Discussion

4.4.1 Completeness and soundness parameters

For classical interactive protocols, the completeness and soundness parameters can be amplified in a black box fashion. As a result, there one typically chooses canonical parameters (e.g., completeness $= 2/3$ and soundness $= 1/3$). In the state synthesis setting, the soundness parameter can also be generically amplified via sequential repetition (see [RY22] for a proof).

However, it is not clear whether soundness amplification is possible in the unitary synthesis setting. Conceptually, this is because the verifier only gets one copy of the input state, and if a verifier does not accept the interaction it is unclear how to recover the input state for another repetition of the protocol. This is why we keep the subscripts for completeness and soundness in our definitions of avgUnitaryQIP and avgUnitaryHVSZK explicit.

Open Problem 5. Can completeness/soundness amplification be performed for avgUnitaryQIP, or is there evidence that this is impossible?

4.4.2 Definition of average-case interactive unitary synthesis

In Section 3.6.1, we have explained how distinguishing between classical and quantum inputs allows us to consider two different average-case notions for unitary synthesis: distributional unitary synthesis problems, where the input state to the unitary is part of a larger entangled state, and "instance-average-case" unitary synthesis problems, where we consider a distribution over classical instances x.

This distinction between distributional and instance-average-case unitary synthesis problems is particularly important in the context of interactive unitary synthesis. Recall from Remark 3.5 that we can view the quantum input as being a pure state $|\theta\rangle$ sampled from some distribution (because the verifier sees half of some entangled state $|\psi\rangle$, of which $|\theta\rangle$ is a Schmidt vector). In our definition, while the prover can know the classical instance x and the distribution from which $|\theta\rangle$ is sampled, the prover is *not* allowed to know which state $|\theta\rangle$ was sampled from the distribution. The reason for this is because distributional unitary synthesis problems are meant to capture the task of transforming an entangled state $|\psi\rangle$ (for example, breaking the security of a commitment scheme or decoding the radiation of a black hole). Allowing the prover to "know" what marginal state (more precisely, Schmidt vector) $|\theta\rangle$ was received by the verifier would lead to unphysical operations on the state $|\psi\rangle$.

4.4.3 Closure under polynomial-time reductions

Henry: Added June 16, 2025: It is not immediately clear from the definitions of avgUnitaryQIP and avgUnitaryHVSZK whether they are closed under polynomial-time reductions. Let us see why this is not so straightforward. Let $(\mathscr{U} = (U_x), \Psi = (\psi_x)) \in$ avgUnitaryQIP, and let $(\mathscr{V} = (V_x), \Phi = (\phi_x)) \in$ avgUnitaryBQP$^{(\mathscr{U},\Psi)}$, meaning that there exists a polynomial time query algorithm A with oracle access to $(\mathscr{U}, \Psi)$ that implements $(\mathscr{V}, \Phi)$.

We would like to argue that $(\mathscr{V}, \Phi) \in$ avgUnitaryQIP by giving an interactive synthesis protocol for it. A natural verifier V would be as follows: it would simulate the query algorithm A; every time A makes a query to $\mathscr{U}$, the verifier V would run the interactive protocol for $\mathscr{U}$. Then V would accept only if all of the invocations of the $\mathscr{U}$ protocols accepted. The completeness of this protocol is straightforward; the overall protocol would accept with high probability, provided that each of the sub-protocols accepted with high enough probability.

The soundness of the protocol is less clear. Supposing the overall protocol succeeded with probability at least $1/2$ (say), each of the sub-protocols must have accepted with probability at least $1/2$. One would like to invoke the soundness of the sub-protocol, except it only holds if the input state was the appropriate distribution state from Φ. Unfortunately, the query algorithm A can query the oracle $\mathscr{V}$ on any input state it likes. For example, one can imagine algorithms A that, for some reason, query $\mathscr{U}$ on a completely random input state, unrelated to the distribution state Φ. This may be fine in the query setting, but because there is an adversarial prover involved, the soundness of the protocol for $\mathscr{U}$ does not directly imply that (conditioned on acceptance) the protocol has implemented an average-case implementation of $\mathscr{U}$.

As it turns out, $\mathsf{avgUnitaryQIP}$ *is* closed under polynomial-time reductions, but this follows from our proof of $\mathsf{avgUnitaryQIP} = \mathsf{avgUnitaryPSPACE}$ in Section 7. This still leaves a couple open questions:

Open Problem 6. Is the protocol based on simulating the query algorithm sound? In other words, is there a more direct way to show that $\mathsf{avgUnitaryQIP}$ is closed under polynomial-time reductions?

Open Problem 7. Is $\mathsf{avgUnitaryHVSZK}$ closed under polynomial-time reductions?

We note that even if one shows that the protocol which simulates the query algorithm is sound, there is still a question of whether the protocol is zero-knowledge (i.e., there is a simulator).

4.4.4 Other interactive unitary complexity classes

In this section, we have introduced the unitary complexity classes $(\mathsf{avg})\mathsf{UnitaryQIP}$, $\mathsf{avgUnitaryHVSZK}$, and $\mathsf{avgUnitaryHVPZK}$. We will explore these in detail in Part II and show that they are closely related to the Uhlmann Transformation Problem. One can of course introduce and study additional classes for interactive unitary synthesis; the most obvious is $\mathsf{unitaryQMA}$, which we have already mentioned in Open Problem 3.

Beyond this, a natural question is whether our notion of zero knowledge, which we have introduced for the honest verifier setting, can be meaningfully generalized to the *malicious verifier* setting. In that setting, the interaction between the honest prover and verifier can be efficiently simulated even if the verifier deviates from the protocol. This is typically the notion of zero knowledge that is useful in the cryptographic setting. It is known that in both the classical and quantum settings, the malicious verifier and honest verifier definitions of statistical zero knowledge proofs yield the same complexity classes (i.e., $\mathsf{HVSZK} = \mathsf{HVSZK}$ and $\mathsf{QSZK} = \mathsf{QSZK}$) [Oka96, GSV98, Wat06]. We leave studying stronger notions of zero knowledge protocols for unitary synthesis to future work:

Open Problem 8. Is there a meaningful notion of malicious verifier zero knowledge for unitary synthesis problems, and how is that related to the honest verifier setting that we considered here?

Finally, in this section we have only considered single-prover interactive protocols. However, in traditional (classical and quantum) complexity theory, multi-prover protocols have been shown to be surprisingly powerful [BFL91, JNV+21]. It is natural to ask whether multi-prover models might also provide additional power (and insights) in the unitary synthesis setting:

Open Problem 9. Is there a meaningful notion of multi-prover unitary synthesis protocols, and what is their power?

Part II
Uhlmann Transformation Problem: Definitions and Complexity

5 The Uhlmann Transformation Problem

In this section we formally define the Uhlmann Transformation Problem as a unitary synthesis problem. We also define a "succinct" version of it, in which the two states $|C\rangle, |D\rangle$ specifying an instance of the Uhlmann Transformation Problem may have exponential circuit complexity, but have a succinct polynomial-size classical description.

5.1 Uhlmann's theorem and canonical Uhlmann transformations

We begin by recalling Uhlmann's theorem.

Theorem 5.1 (Uhlmann's theorem [Uhl76])**.** Let $|C\rangle_{\mathsf{AB}}$ and $|D\rangle_{\mathsf{AB}}$ be pure states on registers AB and denote their reduced states on register A by ρ and σ, respectively. Then, there exists a unitary U acting only on register B such that

$$\mathrm{F}(\rho,\sigma) = |\langle D| (\mathrm{id}_{\mathsf{A}} \otimes U_{\mathsf{B}}) |C\rangle|^2 .$$

We would like to define a unitary synthesis problem $(U_x)_x$ corresponding to Uhlmann's theorem. Intuitively, whenever the string x represents a pair of bipartite states $|C\rangle, |D\rangle$ (by specifying circuits for them, for example), the unitary U_x should satisfy the conclusion of Uhlmann's theorem. However a subtlety that arises: the unitary U in Theorem 5.1 is not unique; outside of the support of $\rho = \mathrm{Tr}_{\mathsf{A}}(|C\rangle\langle C|)$, U can act arbitrarily. This motivates defining a *canonical* Uhlmann transformation W corresponding to a pair of bipartite states $|C\rangle, |D\rangle$.

Definition 5.2 (Canonical Uhlmann transformation)**.** The *canonical Uhlmann transformation* corresponding to a pair of pure states $(|C\rangle_{\mathsf{AB}}, |D\rangle_{\mathsf{AB}})$ is defined as

$$W = \mathrm{sgn}(\mathrm{Tr}_{\mathsf{A}}(|D\rangle\langle C|)) . \tag{5.1}$$

For any linear operator K with singular value decomposition $U\Sigma V^\dagger$, we define $\mathrm{sgn}(K) = U \,\mathrm{sgn}(\Sigma) V^\dagger$ with $\mathrm{sgn}(\Sigma)$ denoting replacing all the nonzero entries of Σ with 1 (which is the same as the usual sign function since all singular values are non-negative).

The next proposition justifies why Definition 5.2 is canonical:

Proposition 5.3. The map W defined in Equation (5.1) is a partial isometry, and satisfies the following. Let ρ, σ denote the reduced density matrices of $|C\rangle, |D\rangle$, respectively, on register A. Then a channel Φ acting on register B satisfies

$$\mathrm{F}\Big((\mathrm{id}_{\mathsf{A}} \otimes \Phi_{\mathsf{B}})(|C\rangle\langle C|)\,,\, |D\rangle\langle D|\Big) = \mathrm{F}(\rho,\sigma)$$

if and only if Φ is a channel completion of W.

Proof. Let X, Y be unitary operators acting on register B such that

$$|C\rangle = \sqrt{\rho} \otimes X |\Omega\rangle$$
$$|D\rangle = \sqrt{\sigma} \otimes Y |\Omega\rangle$$

where $|\Omega\rangle = \sum_i |i\rangle_{\mathsf{A}} |i\rangle_{\mathsf{B}}$ is the unnormalized maximally entangled state in the standard basis. Let $U\Sigma V^\dagger$ denote the singular value decomposition of $(\sqrt{\rho}\sqrt{\sigma})^\top$, the transpose of $\sqrt{\rho}\sqrt{\sigma}$ with respect to the standard basis. Then the proof of [MY23, Lemma 7.6] shows that

$$W = YU\,\mathrm{sgn}(\Sigma)V^\dagger X^\dagger\,. \tag{5.2}$$

The fact that W is a partial isometry is clear: since the matrices X, U, V, Y are unitary and $\mathrm{sgn}(\Sigma)$ is a projection, it can be written in the form $W = \Pi F$ where $\Pi = XU\,\mathrm{sgn}(\Sigma)U^\dagger X^\dagger$ is a projection and $F = XUV^\dagger Y^\dagger$ is a unitary. This means that W is a parital isometry.

We now prove the "if" statement (if Φ is a channel completion of W, then it achieves the optimal Uhlmann fidelity); first we assume that Φ is in fact a unitary channel $X \mapsto RXR^\dagger$ for a unitary completion $R = cW + W^\perp$ for some constant $c \in \mathbb{C}$. Assume without loss of generality that $c = 1$.

Suppose for sake of contradiction that $\mathrm{F}((\mathrm{id}\otimes\Phi)\,|C\rangle\!\langle C|\,, |D\rangle\!\langle D|) = |\,\langle D|\,\mathrm{id}\otimes R\,|C\rangle\,|^2 \neq \mathrm{F}(\rho,\sigma)$. The proof of [MY23, Lemma 7.6] shows that $\langle D|\,(\mathrm{id}\otimes W)\,|C\rangle = \sqrt{\mathrm{F}(\rho,\sigma)}$; this then implies that $\langle D|\,\mathrm{id}\otimes W^\perp\,|C\rangle \neq 0$. Let $e^{i\theta}$ be a complex phase such that $e^{i\theta}\,\langle D|\,\mathrm{id}\otimes W^\perp\,|C\rangle$ is a strictly positive number. Then consider the unitary $R' = W + e^{i\theta}W^\perp$. Then

$$|\,\langle D|\,\mathrm{id}\otimes R'\,|C\rangle\,|^2 = |\sqrt{\mathrm{F}(\rho,\sigma)} + e^{i\theta}\,\langle D|\,\mathrm{id}\otimes W^\perp\,|C\rangle\,|^2 > \mathrm{F}(\rho,\sigma)$$

which contradicts Uhlmann's theorem.

Now suppose that Φ is a general channel completion of W. Let V denote a unitary Stinespring dilation of Φ that maps registers BE to BE. Note that

$$\mathrm{F}\Big((\mathrm{id}\otimes\Phi)\,|C\rangle\!\langle C|\,, |D\rangle\!\langle D|\Big) = \max_{|\theta\rangle}\Big|(\langle D|\otimes\langle\theta|)(\mathrm{id}_{\mathsf{A}}\otimes V)(|C\rangle\otimes|0\rangle)\Big|^2 \tag{5.3}$$

where the maximization is over pure states $|\theta\rangle$ on register E.

Let $P = W^\dagger W$ denote the projection onto the domain of W, respectively. Since $\Phi(|a\rangle\!\langle b|) = W\,|a\rangle\!\langle b|\,W^\dagger$ for all $|a\rangle\,, |b\rangle$ in the support of P, we have that $V\,|a\rangle\,|0\rangle = (W\,|a\rangle)_{\mathsf{B}}\otimes|\varphi\rangle$ for some state $|\varphi\rangle$ on register E. This implies that $V = W\otimes|\varphi\rangle\!\langle 0| + V^\perp$ for some partial isometry $V^\perp$. On the other hand, this means that V is a unitary completion of the canonical Uhlmann transformation between the pair of states $(|C\rangle\otimes|0\rangle\,, |D\rangle\otimes|\varphi\rangle)$, which is $W\otimes|\varphi\rangle\!\langle 0|$. Using reasoning analogous to that about unitary completions of W, we obtain that (5.3) is at least $\mathrm{F}(\rho,\sigma)$, but on the other hand by Uhlmann's theorem is at most $\mathrm{F}(\rho,\sigma)$ which concludes the proof of the "if" direction.

We now prove the "only if" direction (if the channel Φ achieves the optimal Uhlmann fidelity, it must be a channel completion of W). Similarly to the proof of the "if" direction we prove this first for unitary channels. Let R be a unitary such that $|\,\langle D|\,(\mathrm{id}\otimes R)\,|C\rangle\,|^2 = \mathrm{F}(\rho,\sigma)$. We note that the proof of Uhlmann's theorem [Wil17, Theorem 9.2.1] shows that

$$|\,\langle D|\,(\mathrm{id}_{\mathsf{A}}\otimes R_{\mathsf{B}})\,|C\rangle\,|^2 = |\mathrm{Tr}(Y^\dagger RX(\sqrt{\sigma}\sqrt{\rho})^\top)|^2\,.$$

Note that the singular value decomposition of $(\sqrt{\sigma}\sqrt{\rho})^\top$ is $V\Sigma U^\dagger$. By assumption,

$$|\mathrm{Tr}(Y^\dagger RX(\sqrt{\sigma}\sqrt{\rho})^\top)|^2 = \mathrm{F}(\rho,\sigma) = \mathrm{Tr}(\Sigma)^2\,.$$

The last equality follows from the fact that $\mathrm{F}(\rho,\sigma) = \mathrm{Tr}(|\sqrt{\rho}\sqrt{\sigma}|)^2 = \mathrm{Tr}(\Sigma)^2$. Let c be a phase such that $c^\dagger\cdot\mathrm{Tr}(Y^\dagger RX(\sqrt{\sigma}\sqrt{\rho})^\top)$ is a nonnegative real number. Substituting in the singular value decomposition of $(\sqrt{\sigma}\sqrt{\rho})^\top$, we get

$$\mathrm{Tr}(\Sigma) = \mathrm{Tr}(\Sigma M)$$

where $M := c^\dagger U^\dagger Y^\dagger R X V$. The only way that equality is achieved is if M acts as identity on the support of Σ. Therefore $M = P + M^\perp$ where $P = \mathrm{sgn}(\Sigma)$ is the projector onto the nonzero entries of Σ and $M^\perp$ is some unitary acting on $I - P$, the orthogonal complement of P.

Note that

$$R = cYU(P + M^\perp)V^\dagger X^\dagger = cW + cYUM^\perp V^\dagger X^\dagger \, .$$

Letting $W^\perp := cYUM^\perp V^\dagger X^\dagger$, we observe that it is a partial isometry with support and range disjoint from the support and range respectively of W. This concludes the proof of the "only if" direction for unitary channels $\Phi(X) = RXR^\dagger$.

Now suppose that Φ were a general channel achieving the optimal Uhlmann fidelity. Just like with the proof of the "if" direction, consider the unitary Stinespring dilation V of Φ. This satisfies

$$\mathrm{F}(\rho, \sigma) = \mathrm{F}\Big((\mathrm{id} \otimes \Phi) |C\rangle\langle C| \, , |D\rangle\langle D| \Big) = \Big| (\langle D| \otimes \langle \varphi|)(\mathrm{id}_{\mathsf{A}} \otimes V_{\mathsf{BE}})(|C\rangle \otimes |0\rangle) \Big|^2 \tag{5.4}$$

for some state $|\varphi\rangle$. This implies that V is a unitary completion of the canonical Uhlmann transformation $W \otimes |\varphi\rangle\langle 0|$ for the pair of states $(|C\rangle \otimes |0\rangle \, , |D\rangle \otimes |\varphi\rangle)$. By the above reasoning, this implies that $V = cW \otimes |\varphi\rangle\langle 0| + V^\perp$ for some partial isometry $V^\perp$ with disjoint support and range and some constant $c \in C$. It can be verified that the corresponding channel $\Phi(X) = \mathrm{Tr}_{\mathsf{E}}(V(X \otimes |0\rangle\langle 0|)V^\dagger)$ is a channel completion of W. This completes the proof of the "only if" direction.

□

5.2 Uhlmann Transformation Problem

We now formulate unitary synthesis problems corresponding to Uhlmann transformations. First, we define explicit and succinct descriptions of quantum circuits.

Definition 5.4 (Explicit and succinct descriptions of quantum circuits)**.** An *explicit description* of a unitary quantum circuit C is a sequence $(1^n, g_1, g_2, \ldots)$ where 1^n represents in unary the number of qubits that C acts on, and $g_1, g_2, g_3, \ldots$ is a sequence of unitary gates.

A *succinct description* of a quantum circuit C is a pair $(1^n, \hat{C})$ where $\hat{C}$ is a description of a classical circuit[16] that takes as input an integer t in binary and outputs the description a unitary gate g_t coming from some universal gate set, as well as the (constant-sized) set of qubits that g_t acts on. Together, the gates $g_1, \ldots, g_T$ describe a circuit C acting on n qubits; we will always denote the classical circuit with a hat (e.g. $\hat{C}$) and use the same letter without a hat (e.g. C) for the associated quantum circuit.

We make a few remarks about the definitions of explicit and succinct descriptions of quantum circuits:

(i) The length of an explicit description of a quantum circuit is polynomial in the number of gates in the circuit as well as the number of qubits it acts on.

(ii) In a succinct description of a quantum circuit C, the size of the circuit may be exponentially larger than the length of the description $(1^n, \hat{C})$. However, the number of qubits that C acts on is polynomial (in fact, at most linear) in the description length.

(iii) For a succinct description, we provide the number of qubits n in the quantum circuit explicitly in unary because given only the classical circuit $\hat{C}$ it may be difficult to compute the the number of qubits that the quantum circuit C acts on.

[16] Here, we think of $\hat{C}$ as being a list of AND, OR, and NOT gates.

We now define two variants of the Uhlmann Transformation Problem. In the first, the two bipartite states are described by explicit circuit descriptions, and in the second they are described by succinct circuit descriptions.

Definition 5.5 (Valid Uhlmann instances)**.** We say that a string $x \in \{0,1\}^*$ is a *valid Uhlmann instance* if it encodes a tuple $(1^n, C, D)$ where C, D are explicit descriptions of *unitary* circuits that each act on $2n$ qubits. We say that x is a *valid succinct Uhlmann instance* if $x = (1^n, \hat{C}, \hat{D})$ is a succinct description of a pair (C, D) of unitary circuits that each act on $2n$ qubits for some n.

We further say that a valid (possibly succinct) Uhlmann instance x is a *fidelity-κ instance* if the reduced states ρ, σ of the states $|C\rangle = C\,|0^{2n}\rangle$, $|D\rangle = D\,|0^{2n}\rangle$ on the first n qubits satisfy $\mathrm{F}(\rho,\sigma) \geq \kappa$.

Definition 5.6 (Uhlmann Transformation Problem)**.** Let $\kappa : \mathbb{N} \to [0,1]$ be a function. The *κ-fidelity Uhlmann Transformation Problem* is the unitary synthesis problem $\textsc{Uhlmann}_\kappa = (U_x)_{x\in\{0,1\}^*}$ where whenever $x = (1^n, C, D)$ is a fidelity-$\kappa(n)$ Uhlmann instance specifying a pair (C, D) of unitary circuits that each act on $2n$ qubits for some n, then U_x is the canonical Uhlmann transformation for the pair of states $(|C\rangle, |D\rangle)$. Otherwise if x is not a valid Uhlmann instance, then we define $U_x = 0$ (i.e., a partial isometry with zero-dimensional support).

The *κ-fidelity Succinct Uhlmann Transformation Problem*, denoted by $\textsc{SuccinctUhlmann}_\kappa$, is the sequence $(U_x)_x$ where whenever $x = (1^n, \hat{C}, \hat{D})$ is a valid fidelity-$\kappa(n)$ succinct Uhlmann instance specifying a pair (C, D) of unitary circuits that each act on $2n$ qubits for some n, then U_x is the canonical Uhlmann transformation for the pair of states $(|C\rangle, |D\rangle)$; if x is not a valid succinct Uhlmann instance, then we define $U_x = 0$.

Tony: added: One should think of the fidelity parameter κ as a promise: an algorithm for $\textsc{Uhlmann}_\kappa$ only has to work for state pairs $|C\rangle, |D\rangle$ whose reduced states have fidelity at least κ. The smaller κ, the more difficult $\textsc{Uhlmann}_\kappa$ can become, in the sense that an algorithm for $\textsc{Uhlmann}_\kappa$ also works for all $\textsc{Uhlmann}_{\kappa'}$ for $\kappa' \geq \kappa$.

5.3 Distributional Uhlmann Transformation Problem

To define average case versions of the Uhlmann Transformation Problems we specify a distribution state $|\psi_x\rangle$ for every valid (succinct or non-succinct) Uhlmann instance x.

Definition 5.7 (Distributional Uhlmann Transformation Problems)**.** We define a state sequence $\Psi_{\textsc{Uhlmann}} = (|\psi_x\rangle)_{x\in\{0,1\}^*}$ as follows: for all $x \in \{0,1\}^*$,

$$|\psi_x\rangle = \begin{cases} |C\rangle & \text{if } x = (1^n, C, D) \text{ is valid Uhlmann instance,} \\ 0 & \text{otherwise.} \end{cases}$$

Then, the *distributional κ-fidelity Uhlmann Transformation Problem* is the distributional unitary synthesis problem $\textsc{DistUhlmann}_\kappa = (\textsc{Uhlmann}_\kappa, \Psi_{\textsc{Uhlmann}})$.

The state sequence $\Psi_{\textsc{SuccinctUhlmann}}$ and the distributional unitary synthesis problem $\textsc{DistSuccinctUhlmann}_\kappa$ are defined analogously.

We now argue that this choice of distribution state is natural for the Uhlmann Transformation Problems: being able to solve the distributional Uhlmann Transformation Problems in the average-case essentially coincides with being able to perform the Uhlmann transformation corresponding to a pair of (succinctly or non-succinctly described) states. The next proposition captures this equivalence in the *high κ regime*, where the promised fidelity κ is close to 1. It can also be viewed as a robust version of Proposition 5.3.

Proposition 5.8. Let $|C\rangle_{\mathsf{AB}}, |D\rangle_{\mathsf{AB}}$ denote two bipartite states with reduced density matrices ρ, σ respectively such that $\mathrm{F}(\rho,\sigma) = \kappa$. Let M is a quantum algorithm acting on register B such that

$$\mathrm{F}\Big((\mathrm{id}_{\mathsf{A}} \otimes M_{\mathsf{B}})(|C\rangle\!\langle C|), |D\rangle\!\langle D|\Big) \geq \kappa - \delta \tag{5.5}$$

for some δ. Then there exists a channel completion Φ of the canonical Uhlmann transformation W for $(|C\rangle, |D\rangle)$ such that

$$\mathrm{td}\Big((\mathrm{id} \otimes M)(|C\rangle\!\langle C|)\,,\,(\mathrm{id} \otimes \Phi)(|C\rangle\!\langle C|)\Big) \leq 2\sqrt{1-\kappa} + \sqrt{\delta}\,.$$

Conversely, suppose that there exists a channel completion Φ of W such that

$$\mathrm{td}\Big((\mathrm{id} \otimes M)(|C\rangle\!\langle C|)\,,\,(\mathrm{id} \otimes \Phi)(|C\rangle\!\langle C|)\Big) \leq \delta\,.$$

Then

$$\mathrm{td}\Big((\mathrm{id} \otimes M)(|C\rangle\!\langle C|)\,,\,|D\rangle\!\langle D|\Big) \leq \delta + \sqrt{1-\kappa}\,.$$

Proof. We will prove this proposition for the case of Uhlmann instances; the case of succinct Uhlmann instances is entirely analogous.

We begin with the first part of the proposition. Let W denote the canonical Uhlmann transformation corresponding to $(|C\rangle, |D\rangle)$. Let Φ denote a channel completion of W; by Proposition 5.3 we have that $\mathrm{F}((\mathrm{id} \otimes \Phi)\, |C\rangle\!\langle C|\,, |D\rangle\!\langle D|) = \kappa$. By the triangle inequality, we have

$$\begin{aligned}
&\mathrm{td}\Big((\mathrm{id} \otimes M)(|C\rangle\!\langle C|), (\mathrm{id} \otimes \Phi)(|C\rangle\!\langle C|)\Big)\\
&\quad\leq \mathrm{td}\Big((\mathrm{id} \otimes M)(|C\rangle\!\langle C|), |D\rangle\!\langle D|\Big) + \mathrm{td}\Big(\,|D\rangle\!\langle D|\,, (\mathrm{id} \otimes \Phi)(|C\rangle\!\langle C|)\Big)\\
&\quad\leq \sqrt{1-\kappa+\delta} + \sqrt{1-\kappa}\\
&\quad\leq 2\sqrt{1-\kappa} + \sqrt{\delta}
\end{aligned}$$

where in the third line we applied the Fuchs-van de Graaf inequality to Equation (5.5). This shows that one the state $|C\rangle$, M_x behaves (approximately) like a channel completion of the canonical Uhlmann transformation. By Definition 3.4, this means that M_x (approximately) implements the DISTUHLMANN problem as claimed in the first part of the proposition.

We now prove the "Conversely" part of the proposition. By the triangle inequality

$$\begin{aligned}
&\mathrm{td}\Big((\mathrm{id} \otimes M)(|C\rangle\!\langle C|), |D\rangle\!\langle D|\Big)\\
&\quad\leq \mathrm{td}\Big((\mathrm{id} \otimes M)(|C\rangle\!\langle C|), (\mathrm{id} \otimes \Phi)\ |C\rangle\!\langle C|\Big) + \mathrm{td}\Big((\mathrm{id} \otimes \Phi)\,|C\rangle\!\langle C|\,, |D\rangle\!\langle D|\Big)\\
&\quad\leq \delta + \sqrt{1-\kappa}
\end{aligned} \tag{5.6}$$

where the last line follows from our assumption on M, Proposition 5.3, and Fuchs-van de Graaf.

□

6 Complexity of the Uhlmann Transformation Problem

We show that $\textsc{DistUhlmann}_1$ (the distributional Uhlmann Transformation Problem with fidelity promise $\kappa = 1$) is complete for the unitary complexity class $\mathsf{avgUnitaryHVPZK}$ (honest-verifier perfect zero knowledge unitary synthesis) defined in Section 4. We also discuss an approach to showing that $\textsc{DistUhlmann}_\kappa$ for fidelity promise $\kappa < 1$ is complete for the class $\mathsf{avgUnitaryHVSZK}$ (i.e., where the simulator can make some error). This would be analogous to the famous result of Sahai and Vadhan [SV03] showing that deciding whether the statistical distance between two efficiently sampleable distributions is large or small is complete for the decision class SZK.

6.1 A complete problem for $\mathsf{avgUnitaryHVPZK}$

In this section, we show that $\textsc{DistUhlmann}_1$ is complete for the unitary complexity class $\mathsf{avgUnitaryHVPZK}$; recall that this is the class of unitary synthesis problems implementable via a zero-knowledge interactive proof with perfect completeness, soundness $\frac{1}{2}$, and zero simulation error (see Definition 4.9). First we show containment.

Theorem 6.1. $\textsc{DistUhlmann}_1 \in \mathsf{avgUnitaryHVPZK}$.

Proof. In order to prove the claim, we need to exhibit an interactive verifier and simulator that satisfy the conditions of Definition 4.9. Consider the following protocol (Protocol 1).

Protocol 1. Perfect zero-knowledge protocol for $\textsc{DistUhlmann}_1$

Instance: A valid $\textsc{Uhlmann}_1$ instance $x = (1^n, C, D)$ and precision $r \in \mathbb{N}$.
Input: An n qubit quantum register B_0.

1. Let $m = 8r^2$. Sample $i^* \in [m]$ uniformly at random.
2. For $i = 1$ though m:
   (a) If $i \neq i^*$:
      i. Starting with all zeroes in registers $\mathsf{A}'\mathsf{B}'$, prepare the state $|C\rangle_{\mathsf{A}'\mathsf{B}'}$, send B' to the prover.
      ii. After receiving B' back from the prover, apply $D^\dagger$ to $\mathsf{A}'\mathsf{B}'$, and measure all qubits. If it is not equal to all zeroes, reject.
   (b) If $i = i^*$:
      i. Send B_0 to the prover and receive B_0 back.
3. If the verifier has not rejected yet, accept and output B_0.

We show that the honest verifier and prover specified in Protocol 1 satisfy the properties of Definition 4.9. We first prove that the honest prover P^* is accepted with probability 1.

Lemma 6.2 (Completeness)**.** For all valid $\textsc{Uhlmann}_1$ instances $x = (1^n, C, D)$ and error parameters $r \in \mathbb{N}$, for sufficiently large n the honest prover P^* satisfies

$$\Pr[V_{x,r}(|C\rangle_{\mathsf{A}_0\mathsf{B}_0}) \leftrightarrows P^*] = 1\,.$$

Proof. Since x is an $\textsc{Uhlmann}_1$ instance, the canonical Uhlmann transformation exactly maps $|C\rangle$ to $|D\rangle$. We define the honest prover as follows: in every round the honest prover receives the B register of $|C\rangle$ and applies the canonical Uhlmann transformation, mapping the pure state to $|D\rangle$. The verifier always measures the all 0 string. Thus, the honest prover is accepted with probability 1. □

We now prove the soundness property, i.e., if the verifier accepts with probability at least $1/2$ when interacting with a prover P, then conditioned in accepting, the verifier outputs a state $\frac{1}{r}$ close to the ideal output.

Lemma 6.3 (Soundness)**.** For all $\textsc{Uhlmann}_1$ instances $x = (1^n, C, D)$ and error parameters $r \in \mathbb{N}$, for sufficiently large n, for all quantum interactive provers P, there exists a channel completion Φ_x of U_x such that

$$\text{if} \quad \Pr[V_{x,r}(|C\rangle) \leftrightarrows P \text{ accepts}] \geq \frac{1}{2} \qquad \text{then} \qquad \mathrm{td}(\sigma, (\Phi_x \otimes \mathrm{id})\, |C\rangle\!\langle C|) \leq \frac{1}{r}\,,$$

where σ denotes the output of $V_{x,r}(|C\rangle) \leftrightarrows P$, conditioned on $V_{x,r}$ accepting.

Proof. The verifier in Protocol 1 is described as sequentially checking, for the "decoy rounds" $i \neq i^*$, whether the i'th copy of the state $|C\rangle$ was transformed to $|D\rangle$. However its messages to the prover are nonadaptive; thus we can equivalently analyze its soundness by considering the following process:

1. Generate m copies of $|C\rangle$ in registers $\mathsf{A}_1\mathsf{B}_1, \ldots, \mathsf{A}_m\mathsf{B}_m$;

2. Send and receive the registers B_i to the prover one at a time;

3. Choose a random index $i^* \in [m]$;

4. Measure all registers $\mathsf{A}_i\mathsf{B}_i$ for $i \neq i^*$ using the measurement $\{\Pi, \mathrm{id} - \Pi\}$ where $\Pi = |D\rangle\!\langle D|$. Accept if all measurements return the Π outcome, and output the $\mathsf{A}_{i^*}\mathsf{B}_{i^*}$ registers. Otherwise, reject.

This can be seen to be equivalent to the verifier in Protocol 1; the "special" index i^* corresponds to where we embed the "true" copy of $|C\rangle_{\mathsf{A}_0\mathsf{B}_0}$.

In this process, the state of the system before the measurement can be written as

$$\rho = (\mathrm{id} \otimes \Lambda)(|C\rangle\!\langle C|^{\otimes m})$$

where $\Lambda(\cdot)$ denotes the prover's quantum channel acting on the registers $\mathsf{B}_1 \cdots \mathsf{B}_m$. Note that the prover's action is completely independent of the embedding index i^*.

Consider sampling a random m-bit string X in the following way: measure each register $\mathsf{A}_i\mathsf{B}_i$ of ρ with the $\{\Pi, \mathrm{id} - \Pi\}$ measurement, and set $X_i = 0$ if the Π outcome occurs, otherwise set $X_i = 1$. For each i let E_i denote the event that $X_j = 1$ for all $j \neq i$. The acceptance probability of the verifier is equal to $\frac{1}{m}\sum_{i^* \in [m]} \Pr[E_{i^*}]$.

On the other hand, the probability of measuring registers $\mathsf{A}_{i^*}\mathsf{B}_{i^*}$ and getting the $\mathrm{id} - \Pi$ outcome, conditioned on the verifier accepting, is given by

$$\frac{\frac{1}{m}\sum_{i^*} \Pr[X_{i^*} = 0 \wedge E_{i^*}]}{\frac{1}{m}\sum_{i^*} \Pr[E_{i^*}]} \leq \frac{2}{m} \sum_{i^*} \Pr[X_{i^*} = 0 \wedge E_{i^*}] \leq \frac{2}{m}$$

where we used the assumption that the acceptance probability of the verifier is at least $1/2$, and that all of the events $X_{i^*} = 0 \wedge E_{i^*}$ are mutually exclusive. By the Gentle Measurement Lemma [Wil17], we have

$$\mathrm{td}(\sigma, |D\rangle\!\langle D|) \leq 2\sqrt{\frac{2}{m}} \leq \sqrt{\frac{8}{m}}$$

where we let σ denote the state of the registers $\mathsf{A}_{i^*}\mathsf{B}_{i^*}$ (or in Protocol 1, registers $\mathsf{A}_0\mathsf{B}_0$) conditioned on the verifier accepting. By our choice of m, this is at most $1/r$.

Finally, let Φ denote a channel completion of the canonical Uhlmann transformation U for x. By Proposition 5.3, $|D\rangle\!\langle D| = (\mathrm{id} \otimes \Phi)(|C\rangle\!\langle C|)$, and thus

$$\mathrm{td}(\sigma, (\mathrm{id} \otimes \Phi)(|C\rangle\!\langle C|)) \leq 1/r$$

as desired.

□

We now show the protocol staisfies the perfect zero-knowledge condition.

Lemma 6.4 (Zero-knowledge)**.** There exists a polynomial-time simulator that, on input (x, r, t), outputs a state equal to $\sigma_{x,r,t}$ which is the reduced density matrix of $V^*_{x,r}$'s private register and the purifying register A_0 of the quantum input, immediately after the t'th round of interaction with the honest prover P^*.

Proof. We assume that the simulator samples the random index $i^* \in [m]$ by preparing a uniform superposition in some register C. Then the state of the verifier at time t is equal to

$$\frac{1}{\sqrt{m}}\Big[\sum_{i^*<t}|i^*\rangle_{\mathsf{C}}\otimes|D\rangle_{\mathsf{A}_0\mathsf{B}_0}\otimes|D\rangle_{\mathsf{A'B'}}\Big]+\frac{1}{\sqrt{m}}\,|t\rangle_{\mathsf{C}}\otimes|D\rangle_{\mathsf{A}_0\mathsf{B}_0}\otimes|0\rangle_{\mathsf{A'B'}}+\frac{1}{\sqrt{m}}\Big[\sum_{i^*>t}|i^*\rangle_{\mathsf{C}}\otimes|C\rangle_{\mathsf{A}_0\mathsf{B}_0}\otimes|D\rangle_{\mathsf{A'B'}}\Big]$$

because when $i^* < t$, the prover will have already transformed both the true copy as well as the decoy copy of $|C\rangle$; when $i^* = t$, the prover will have already transformed the true copy, and the decoy copy is still the all zeroes state; and when $i^* > t$ the true copy will not have been transformed yet, but the decoy copy has. It is easy to see that this state can be prepared in polynomial time.

□

This completes the proof of Theorem 6.1. □

We now show that all problems in avgUnitaryHVPZK reduce to $\textsc{DistUhlmann}_1$.

Theorem 6.5. $\textsc{DistUhlmann}_1$ is avgUnitaryHVPZK-hard.

Proof. The main idea is as follows: the honest prover for an avgUnitaryHVPZK protocol can be efficiently implemented using a $\textsc{DistUhlmann}_1$ oracle. The oracle is used to perform Uhlmann transformations between the consecutive "snapshots" of the verifier's state, which can be efficiently produced from the simulator.

Let $(\mathscr{U}, \Psi) \in$ avgUnitaryHVPZK. Let $V = (V_{x,r})$ denote the corresponding $m(|x|, r)$-round verifier. For notational simplicity we fix an instance $x \in \{0,1\}^*$, a precision parameter $r \in \mathbb{N}$, and write $m = m(|x|, r)$, $V = V_{x,r}$, $|\psi\rangle = |\psi_x\rangle$, $U = U_x$, and $\mathrm{Sim}(t) = \mathrm{Sim}(x, r, t)$. Let A and B denote the target and ancilla registers of $|\psi\rangle$, respectively (i.e., register B is never touched during the protocol).

Fix a round $1 \leq t \leq m$. Consider the purified circuit of the simulator $\mathrm{Sim}(t)$. On the all zeroes input it outputs a pure state $|\varphi_t\rangle$ on registers BFQP where B represents the ancilla register of the input state $|\psi\rangle$, F represents the verifier's workspace register, Q represents the verifier's message register, and P represents the rest of the purification. By definition of perfect zero-knowledge, the reduced density matrix of $|\varphi_t\rangle$ on registers BFQ is identical to the same registers of the protocol after the verifier has received the t'th message from the honest prover P^*. Thus, $|\varphi_t\rangle$ denotes the state of the protocol up to a unitary on register P. Let L denote the total number of qubits.

At the beginning of the $(t+1)$'st round of the protocol, the verifier applies the unitary V_{t+1} to registers FQ of $|\varphi_t\rangle$, before sending the register Q to the prover (who applies a unitary to Q as well as its private memory register P). Note that

$$\mathrm{Tr}_{\mathsf{QP}}(V_{t+1} |\varphi_t\rangle\!\langle\varphi_t| V_{t+1}^\dagger) = \mathrm{Tr}_{\mathsf{QP}}(|\varphi_{t+1}\rangle\!\langle\varphi_{t+1}|)$$

where $|\varphi_{t+1}\rangle$ denotes the (purified) output of the simulator $\mathrm{Sim}(t+1)$. This is because the registers BF do not change between $V_{t+1}|\varphi_t\rangle$ and $|\varphi_{t+1}\rangle$ in the actual protocol; the only difference is the prover's action on registers QP.

Define $|C_{t+1}\rangle = V_{t+1}|\varphi_t\rangle$ and $|D_{t+1}\rangle = |\varphi_{t+1}\rangle$. Thus the prover's action is an Uhlmann transformation on the registers QP between the pair of states $(|C_{t+1}\rangle, |D_{t+1}\rangle)$. Since Sim and V have polynomial-size circuits, so do the pair of states $(|C_{t+1}\rangle, |D_{t+1}\rangle)$. Call this pair of circuits (C_{t+1}, D_{t+1}).

Define $|\varphi_0\rangle = |\psi\rangle_{\mathsf{BA}} |0\cdots 0\rangle$. Since the state family Ψ is in $\mathsf{stateBQP}$ this implies that $|\varphi_0\rangle$ also has a polynomial-size circuit.

Consider the following query algorithm:

1. Given input register A, prepare the rest of the verifier's workspace F, message register Q, and the prover's workspace P in the state $|0\cdots 0\rangle$.
2. For $1 \le t \le m$:
   (a) Apply the verifier unitary V_t to register FQ.
   (b) Query the DISTUHLMANN$_1$ oracle with instance $(1^L, C_t, D_t)$, precision parameter $s = rm$, and register QP of C_t as the quantum input.
3. Apply the final verifier unitary V_{m+1} to register FQ.
4. Output register A of the verifier's workspace register, which denotes the output of the verifier.

This is a polynomial-time query algorithm since it makes only polynomially-many queries and the circuits $V = (V_t)$ are all polynomial-size. Suppose each of the DISTUHLMANN$_1$ oracle calls were implemented without error. By induction, the state at the end of step 2(b) in the query algorithm is $|D_t\rangle = |\varphi_t\rangle$ (this is because by Proposition 5.3, any channel completion of the canonical Uhlmann transformation maps $|C_t\rangle$ to $|D_t\rangle$). By the completeness property of the zero-knowledge protocol for $(\mathscr{U}, \Psi)$ implies that the state $|\psi\rangle$ has been exactly transformed to $(U \otimes \mathrm{id})|\psi\rangle$. However, since each prover action is simulated up to error $1/s$, the total error is at most $m/s = 1/r$. This shows that $(\mathscr{U}, \Psi)$ can be implemented in polynomial-time, given oracle access to DISTUHLMANN$_1$.

□

6.2 The imperfect fidelity case

We now turn to the complexity of DISTUHLMANN$_\kappa$ when $\kappa < 1$. Note that for all $0 \le \kappa_1 \le \kappa_2 \le 1$, we have that all valid instances of UHLMANN$_{\kappa_2}$ are valid instances of UHLMANN$_{\kappa_1}$ but not vice versa (a similar statement holds for SUCCINCTUHLMANN). Thus, implementing general UHLMANN$_{\kappa_1}$ transformations may potentially be more difficult than implementing UHLMANN$_{\kappa_2}$ transformations. Furthermore, it is no longer apparent that there is a zero-knowledge protocol for, say, DISTUHLMANN$_{1/2}$. Thus it is not clear how the complexities of UHLMANN$_{\kappa_1}$ and UHLMANN$_{\kappa_2}$ relate to each other for different κ_1, κ_2.

We present a simple padding trick which shows that as long as κ_1, κ_2 are bounded by at least some inverse polynomial from either 0 or 1, the complexities of DISTUHLMANN$_{\kappa_1}$ and DISTUHLMANN$_{\kappa_2}$ are equivalent under polynomial-time reductions.

Lemma 6.6 (Padding trick)**.** Let $0 \leq \kappa_1 \leq \kappa_2 \leq 1$ and let C, D be circuits on $2n$ qubits such that $\mathrm{F}(\rho, \sigma) \geq \kappa_1$ where ρ, σ are the reduced density matrices of $|C\rangle = C\,|0^{2n}\rangle\,, |D\rangle = D\,|0^{2n}\rangle$, respectively, on the first n qubits. Let $0 < \alpha \leq (1-\kappa_2)/(1-\kappa_1)$. Define the following states $|E\rangle\,, |F\rangle$ on $2(n+1)$ qubits where

$$\begin{aligned}|E\rangle &= \sqrt{\alpha}\,|0\rangle\,|C\rangle\,|0\rangle + \sqrt{1-\alpha}\,|1^{2(n+1)}\rangle\\ |F\rangle &= \sqrt{\alpha}\,|0\rangle\,|D\rangle\,|0\rangle + \sqrt{1-\alpha}\,|1^{2(n+1)}\rangle\ .\end{aligned}$$

Suppose that the state $\sqrt{\alpha}\,|0\rangle + \sqrt{1-\alpha}\,|1\rangle$ can be prepared using a circuit of size s. Then the following hold:

1. $|E\rangle$, $|F\rangle$ can be computed by circuits E, F of size $O(|C| + |D| + s)$;
2. $\mathrm{F}(\tau, \mu) \geq \kappa_2$ where τ, μ are the reduced density matrices of $|E\rangle\,, |F\rangle$ on the first $n+1$ qubits;
3. The canonical $(n+1)$-qubit Uhlmann isometry V for $(|E\rangle\,, |F\rangle)$ can be written as

$$V = U \otimes |0\rangle\!\langle 0| + \mathrm{id} \otimes |1\rangle\!\langle 1|$$

where U is the n-qubit canonical Uhlmann isometry for $(|C\rangle\,, |D\rangle)$.

Proof. We prove the first item. To compute the state $|E\rangle$, consider the circuit E on $2(n+1)$ qubits that does the following:

1. Initialize the first qubit in the state $\sqrt{\alpha}\,|0\rangle + \sqrt{1-\alpha}\,|1\rangle$.
2. Apply a CNOT from the first qubit to the last qubit.
3. Controlled on the first qubit being $|0\rangle$, run the n-qubit circuit C on qubits 2 through $n+1$.
4. Controlled on the first qubit being $|1\rangle$, apply a bitflip operator to qubits 2 through $n+1$.

Clearly the size of E is $O(|C| + s)$ where $|C|$ denotes the size of circuit C where by assumption there is a circuit of size s to initialize the first qubit. An analogous construction holds for $|F\rangle$.

For the second item, we have

$$\begin{aligned}\tau &= \alpha\,|0\rangle\!\langle 0| \otimes \rho + (1-\alpha)\,|1\rangle\!\langle 1| \otimes |1^n\rangle\!\langle 1^n|\\ \mu &= \alpha\,|0\rangle\!\langle 0| \otimes \sigma + (1-\alpha)\,|1\rangle\!\langle 1| \otimes |1^n\rangle\!\langle 1^n|\ .\end{aligned}$$

The fidelity between τ and μ can be bounded as $\mathrm{F}(\tau, \mu) = \alpha \mathrm{F}(\rho, \sigma) + 1 - \alpha \geq \alpha\kappa_1 + 1 - \alpha \geq \kappa_2$.

For the third item, recall that the canonical Uhlmann isometry (where we have set the cutoff η to 0) for $(|E\rangle\,, |F\rangle)$ is defined as

$$V = \mathrm{sgn}(\mathrm{Tr}_{\mathsf{A}'}(|E\rangle\!\langle F|))$$

where A' denotes the first $n+1$ qubits of $|E\rangle\,, |F\rangle$. This is equal to

$$\mathrm{sgn}\Big(\alpha \mathrm{Tr}_{\mathsf{A}}(|C\rangle\!\langle D|) \otimes |0\rangle\!\langle 0| + (1-\alpha)\,|1^n\rangle\!\langle 1^n| \otimes |1\rangle\!\langle 1|\Big) = \mathrm{sgn}(\mathrm{Tr}_{\mathsf{A}}(|C\rangle\!\langle D|)) \otimes |0\rangle\!\langle 0| + |1^n\rangle\!\langle 1^n| \otimes |1\rangle\!\langle 1|$$

where A denotes the first n qubits of $|C\rangle\,, |D\rangle$. To conclude, note that $\mathrm{sgn}(\mathrm{Tr}_{\mathsf{A}}(|C\rangle\!\langle D|))$ is the canonical Uhlmann isometry for $(|C\rangle\,, |D\rangle)$. □

Lemma 6.7 (Reductions for $\textsc{DistUhlmann}_\kappa$ for different fidelities κ)**.** Let $\kappa : \mathbb{N} \to [0,1]$ be such that $1/p(n) \leq \kappa(n) \leq 1 - 1/p(n)$ for all n for some polynomial $p(n)$. Then $\textsc{DistUhlmann}_\kappa$ polynomial-time reduces to $\textsc{DistUhlmann}_{1-1/p}$.

Proof. For every valid $\textsc{Uhlmann}_\kappa$ instance $x = (1^n, C, D)$, let $y = (1^{2(n+1)}, E, F)$ denote the valid $\textsc{Uhlmann}_{1-1/p}$ instance given by the padding trick (Lemma 6.6), where $\alpha(n) = 1/p(n)$. The state $\sqrt{\alpha(n)}\,|0\rangle + \sqrt{1-\alpha(n)}\,|1\rangle$ can be prepared with circuits of size $O(\log n)$ by the Solovay-Kitaev theorem, so by Lemma 6.6 E and F are also polynomial-sized (in n) circuits. Furthermore, given explicit descriptions of C, D one can efficiently compute explicit descriptions of E, F.

In order to prove the theorem, by Definition 3.18, for every precision r we need to find another precision r' (which can be polynomial in r and n) and a polynomial-time quantum query algorithm A^* such that any $1/r'$-error average case instantiation (see Definition 3.14) of $A^{\textsc{DistUhlmann}}_{1-1/p}$ implements $\textsc{DistUhlmann}_{1/p}$ with average-case error $1/r$.

We define $A^* = (A^*_x)_x$ as follows. The circuit A^*_x takes as input an n-qubit register B and initializes a single-qubit register F in the state $|0\rangle$. It then applies the $\textsc{DistUhlmann}_{1-1/p}$ oracle for instance y (whose description can be efficiently computed from x) on registers FB and outputs the result.

To show that this implements $\textsc{DistUhlmann}_{1/p}$, let $r' = p(n)r$, and let $A^{\textsc{DistUhlmann}_{1-1/p}}$ denote a $1/r'$-error average-case instantiation. Concretely, let V_y denote the (exact) Uhlmann partial isometry for instance y and let $H = (H_y)_y$ denote a quantum algorithm that implements $\textsc{DistUhlmann}_{1-1/p}$ with average-case error $1/r'$ and is used to instantiate the $\textsc{DistUhlmann}_{1-1/p}$-oracle. This means there is a channel completion Φ_y of V_y such that

$$\mathrm{td}\Big((\mathrm{id} \otimes H_y)(|E\rangle\!\langle E|), (\mathrm{id} \otimes \Phi_y)(|E\rangle\!\langle E|)\Big) \leq \frac{1}{r'}\,.$$

By the third item of Lemma 6.6, any channel completion Φ_y of V_y can be turned into a channel completion of Ξ_x of U_x, the $\textsc{Uhlmann}_\kappa$ transformation corresponding to $(|C\rangle, |D\rangle)$. Define $\Xi_x(\rho) := \mathrm{Tr}_{\mathsf{G}}(\Phi_x(\rho \otimes |0\rangle\!\langle 0|_{\mathsf{G}}))$ where G denotes the last qubit. Let Π denote the support onto U_x. Then $\Xi_x(\Pi\rho\Pi) = \mathrm{Tr}_{\mathsf{G}}(\Phi_x(\Pi\rho\Pi \otimes |0\rangle\!\langle 0|_{\mathsf{G}}))$. But notice that the state $\Pi\rho\Pi \otimes |0\rangle\!\langle 0|$ is contained in the support of V_y; therefore

$$\mathrm{Tr}_{\mathsf{G}}(\Phi_x(\Pi\rho\Pi \otimes |0\rangle\!\langle 0|)) = \mathrm{Tr}_{\mathsf{G}}\Big(V_y(\Pi\rho\Pi \otimes |0\rangle\!\langle 0|)V_y^\dagger\Big) = U_x \rho U_x^\dagger$$

where we used the expression for V_y given by Lemma 6.6. Thus we can evaluate the performance of the instantiation $A^{\textsc{DistUhlmann}_{1-1/p}}$ on the input $|C\rangle$:

$$\begin{aligned}
&\mathrm{td}\Big((\mathrm{id} \otimes A_x^{\textsc{DistUhlmann}_{1-1/p}})(|C\rangle\!\langle C|),\, (\mathrm{id} \otimes \Xi_x)(|C\rangle\!\langle C|)\Big)\\
&= \mathrm{td}\Big((\mathrm{id} \otimes H_y)(|0\rangle\!\langle 0| \otimes |C\rangle\!\langle C| \otimes |0\rangle\!\langle 0|),\, (\mathrm{id} \otimes \Phi_y)(|0\rangle\!\langle 0| \otimes |C\rangle\!\langle C|) \otimes |0\rangle\!\langle 0|\Big)\\
&= \frac{1}{\alpha(n)}\mathrm{td}\Big((\mathrm{id} \otimes H_y)(P\,|E\rangle\!\langle E|\,P^\dagger),\, (\mathrm{id} \otimes \Phi_y)(P\,|E\rangle\!\langle E|\,P^\dagger)\Big)\\
&\leq \frac{1}{\alpha(n)}\mathrm{td}\Big((\mathrm{id} \otimes H_y)(|E\rangle\!\langle E|),\, (\mathrm{id} \otimes \Phi_y)(|E\rangle\!\langle E|)\Big)\\
&\leq \frac{1}{\alpha(n)r'} = \frac{1}{r}\,.
\end{aligned}$$

In the second line, we expanded the definitions of the query circuit A_x and the channel completion Ξ_x. In the third line, we define the projector $P = |0\rangle\!\langle 0|$ which acts on the first qubit so that $|0\rangle\,|C\rangle\,|0\rangle = \frac{1}{\sqrt{\alpha(n)}}P\,|E\rangle$. In the fifth line we used the guarantees about the algorithm H_y and our definitions of $\alpha(n), r'$. □

The padding trick shows that $\textsc{Uhlmann}_\kappa$ and $\textsc{DistUhlmann}_\kappa$ are equivalent in complexity whenever κ is bounded away from 0 or 1 by an inverse polynomial. It could be that there are (at least) three different complexities between $\textsc{DistUhlmann}_{\mathrm{negl}}$, $\textsc{DistUhlmann}_{1/2}$, and $\textsc{DistUhlmann}_{1-\mathrm{negl}}$. This leads to the following natural questions:

1. What is the complexity of $\textsc{DistUhlmann}_\kappa$ for negligibly small κ?
2. What is the complexity of $\textsc{DistUhlmann}_\kappa$ for $\kappa = 1 - \mathrm{negl}(n)$?
3. Is the complexity of $\textsc{DistUhlmann}_{1/2}$ the same as the complexity of $\textsc{DistUhlmann}_{1-\mathrm{negl}}$?

In the next section we explore an approach to answering the last two questions.

6.3 A polarization lemma for Uhlmann transformations?

The padding trick is reminiscent of a result in complexity theory and cryptography called the *polarization lemma*. This is used to show complete problems for SZK and QSZK [SV03, Wat02], the analogous decision classes to $\mathsf{avgUnitaryHVSZK}$. The complete problem for QSZK is $\textsc{QuantumStateDistinguishing}$ [Wat02], where one is given a pair of quantum circuits (C, D) that generate mixed states (ρ, σ), and one has to decide whether $\mathrm{td}(\rho, \sigma) \leq 1/3$ (the "yes" case) or $\mathrm{td}(\rho, \sigma) \geq 2/3$ (the "no" case), promised that one is the case. The polarization lemma yields an efficient transformation from (C, D) that produces two circuits (C', D') generating mixed states (ρ', σ') such that in the "yes" case, $\mathrm{td}(\rho', \sigma') \leq 2^{-n}$, whereas in the "no" case, $\mathrm{td}(\rho', \sigma') \geq 1 - 2^{-n}$. Thus, if one can distinguish between circuit descriptions in the highly polarized case (i.e., the two density matrices are either exponentially close or exponentially far), then one can efficiently distinguish between the mildly polarized case.

The analogous statement in the unitary complexity setting would be to have an efficient polynomial-time reduction from (say) $\textsc{DistUhlmann}_{1/2}$ to (say) $\textsc{DistUhlmann}_{1-2^{-n}}$. That is, implementing the Uhlmann transformation for an instance $(1^n, C, D)$ where the reduced density matrices of $|C\rangle, |D\rangle$ have fidelity $1/2$ can be efficiently reduced to implementing Uhlmann transformations for instances with high fidelity $1 - 2^{-n}$. We conjecture that such a transformation is possible.

Conjecture 6.8 (Polarization for the Uhlmann Transformation Problem)**.** For all polynomials $p(n)$, there exists a polynomial-time reduction from $\textsc{DistUhlmann}_{1/2}$ to $\textsc{DistUhlmann}_{1-2^{-p(n)}}$.

One might hope that with such a polarization lemma, one can show completeness of $\textsc{DistUhlmann}_{1/2}$ for $\mathsf{avgUnitaryHVSZK}$ (for some choice of completeness, soundness, and simulation error), which is like $\mathsf{avgUnitaryHVPZK}$ except the completeness and simulation errors may not be zero. Showing *hardness* of $\textsc{DistUhlmann}_{1/2}$ for $\mathsf{avgUnitaryHVSZK}$ is straightforward, using similar ideas to Theorem 6.5. However it is unclear how to use the conjectured polarization lemma to argue that $\textsc{DistUhlmann}_{1/2}$ has a statistical zero-knowledge protocol; the trouble is that we don't know if $\mathsf{avgUnitaryHVSZK}$ is closed under polynomial-time reductions (as discussed in Section 4.4.3).

However, the conjectured polarization lemma *does* imply a slightly weaker notion of completeness:

Lemma 6.9. Let $c = 1 - 2^{-\mathrm{poly}(n,r)}$ and $s = \frac{1}{2}$. Assuming Conjecture 6.8, for all inverse polynomials $\kappa(n)$,

1. All problems in $\mathsf{avgUnitaryHVSZK}_{c,s}$ are polynomial-time reducible to $\textsc{DistUhlmann}_\kappa$, and
2. $\textsc{DistUhlmann}_\kappa$ is polynomial-time reducible to a problem in $\mathsf{avgUnitaryHVSZK}_{c,s}$.

Proof. We sketch the proof. The first item follows from the fact that $\mathsf{avgUnitaryHVSZK}_{c,s}$ is polynomial-time reducible to $\textsc{DistUhlmann}_{1-2^{-(n+r)}}$ using a very similar proof to Theorem 6.5, and $\textsc{DistUhlmann}_{1-2^{-(n+r)}}$ is trivially reducible to $\textsc{DistUhlmann}_{\kappa}$ for any inverse polynomial $\kappa(n)$.

The second item directly follows from the conjectured polarization lemma, and the fact that $\textsc{DistUhlmann}_{1-2^{-(n+r)}}$ is contained in $\mathsf{avgUnitaryHVSZK}$ using Protocol 1, and a similar analysis. □

We give evidence for Conjecture 6.8 by proving a *weak* polarization lemma for Uhlmann transformations.

Theorem 6.10. Let $p(n)$ be a polynomial. Suppose there is a polynomial-time algorithm Q that implements $\textsc{DistUhlmann}_{1-2^{-p(n)}}$ with average-case error at most $1/32$. Then for all $0 < \epsilon < 1$ there exists a quantum algorithm $A = (A_x)_{x \in \{0,1\}^*}$ that runs in $n^{O(1/\epsilon)}$ time, makes queries to the unitary purification of Q and its inverse, such that for all valid instances $x = (1^n, C, D)$ of $\textsc{Uhlmann}_{1/2}$,

$$\mathrm{F}((\mathrm{id} \otimes A_x)(|C\rangle\langle C|), |D\rangle\langle D|) \geq \frac{1}{2} - \epsilon\,.$$

We prove Theorem 6.10 in Appendix A. We compare Theorem 6.10 with Conjecture 6.8. The main difference is that the algorithm A for $\textsc{Uhlmann}_{1/2}$ instances runs in time that scales *exponentially* with the (inverse) precision parameter $1/\epsilon$, whereas Conjecture 6.8 posits that there is an implementation of $\textsc{DistUhlmann}_{1/2}$ that runs in time $\mathrm{poly}(n, 1/r)$ where r is the precision parameter (here we think of $\epsilon = 1/r$). Finally, one might also wonder why the conclusion of Theorem 6.10 is not expressed as "A implements $\textsc{DistUhlmann}_{1/2}$ with error ϵ". The reason is that while A maps $|C\rangle$ to having near-optimal overlap with $|D\rangle$, it is no longer clear that A must be close to the canonical Uhlmann transformation corresponding to (C, D); Proposition 5.8 which connects the two notions only works in the *high κ regime*.[17]

Nonetheless, Theorem 6.10 does achieve a nontrivial guarantee: being able to perform Uhlmann transforms for $\textsc{Uhlmann}_{1-2^{-\mathrm{poly}(n)}}$ instances with some fixed constant error (i.e., $1/32$) can be efficiently converted into Uhlmann transformations for $\textsc{Uhlmann}_{1/2}$ instances with arbitrarily small constant error.

7 Complexity of the Succinct Uhlmann Transformation Problem

In this section, we show that the $\textsc{DistSuccinctUhlmann}_1$ problem is complete for both $\mathsf{avgUnitaryPSPACE}$ and $\mathsf{avgUnitaryQIP}$. We do this by establishing the following statements:

1. $\textsc{DistSuccinctUhlmann}_1 \in \mathsf{avgUnitaryQIP}$ (Lemma 7.2).

2. $\mathsf{avgUnitaryPSPACE}$ polynomial-time reduces to $\textsc{DistSuccinctUhlmann}_1$ (Lemma 7.5).

3. $\mathsf{avgUnitaryQIP} \subseteq \mathsf{avgUnitaryPSPACE}$ (Lemma 7.8).

These statements together imply the desired completeness results, as well as the equality $\mathsf{avgUnitaryQIP} = \mathsf{avgUnitaryPSPACE}$ (Theorem 7.10). This also allows us to show that $\mathsf{avgUnitaryQIP}$ is closed under polynomial-time reductions, which addresses a question raised in Section 3.6.4.

[17] This is related to a question of whether Uhlmann transforms are *rigid*; must near-optimal Uhlmann transforms for a pair of states be close to the corresponding canonical Uhlmann transform?

7.1 Interactive synthesis of succinct Uhlmann transformations

We first show that $\textsc{DistSuccinctUhlmann}_1 \in \mathsf{avgUnitaryQIP}_{c,s}$ for $c = 1 - 2^{-\mathrm{poly}(n,r)}$ and $s = 1/2$. The protocol mirrors that of Protocol 1 (the $\mathsf{avgUnitaryHVPZK}$ protocol for $\textsc{DistUhlmann}_1$), except that the circuits C and D are no longer polynomial size since now they are specified succinctly. As a result, the polynomial time verifier can no longer efficiently prepare copies of the state $|C\rangle$ and can no longer directly implement the unitary $D^\dagger$ to check that the Uhlmann transformation was applied correctly; these were critical steps in Protocol 1.

To address the first issue, we leverage the $\mathsf{statePSPACE} \subseteq \mathsf{stateQIP}$ result of [RY22, Ros24], so by interacting with the prover, the verifier approximately synthesizes the input state $|C\rangle$. To solve the second issue, we show that the verifier can approximately perform the measurement $\{|D\rangle\langle D|, \mathrm{id} - |D\rangle\langle D|\}$ using copies of $|D\rangle$ as a resource; again we use $\mathsf{statePSPACE} = \mathsf{stateQIP}$ to show that the verifier can prepare copies of $|D\rangle$ with the help of the prover. We describe these solutions in more detail next.

Interactive state synthesis. First we recall Rosenthal's interactive state synthesis protocol [Ros24] (improving upon the state synthesis protocol of [RY22]), which can synthesize any state sequence $(|\psi_x\rangle)_x \in \mathsf{statePSPACE}$. We describe this result at a high level (for formal details see [Ros24]): for every $\mathsf{statePSPACE}$ state sequence $(|\psi_x\rangle)_x$ there exists a polynomial-time quantum verifier $V = (V_{x,q})_{x,q}$ such (a) there exists an honest prover P^* that is accepted by the verifier with probability 1 (*perfect completeness*), (b) after interacting with the honest prover P^*, conditioned on accepting, the verifier outputs a state that is at most $2^{-(n+q)}$-close to $|\psi_x\rangle$ (*honest closeness*)[18], and (c) for all provers P that are accepted with probability at least $\frac{1}{2}$, the output register of the verifier is close to $|\psi_x\rangle$ within $1/q$ in trace distance (*soundness*).

In what follows we utilize as a subroutine the interactive state synthesis protocol for the sequence $(|C\rangle)_{\hat{C}}$ which is indexed by all succinct descriptions $\hat{C}$ of a unitary circuit C and $|C\rangle$ is the corresponding output state of the circuit (given all zeroes). It is straightforward to see that $(|C\rangle) \in \mathsf{statePSPACE}$, and therefore there is a $\mathsf{stateQIP}$ protocol to synthesize the state family.

Approximate reflections from copies of a state. To perform the measurement $\{|D\rangle\langle D|, \mathrm{id} - |D\rangle\langle D|\}$ on a state ρ, it suffices to initialize an ancilla qubit $|+\rangle$, and controlled on the ancilla qubit perform the reflection $\mathrm{id} - 2|D\rangle\langle D|$ on ρ. By performing a Hadamard on the ancilla qubit and measuring it, the desired measurement $\{|D\rangle\langle D|, \mathrm{id} - |D\rangle\langle D|\}$ is performed. The (controlled) reflection $\mathrm{id} - 2|\psi\rangle\langle\psi|$ can be approximately performed given copies of the state $|D\rangle\langle D|$, via the following result from Ji, Liu, Song [JLS18, Theorem 5].

Theorem 7.1 (Approximate reflections from copies of a state [JLS18])**.** Let $|\psi\rangle$ be a state and let A^R be an algorithm that takes as input a register A and makes q (possibly controlled) queries to the reflection oracle $R = \mathrm{id} - 2|\psi\rangle\langle\psi|$. Then for all integers $\ell > 0$ there exists an algorithm B that takes as input a register A in addition to $|\psi\rangle^{\otimes \ell}$ and makes no queries to R, such that for all input states ρ_{EA}

$$\mathrm{td}\Big((\mathrm{id}_{\mathsf{E}} \otimes A^R)(\rho_{\mathsf{EA}}), (\mathrm{id}_{\mathsf{E}} \otimes B)(\rho_{\mathsf{EA}} \otimes |\psi\rangle\langle\psi|^{\otimes \ell})\Big) \leq \frac{2q}{\sqrt{\ell+1}}.$$

Furthermore, if A^R is an algorithm such that performs the measurement $\{|\psi\rangle\langle\psi|, \mathrm{id} - |\psi\rangle\langle\psi|\}$ on the input register A, then $B(|\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi|^{\otimes \ell})$ accepts with probability 1.

[18] We note that this honest closeness property is not part of our definition of $\mathsf{stateQIP}$ in Definition 2.12, but it is an additional property guaranteed by [Ros24].

The "furthermore" part of the theorem statement above comes from examining the algorithm B described in [JLS18], which for every query to R performs a reflection about the symmetric subspace on $\ell+1$ registers.

Augmenting the protocol from Protocol 1 with the interactive state synthesis and the approximate reflections protocols enables us to prove the following.

Lemma 7.2. $\textsc{DistSuccinctUhlmann}_1 \in \mathsf{avgUnitaryQIP}_{c,s}$ for $c = 1 - 2^{-(n+r)}$, $s = 1/2$.

Proof. We present in Protocol 2 an $\mathsf{avgUnitaryQIP}$ protocol for $\textsc{DistSuccinctUhlmann}_1$ with completeness $1 - 2^{-(n+r)}$ and soundness $\frac{1}{2}$, where r is the precision parameter.

Protocol 2. Interactive protocol for $\textsc{DistSuccinctUhlmann}_1$

Instance: A valid $\textsc{SuccinctUhlmann}_1$ instance $x = (1^n, \hat{C}, \hat{D})$ specifying a succinct description of a pair of circuits (C, D) and precision r.
Input: Register B_0.

1. (***State synthesis***). Let $m = 64r^2 + 1$, $\ell = 2^{20} \cdot r^6$. Run the $\mathsf{stateQIP}$ protocol from [Ros24] to synthesize $|C\rangle^{\otimes m} \otimes |D\rangle^{\otimes \ell}$ with precision parameter $q = 8rn$. Let $\mathsf{A}_1\mathsf{B}_1 \cdots \mathsf{A}_m\mathsf{B}_m$ denote the registers for $|C\rangle^{\otimes m}$. If the $\mathsf{stateQIP}$ protocol rejects, reject.
2. (***Uhlmann transformation testing***). Sample $i^* \in [m]$ uniformly at random.
   (a) For $i = 1$ though m:
      i. If $i \neq i^*$, send register B_i to the prover and receive B_i back.
      ii. If $i = i^*$, send B_0 to the prover and receive B_0 back.
   (b) For $i \neq i^*$, use the approximate reflections protocol of Theorem 7.1 with the states $|D\rangle^{\otimes \ell}$ synthesized earlier to perform the measurement $\{|D\rangle\!\langle D|, \mathrm{id} - |D\rangle\!\langle D|\}$ on registers $\mathsf{A}_i\mathsf{B}_i$. If the $\mathrm{id} - |D\rangle\!\langle D|$ outcome is obtained for any i, then reject.
   (c) Otherwise, accept and output register B_0.

We show that the verifier described in Protocol 2 satisfies the required properties of $\mathsf{avgUnitaryQIP}$ protocols. First, the verifier runs in $\mathrm{poly}(n, r)$ time. This uses the fact that the $\mathsf{stateQIP}$ protocol and approximate reflection algorithm runs in $\mathrm{poly}(n, r)$ time, and the succinct descriptions of $|C\rangle^{\otimes m}$ and $|D\rangle^{\otimes \ell}$ are $\mathrm{poly}(n, r)$-sized in the lengths of the succinct descriptions $\hat{C}$ and $\hat{D}$. We now prove that the verifier satisfies the completeness and soundness properties.

□

Lemma 7.3 (Completeness)**.** For all valid $\textsc{SuccinctUhlmann}_1$ instances $x = (1^n, \hat{C}, \hat{D})$, precision parameter $r \in \mathbb{N}$, and sufficiently large n, there exists an honest prover P^* for Protocol 2 satisfying

$$\Pr[V_{x,r}(|C\rangle) \leftrightarrows P^*] \geq 1 - 2^{-(n+r)} .$$

Proof. We define an honest prover P^* for $\textsc{DistSuccinctUhlmann}_1$ as follows. Let $x = (1^n, \hat{C}, \hat{D})$ denote the $\textsc{SuccinctUhlmann}_1$ instance. In the state synthesis stage, P^* implements the honest prover in the $\mathsf{stateQIP}$ protocol for synthesizing $|C\rangle^{\otimes m} \otimes |D\rangle^{\otimes \ell}$, which has completeness 1 [Ros24]. In the Uhlmann transformation testing stage, in each of the m rounds P^* applies the canonical Uhlmann transformation U_x on the given register B (just like in Section 6).

We ignore the register B_0 for now, because it doesn't affect the acceptance probability of the verifier. By the honest closeness property of the protocol described in [Ros24], the state of the verifier after the first stage is $2^{-(n+q)}$-close to $|C\rangle^{\otimes m} \otimes |D\rangle^{\otimes \ell}$. Thus the state of the verifier after Step 2(a) of the protocol is $2^{-(n+q)}$-close to $|D\rangle^{\otimes m-1} \otimes |C\rangle \otimes |D\rangle^{\otimes \ell}$ where the first $m-1$ copies of $|D\rangle$ are from applying the honest prover to registers $\mathsf{A}_i\mathsf{B}_i$ for $i \neq i^*$, the lone copy of $|C\rangle$ is in register $\mathsf{A}_{i^*}\mathsf{B}_{i^*}$ (which was not sent over to the prover), and the last ℓ copies of $|D\rangle$ are from the state synthesis stage. By the "furthermore" part of Theorem 7.1, each of the (approximate) $\{|D\rangle\langle D|, \mathrm{id} - |D\rangle\langle D|\}$ measurements will succeed with probability at least $1 - 2^{-(n+q)}$. Thus the overall probability of acceptance is at least $1 - m2^{-(n+q)} \geq 1 - 2^{-(n+r)}$ for sufficiently large n (this uses our choices of m, q).

□

Lemma 7.4 (Soundness)**.** For all valid SUCCINCTUHLMANN$_1$ instances $x = (1^n, \hat{C}, \hat{D})$ and precision $r \in \mathbb{N}$, for sufficiently large n, for all quantum provers P, there exists a channel completion Φ_x of U_x such that

$$\text{if} \quad \Pr[V_{x,r}(|C\rangle) \leftrightarrows P \text{ accepts}] \geq \frac{1}{2} \qquad \text{then} \qquad \mathrm{td}(\sigma, (\Phi_x \otimes \mathrm{id})(|C\rangle\langle C|)) \leq \frac{1}{r},$$

where σ denotes the output of $V_{x,r}(|C\rangle) \leftrightarrows P$ conditioned on the verifier V_x.

Proof. Since $x = (1^n, \hat{C}, \hat{D})$ is a SUCCINCTUHLMANN$_1$ instance, by Proposition 5.3 $(\Phi_x \otimes \mathrm{id})(|C\rangle\langle C|) = |D\rangle\langle D|$ for all channel completions Φ_x of U_x, so it suffices to show that conditioned on accepting, the verifier outputs a state within $1/r$ of $|D\rangle$ in trace distance.

Let $\mathsf{A}_0\mathsf{B}_0$ denote the registers for the input state $|C\rangle$, so that A_0 is the reference register that is not accessed by either the prover or the verifier. Let P be a prover that is accepted with probability at least $1/2$. This means that the state synthesis stage is accepted with probability at least $1/2$, and the Uhlmann transformation testing stage is accepted with probability at least $1/2$ (conditioned on the first stage accepting). By the soundness property of the stateQIP protocol, the state of the verifier (plus reference system A_0), conditioned on acceptance of the state synthesis stage, is $1/q$-close to $|C\rangle^{\otimes(m+1)} \otimes |D\rangle^{\otimes \ell}$.

Let $\mathcal{P}$ denote the prover channel acting on registers $\mathsf{B}_0 \cdots \mathsf{B}_m$. Let $\mathcal{B}$ denote the channel corresponding to the approximate reflections protocol from Theorem 7.1 used in Step 2(b), that traces out the copies of $|D\rangle^{\otimes \ell}$ at the end. Let $\mathcal{A}$ denote the channel that performs the *exact* reflections instead of the approximate ones, which Theorem 7.1 guarantees is $2(m-1)/\sqrt{\ell+1}$-close to $\mathcal{B}$.

We consider a sequence of hybrids. Define ρ_0 to be the state of the verifier and registers $\mathsf{A}_0\mathsf{B}_0$ conditioned on the first stage accepting. Define $\rho_1 := |C\rangle\langle C|^{\otimes m+1} \otimes |D\rangle\langle D|^{\otimes \ell}$. Define

$$\sigma_b = \mathcal{B}\Big(\mathcal{P}(\rho_b)\Big)$$

for $b \in \{0, 1\}$. Note that σ_0 is the state of the verifier at the end of the protocol (but before conditioning on acceptance in the second stage). Define

$$\sigma_2 = \mathcal{A}\Big(\mathcal{P}(|C\rangle\langle C|^{\otimes m+1})\Big) .$$

Since $\mathrm{td}(\rho_0, \rho_1) \leq 1/q$, this means $\mathrm{td}(\sigma_0, \sigma_1) \leq 1/q$. By Theorem 7.1, $\mathrm{td}(\sigma_1, \sigma_2) \leq 2(m-1)/\sqrt{\ell+1}$. Since the probability of acceptance in the state σ_0 is at least $1/2$, the probability of acceptance in the state σ_2 is at least $1/2 - \delta$ for

$$\delta := \frac{1}{q} + \frac{2(m-1)}{\sqrt{\ell+1}} \leq \frac{1}{4r}$$

by our choices of q, m, ℓ.

Let $\tilde{\sigma}_b$ for $b \in \{0,1,2\}$ denote the states conditioned on acceptance of the second stage. The soundness analysis of the $\mathsf{avgUnitaryHVPZK}$ protocol in Lemma 6.3 shows that the $\mathsf{A}_0\mathsf{B}_0$ registers of $\tilde{\sigma}_2$ are $\sqrt{16/m}$-close to $|D\rangle$. Furthermore, [CY13, Lemma B.1] implies that

$$\mathrm{td}(\tilde{\sigma}_0, \tilde{\sigma}_2) \leq \frac{\mathrm{td}(\sigma_0, \sigma_2)}{\max\{p_0, p_2\}} \leq 2\mathrm{td}(\sigma_0, \sigma_2) \leq 2\delta\ .$$

where p_b denotes the probability of acceptance in σ_b, respectively. Thus, by our choice of m, ℓ, q, we have

$$\mathrm{td}\Big((\tilde{\sigma}_0)_{\mathsf{A}_0\mathsf{B}_0}\ , \ |D\rangle\!\langle D|\Big) \leq 2\delta + \sqrt{\frac{16}{m}} \leq \frac{1}{r}\ .$$

Note that $(\tilde{\sigma}_0)_{\mathsf{A}_0\mathsf{B}_0}$ is precisely the state of the reference register A_0 and the register output by the verifier conditioned on accepting. This concludes the proof of soundness.

□

7.2 Hardness for unitary polynomial space

We now show that DISTSUCCINCTUHLMANN$_1$ is hard for $\mathsf{avgUnitaryPSPACE}$.

Lemma 7.5. $\mathsf{avgUnitaryPSPACE}$ polynomial-time reduces to DISTSUCCINCTUHLMANN$_1$.

Proof. We show that any distributional unitary synthesis problem $(\mathscr{U} = (U_x)_x, \Psi = (\psi_x)_x) \in \mathsf{avgUnitaryPSPACE}$ can be reduced to implementing the Uhlmann transformation corresponding to a SUCCINCTUHLMANN$_1$ instance. The idea for this is natural: to implement U_x on ψ_x, we can simply perform the Uhlmann transformation corresponding to the pair of states $(|\psi_x\rangle, (\mathrm{id} \otimes U_x)|\psi_x\rangle)$.

There are, however, some subtleties in making this to work. Instances of SUCCINCTUHLMANN$_1$ are tuples $y = (1^n, \hat{C}, \hat{D})$ where $\hat{C}, \hat{D}$ are succinct descriptions of *unitary* circuits C, D, and furthermore the states $|C\rangle, |D\rangle$ have *identical* reduced density matrices on the first register. Even though $(\mathscr{U}, \Psi) \in \mathsf{avgUnitaryPSPACE}$, *a priori* the unitary U_x can only be *approximately* implemented and the state ψ_x can only be *approximately* prepared. Therefore, it seems that we can only compute succinct descriptions of circuits that approximately prepare $|\psi_x\rangle$ and $(\mathrm{id} \otimes U_x)|\psi_x\rangle$. Additionally, these circuits are not necessarily unitary (since the circuits used to synthesize $|\psi_x\rangle$ and U_x may have measurements, resets, and other non-unitary operations). Thus, these succinct descriptions do not directly constitute a SUCCINCTUHLMANN$_1$ instance.

We give a sketch of how we handle these issues. From the instance x of $(\mathscr{U}, \Psi)$ we compute an instance $y = (1^n, \hat{C}, \hat{D})$ of SUCCINCTUHLMANN$_1$ where C is a unitary circuit preparing a state close to $|\psi_x\rangle$, and D is a unitary circuit preparing the state $(\mathrm{id} \otimes A)|C\rangle$, with A being a another unitary circuit such that $(\mathrm{id} \otimes A)|\psi_x\rangle$ is close to $(\mathrm{id} \otimes U_x)|\psi_x\rangle$. Let W denote the canonical Uhlmann transformation corresponding to instance y. Then

$$\begin{aligned}
(\mathrm{id} \otimes W)|\psi_x\rangle &\approx (\mathrm{id} \otimes W)|C\rangle && (|\psi_x\rangle \approx |C\rangle)\\
&= |D\rangle = (\mathrm{id} \otimes A)|C\rangle && (\text{Proposition 5.3})\\
&\approx (\mathrm{id} \otimes A)|\psi_x\rangle && (|\psi_x\rangle \approx |C\rangle)\\
&\approx (\mathrm{id} \otimes U_x)|\psi_x\rangle\ . && (\text{Definition of } A)
\end{aligned}$$

Thus, implementing the canonical Uhlmann transformation W corresponding to y is sufficient for approximately implementing U_x on $|\psi_x\rangle$.

The key behind making this sketch work is the following "algorithmic Uhlmann's theorem" of Metger and Yuen [MY23, Theorem 7.4]:

Theorem 7.6 (Algorithmic Uhlmann's theorem)**.** Let $\Psi_1 = (|\psi_x^{(1)}\rangle)_x, \Psi_2 = (|\psi_x^{(2)}\rangle)_x$ be in families of bipartite pure states in statePSPACE, where for each x, the states $|\psi_x^{(1)}\rangle$ and $|\psi_x^{(2)}\rangle$ have the same number of qubits. Then there exists a $\mathrm{poly}(|x|, r)$-space family of unitary circuits $K = (K_{x,r})_{x,r}$ such that

$$\left\| K_{x,r} |\psi_x^{(1)}\rangle |0 \cdots 0\rangle - |\psi_x^{(2)}\rangle |0 \cdots 0\rangle \right\|^2 \leq 2(1 - \sqrt{\mathrm{F}(\sigma_x^{(1)}, \sigma_x^{(2)})}) + 1/r ,$$

where the $|0 \cdots 0\rangle$ denote the appropriate number of ancilla qubits, and $\sigma_x^{(b)}$ denotes the reduced density matrix of $|\psi_x^{(b)}\rangle$ on the first half of qubits.

A useful corollary of this is that every statePSPACE family of states can be prepared by a polynomial-space *unitary* circuit that uses some ancillas.

Corollary 7.7 (Unitary preparation of statePSPACE families)**.** Let $(|\psi_x\rangle)_x \in \mathsf{statePSPACE}$. Then there exists a $\mathrm{poly}(|x|, r)$ unitary circuit family $K = \{K_{x,r}\}_{x,r}$ such that

$$\left\| K_{x,r} |0 \cdots 0\rangle - |\psi_x\rangle |0 \cdots 0\rangle \right\|^2 \leq \frac{1}{r} .$$

Proof. This follows from Theorem 7.6 by considering the Uhlmann transformation problem between the all zeroes state $|0 \cdots 0\rangle |0 \cdots 0\rangle$ and $|0 \cdots 0\rangle |\psi_x\rangle$. Clearly this pair of states is a fidelity-1 Uhlmann instance. □

In what follows, fix a parameter q and an instance x. Since $\Psi \in \mathsf{statePSPACE}$, by Corollary 7.7 there exists a $\mathrm{poly}(|x|, q)$-space circuit C such that

$$\left\| C |0 \cdots 0\rangle - |\psi_x\rangle |0 \cdots 0\rangle \right\|^2 \leq \frac{1}{q} .$$

Next, since $(\mathscr{U}, \Psi) \in \mathsf{avgUnitaryPSPACE}$, this means that for every x there is a unitary $\tilde{U}_x$ (acting on possibly more qubits than $|\psi_x\rangle$) such that

$$|\varphi_x\rangle := (\mathrm{id} \otimes \tilde{U}_x) |\psi_x\rangle |0 \cdots 0\rangle$$

is such that the marginal of $|\varphi_x\rangle$ is $1/q$-close to a channel completion of U_x applied to the second half of $|\psi_x\rangle$, and furthermore the state sequence $(|\varphi_x\rangle)_x$ is in statePSPACE.

Notice that the pair of states $(|\psi_x\rangle |0 \cdots 0\rangle , |\varphi_x\rangle)$ forms a fidelity-1 instance of the Uhlmann transformation problem. Thus, by the algorithmic Uhlmann's theorem (Theorem 7.6), there exists a $\mathrm{poly}(|x|, q)$-space *unitary* algorithm A such that

$$\left\| (\mathrm{id} \otimes A) |\psi_x\rangle |0 \cdots 0\rangle - |\varphi_x\rangle \right\|^2 \leq \frac{1}{q} .$$

Define the $\mathrm{poly}(|x|, q)$-space unitary circuit D that, starting with all zeroes, does the following:

1. Apply the circuit C, then

2. Apply the circuit A on the second half of the resulting state.

There are succinct descriptions $\hat{C}, \hat{D}$ of C, D, respectively, of $\mathrm{poly}(|x|, q)$-size. This follows from the fact that C and A are space-uniform[19].

Therefore by construction the instance $y = (1^n, \hat{C}, \hat{D})$ is a valid $\textsc{SuccinctUhlmann}_1$ instance. By the above argument, the canonical Uhlmann transformation W corresponding to y will map $|\psi_x\rangle |0 \cdots 0\rangle$ to be within $O(1/q)$ of $(\mathrm{id} \otimes \tilde{U}_x) |\psi_x\rangle |0 \cdots 0\rangle$, as desired.

Thus one can implement the distributional unitary synthesis problem $(\mathscr{U}, \Psi)$ as follows: given instance x, precision parameter r, and input register B, set $q = O(r)$, compute the instance $y = (1^n, \hat{C}, \hat{D})$ which depends on x, q, and call the $\textsc{DistSuccinctUhlmann}_1$ oracle on instance y, precision q, and input register B appended with sufficiently many zeroes. Every average-case instantiation of the $\textsc{DistSuccinctUhlmann}_1$ oracle will implement (a channel completion of) W up to error $1/q$. Thus result has error $O(1/q)$, which is at most $1/r$ if q is set large enough. This reduction can be computed in $\mathrm{poly}(|x|, r)$ time.

□

7.3 avgUnitaryQIP = avgUnitaryPSPACE

We first show that unitaries synthesizable using interactive protocols can also be synthesized in polynomial space, at least in the average-case setting. In what follows, recall that $\mathrm{negl}(n, r)$ means that this is a negligible function of $n + r$ (e.g., $2^{-(n+r)}$).

Lemma 7.8. For all $c, s : \mathbb{N} \times \mathbb{N} \to [0, 1]$ such that $c = 1 - \mathrm{negl}(n, r)$ and $c - s \geq \delta$ for some inverse polynomial function δ, we have that $\mathsf{avgUnitaryQIP}_{c,s} \subseteq \mathsf{avgUnitaryPSPACE}$.

Proof. Let $(\mathscr{U}, \Psi) \in \mathsf{avgUnitaryQIP}$. There exists a verifier $V = (V_{x,r})_{x,r}$ satisfying the properties of Definition 4.5. By the completeness property, there exists an honest prover P^* that is accepted with probability at least $c(n, r) = 1 - \mathrm{negl}(n, r)$. Let $p(n, r)$ be such that $c(n, r) - s(n, r) \geq 1/p(n, r)$ for all sufficiently large n, r.

If we can argue that there is a prover P that can be computed in quantum polynomial space that is accepted with probability at least $1 - \mathrm{negl}(n, r) - \frac{1}{4r}$ by V, then the following is a $\mathsf{avgUnitaryPSPACE}$ algorithm for $(\mathscr{U}, \Psi)$: given an instance x, precision parameter r, and an input register B_0, it runs the verifier V on instance x, precision parameter $2r$, and input register B_0. The $\mathsf{avgUnitaryPSPACE}$ algorithm simulates the prover as needed. At the end of the protocol, the verifier will accept with probability at least $1 - \mathrm{negl}(n, r) - \frac{1}{4r} \geq 1 - \frac{1}{2r} \geq \frac{1}{2}$ for large enough n, r. By the soundness of the verifier V, its output conditioned on acceptance is $1/2r$-close to the desired output. Since the acceptance probability is very high (at least $1 - 1/2r$ for large enough n, r), the output of the verifier (even without conditioning on acceptance) is $1/r$-close to the desired output.

All that remains is to argue that there is a polynomial-space simulation of the prover P^*. This essentially follows from [MY23, Theorem 7.1]:

Theorem 7.9 (Theorem 7.1 of [MY23])**.** Let $m(n)$ be a polynomial. Let $(V_x)_{x \in \{0,1\}^*}$ denote[20] a $m(|x|)$-round, $\mathrm{poly}(|x|)$-space verifier that starts with the all zeroes state. Let ω_x^* denote the optimal acceptance

[19] The succinct descriptions $\hat{C}, \hat{D}$ correspond to polynomial-*time* Turing machines that output the descriptions of polynomial-*space* circuits that compute the circuits C, D, and run them.

[20] Technically, Theorem 7.1 in [MY23] considers verifiers indexed by integers n, rather than strings x as we have written here, but inspection of the proof shows that the string-indexed version holds also.

probability over all provers that interact with the verifier. Then for all polynomials $q(|x|)$ there exists a prover P whose actions are computable in $\mathrm{poly}(|x|, q(|x|))$-space whose acceptance probability is at least $\omega_x^* - 1/q(|x|)$.

Although this theorem doesn't have an explicit r parameter, we can apply it to our verifier $V = (V_{x,r})_{x,r}$ by treating it as a sequence $(V_y)_{y \in \{0,1\}^*}$ where y encodes $(x, 1^r)$ and is of length $O(|x|+r)$, and furthermore the verifier initializes its input to the distributional state ψ_x. Since $\Psi \in \mathsf{statePSPACE}$, it can be prepared in polynomial space, and therefore V corresponds to a $\mathrm{poly}(|y|)$-space verifier as required by the theorem. □

We are now prove the main result of the section. This answers an average-case version of an open problem raised in [RY22, MY23], namely whether $\mathsf{unitaryQIP} = \mathsf{unitaryPSPACE}$, and is one of the first non-trivial results on relations between unitary complexity classes.

Theorem 7.10. $\mathsf{avgUnitaryPSPACE} = \mathsf{avgUnitaryQIP}$.

Proof. We put everything together to prove $\mathsf{avgUnitaryPSPACE} = \mathsf{avgUnitaryQIP}$. First, Lemma 7.8 directly shows that $\mathsf{avgUnitaryQIP} \subseteq \mathsf{avgUnitaryPSPACE}$. For the reverse inclusion, let $(\mathscr{U}, \Psi) \in \mathsf{avgUnitaryPSPACE}$. The proof of Lemma 7.5 shows that every instance x of the distributional unitary synthesis problem $(\mathscr{U}, \Psi)$ and precision parameter r can be mapped in $\mathrm{poly}(|x|, r)$-time to an instance $y = (1^n, \hat{C}, \hat{D})$ of $\textsc{SuccinctUhlmann}_1$ such that $|C\rangle \approx_{1/6r} |\psi_x\rangle |0 \cdots 0\rangle$ and $|D\rangle \approx_{1/6r} (\mathrm{id} \otimes \tilde{U}_x) |\psi_x\rangle |0 \cdots 0\rangle$ where $\tilde{U}_x$ is a Stinespring dilation of a channel that is close to a channel completion of U_x.

By Lemma 7.2, there is an interactive protocol for synthesizing the canonical Uhlmann transformation W corresponding to y. This interactive protocol can be run with instance y, precision parameter $q = 6r$, and half of $|\psi_x\rangle$ as input rather than $|C\rangle$. Let $V = (V_{y,q})_{y,q}$ denote the verifier and let P denote a prover that is accepted with probability at least $1/2$ when interacting with $V_{y,q}$ and input $|\psi_x\rangle$. Before conditioning on acceptance, we have that the output states of $V_{y,q}(|\psi_x\rangle) \leftrightarrows P$ and $V_{y,q}(|C\rangle) \leftrightarrows P$ are $1/6r$ close. Conditioning on acceptance only multiplies the closeness by at most 2, so the outputs are $2/6r$-close. However, by the soundness of the protocol, $V_{y,q}(|C\rangle) \leftrightarrows P$ conditioned on acceptance is $1/6r$-close to $|D\rangle$, which by definition is $1/6r$-close to $(\mathrm{id} \otimes \tilde{U}_x) |\psi_x\rangle |0 \cdots 0\rangle$. Adding up everything together, we have that conditioned on acceptance, the output of $V_{y,q}(|\psi_x\rangle) \leftrightarrows P$ is at $5/6r$-close to $(\mathrm{id} \otimes \tilde{U}_x) |\psi_x\rangle |0 \cdots 0\rangle$. After tracing out some qubits, the resulting state is $1/r$-close to a channel completion of U_x applied to $|\psi_x\rangle$. This concludes the proof of the soundness property.

The completeness of the protocol directly follows from Lemma 7.3. Therefore this implies that $(\mathscr{U}, \Psi) \in \mathsf{avgUnitaryQIP}$, as desired.

□

We record some easy corollaries of Theorem 7.10. First, as discussed in Section 3.6.4, the closure of the interactive unitary synthesis classes under polynomial-time reductions is not *a priori* obvious, but follows easily from $\mathsf{avgUnitaryPSPACE} = \mathsf{avgUnitaryQIP}$:

Corollary 7.11. $\mathsf{avgUnitaryQIP}$ is closed under polynomial-time reductions.

Proof. This follows since $\mathsf{avgUnitaryPSPACE}$ is closed under polynomial-time reductions (Lemma 3.23).

□

The next corollary records the centrality of the succinct Uhlmann transformation problem for these two unitary complexity classes.

Corollary 7.12. $\textsc{DistSuccinctUhlmann}_1$ is complete for $\mathsf{avgUnitaryPSPACE}$ and $\mathsf{avgUnitaryQIP}$.

Now, some questions for future work. The worst-case version of Theorem 7.10 remains open:

Open Problem 10. Does it hold that $\mathsf{unitaryQIP} = \mathsf{unitaryPSPACE}$?

Another interesting open question concerns the relationship between between traditional complexity theory and unitary complexity theory, and in particular the Uhlmann Transformation Problem:

Open Problem 11. $\textsc{SuccinctUhlmann} \in \mathsf{unitaryBQP}^{\mathsf{PSPACE}}$? This is closely related to the Unitary Synthesis Problem of [AK07] – not to be confused with our notion of unitary synthesis problems – which asks if there is a quantum algorithm A and for every n-qubit unitary U a boolean function $f : \{0,1\}^{\mathrm{poly}(n)} \to \{0,1\}$ such that the unitary U can be implemented by A^{f_U}.

Part III
Uhlmann Transformation Problem: Reductions

8 Quantum Cryptography

We show how our unitary complexity framework, and in particular the Uhlmann Transformation Problem, can be used to capture computational assumptions necessary for quantum cryptography. First, we show the security of quantum commitment schemes is *equivalent* to the average-case hardness of the Uhlmann Transformation Problem. We also show that if $\mathsf{avgUnitaryHVSZK}$ is hard on average, then secure quantum commitment schemes exist.

We then show that the hardness of the *succinct* Uhlmann Transformation Problem is necessary for the security of a wide class of quantum cryptographic primitives. This is the class of primitives whose security is based on *falsifiable quantum cryptographic assumptions*. Roughly speaking, a cryptographic assumption is falsifiable if there is an interactive security game with an efficient challenger that can check whether an assumption has been broken. In cryptography, generally speaking most assumptions are falsifiable, although there are some (e.g., knowledge assumptions) that are not.

By the results of Section 6, this means that $\mathsf{avgUnitaryBQP} \neq \mathsf{avgUnitaryPSPACE}$ is necessary for falsifiable quantum assumptions. This establishes the first general upper bound on the complexity of breaking (a large class of) computationally-secure quantum cryptography.

8.1 Quantum bit commitments

We first review the notion of quantum commitment schemes, and in particular the notion of a *canonical quantum bit commitment scheme*, which is a non-interactive protocol for bit commitment involving quantum communication. Yan [Yan22] showed that a general interactive quantum commitment scheme can always be compiled to a non-interactive commitment scheme with the same security properties. Thus without loss of generality we focus on such non-interactive schemes.

Definition 8.1 (Canonical quantum bit commitment [Yan22])**.** A *canonical non-interactive quantum bit commitment scheme* is given by a uniform family of unitary quantum circuits $\{C_{\lambda,b}\}_{\lambda\in\mathbb{N},b\in\{0,1\}}$ where for each λ, the circuits $C_{\lambda,0}, C_{\lambda,1}$ act on $poly(\lambda)$ qubits and output two registers C, R. The scheme has two phases:

1. In the *commit stage*, to commit to a bit $b \in \{0, 1\}$, the sender prepares the state $|\psi_{\lambda,b}\rangle_{\mathsf{RC}} = C_{\lambda,b} |0 \cdots 0\rangle$, and then sends the "commitment register" C to the receiver.
2. In the *reveal stage*, the sender announces the bit b and sends the "reveal register" R to the receiver. The receiver then accepts if performing the inverse unitary $C^{\dagger}_{\lambda,b}$ on registers C, R and measuring in the computational basis yields the all zeroes state.

The security of a canonical commitment scheme consists of two parts, hiding and binding, which we define next.

Definition 8.2 (Hiding property of commitment scheme)**.** Let $\epsilon(\lambda)$ denote a function. We say that a commitment scheme $\{C_{\lambda,b}\}_{\lambda,b}$ satisfies *ϵ-computational (resp. ϵ-statistical) hiding* if for all polynomial-time algorithms (resp. for all algorithms) $A = (A_\lambda)_\lambda$ that take as input the commitment register C of the scheme $\{C_{\lambda,b}\}_{\lambda,b}$, the following holds for sufficiently large λ:

$$\left| \Pr\left[A_\lambda(\rho_{\lambda,0}) = 1\right] - \Pr\left[A_\lambda(\rho_{\lambda,1}) = 1\right]\right| \leq \epsilon(\lambda)\,. \tag{8.1}$$

Here, $\rho_{\lambda,b}$ denotes the reduced density matrix of $|\psi_{\lambda,b}\rangle$ on register C. If ϵ is a negligible function of λ then we simply say that the scheme satisfies *strong* computational (resp. statistical) hiding.

Definition 8.3 (Honest binding property of commitment scheme)**.** Let $\epsilon(\lambda)$ denote a function. We say that a commitment scheme $\{C_{\lambda,b}\}_{\lambda,b}$ satisfies *ϵ-computational (resp. ϵ-statistical) honest binding* if for all polynomial-time algorithms (resp. for all algorithms) $A = (A_\lambda)_\lambda$ that take as input the reveal register R the following holds for sufficiently large λ:

$$\mathrm{F}\left(\left(A_\lambda \otimes \mathrm{id}_{\mathsf{C}}\right)(\psi_{\lambda,0}), \psi_{\lambda,1}\right) \leq \epsilon(\lambda)\,, \tag{8.2}$$

where $\psi_{\lambda,b} = |\psi_{\lambda,b}\rangle\langle\psi_{\lambda,b}|_{\mathsf{RC}}$.

If ϵ is a negligible function of λ then we simply say that the scheme satisfies *strong* computational (resp. statistical) honest binding.

Remark 8.4. Definition 8.3 is called *honest* binding because it requires the binding property only for the states $|\psi_{\lambda,b}\rangle$ that are produced if the commit phase is executed honestly. We refer to [Yan22] for a discussion of this definition and stronger versions thereof. Throughout this paper, we will only consider the honest binding property, so we will just drop the term "honest" for brevity.

Remark 8.5. The definitions of hiding and binding can easily be revised for non-uniform adversaries, perhaps even with quantum side information, but for simplicity we focus on uniform adversaries. The more general security notion would correspond to unitary complexity classes with *advice*, e.g., $\mathsf{avgUnitaryBQP/poly}$ (i.e., non-uniformity via classical advice) or $\mathsf{avgUnitaryBQP/qpoly}$ (i.e., non-uniformity via quantum advice). We leave this for future work.

Before discussing the connection between the Uhlmann Transformation Problem and commitment schemes, we review several basic facts about them. First, information-theoretically secure quantum commitments do not exist:

Theorem 8.6 (Impossibility of unconditionally secure quantum commitments [May97, LC98])**.** There is no quantum commitment scheme that satisfies both strong statistical hiding and strong statistical binding.

Thus at least one of the hiding or binding must be computationally secure. There are two commonly considered *flavors* of quantum commitments: one with statistical hiding and computational binding, and the other with statistical binding and computational hiding. A remarkable fact about canonical quantum commitments is that there is a generic blackbox reduction between these two flavors [CLS01, Yan22, GJMZ23, HMY23].

Proposition 8.7 ([HMY23, Theorem 7])**.** Let $\epsilon(n), \delta(n)$ be functions. If C is an ϵ-computationally (resp. statistical) hiding and δ-statistical (resp. computational) binding commitment scheme, then there is an efficient black-box transformation of C into another commitment scheme C' that is a $\sqrt{\delta}$-statistical (resp. computational) hiding and ϵ-computationally (resp. statistical) binding commitment scheme.

Commitments and the Uhlmann Transformation Problem. The impossibility result of [May97, LC98] implies that information-theoretically secure quantum bit commitment schemes do not exist because Uhlmann transformations suffice to break the security of such schemes. We strengthen this to argue that the security of quantum commitments is *equivalent* to the *instance-average-case hardness* of the Uhlmann Transformation Problem.

First we define what we mean by instance-average-case hardness of a (distributional) unitary synthesis problem. Roughly speaking, this notion of average-case hardness stipulates that there is an efficiently sampleable distribution over *instances* x such that all polynomial-time algorithms fail to implement the unitary transformation U_x up to some inverse-polynomial error, with at least inverse-polynomial probability over instances sampled from the distribution. More precisely:

Definition 8.8 (Hard unitary synthesis instances)**.** Let $(\mathscr{U} = (U_x)_x, \Psi = (|\psi_x\rangle)_x)$ be a distributional unitary synthesis problem and let $D = (D_n)_{n\in\mathbb{N}}$ denote a uniform family of efficiently sampleable distributions over instances (i.e., D_n is a distribution over $\{0,1\}^n$ that can be sampled in polynomial time). We say that D is a *distribution of hard instances for* $(\mathscr{U}, \Psi)$ if there exists a polynomial $p(n)$ such that for all polynomial-time algorithms $A = (A_x)_x$ **Tony: Do we want to comment on the absence of the r parameter here?**, for all sufficiently large n, for all channel completions Φ_x of U_x we have

$$\Pr_{x\leftarrow D_n}\left[\mathrm{F}(A_x(\psi_x), \Phi_x(\psi_x)) \leq 1 - \frac{1}{p(n)}\right] \geq \frac{1}{p(n)} \, .$$

We say that $(\mathscr{U}, \Psi)$ *is instance-average-case hard for* $\mathsf{avgUnitaryBQP}$ if there exists an efficiently sampleable family of distributions of instances $D = (D_n)_n$ that is hard for it.

Remark 8.9. We emphasize that the "average" in the notion of "instance-average-case hard" is different from the "average" in the definition of $\mathsf{avgUnitaryBQP}$ or $\mathsf{avgUnitaryHVSZK}$. The former refers to the distribution over *instances* (i.e., the x subscripting U_x), whereas the latter refers to the distribution over *quantum inputs* (i.e., the mixed state that the unitary transformation U_x is applied to).

We now state the main theorem of this subsection.

Theorem 8.10. $\textsc{DistUhlmann}_{1-\epsilon}$ is instance-average-case hard for $\mathsf{avgUnitaryBQP}$ for some negligible function $\epsilon(n)$ if and only if quantum commitments with strong statistical hiding and strong computational binding exist.

Proof. We first prove the "if" direction (i.e., secure commitments implies the hardness of $\textsc{DistUhlmann}$). Let $C = \{C_{\lambda,b}\}$ denote a strong statistically hiding, strong computationally binding commitment scheme. Let D denote the distribution that on input 1^n, always outputs the pair $(C_{n,0}, C_{n,1})$ (i.e., D_n is a singleton distribution). The strong statistical hiding property of C implies that $(C_{n,0}, C_{n,1})$ (along with the distributional state $|C_{n,0}\rangle$) is a $\textsc{DistUhlmann}_{1-\epsilon}$ instance for some negligible function ϵ. The strong computational binding property implies that D is a distribution of hard instances for $\textsc{DistUhlmann}_{1-\epsilon}$.

Now we prove the "only if" direction (i.e., hardness of $\textsc{DistUhlmann}$ implies secure commitments). Let D denote an efficiently sampleable family of distributions of hard instances for $\textsc{DistUhlmann}_{1-\epsilon}$. These instances are strings x that encode pairs (C_0, C_1) of circuits outputting bipartite pure states $|C_0\rangle, |C_1\rangle$ respectively. First we will show that this implies the existence of a commitment with weak binding security; then we will amplify the security via parallel repetition [BQSY24].

For notational simplicity we fix the parameter n and let it be implicit throughout this proof. Let D_x denote the probability of sampling the $\textsc{DistUhlmann}_{1-\epsilon}$ instance $x = (C_0, C_1)$ from distribution D. Let

$\sum_x \sqrt{D_x}\,|x\rangle \otimes |\vartheta_x\rangle$ denote the purification of the sampling algorithm for D. Thus the following states can be prepared in polynomial time: for $b \in \{0,1\}$,

$$|\psi_b\rangle := \sum_{x \in \{0,1\}^n} \sqrt{D_x}\;|x\rangle \otimes |\vartheta_x\rangle \otimes |C_b\rangle \otimes |x\rangle\;.$$

Here, the division of registers of $|\psi_b\rangle$ are as follows: the initial $|x\rangle$, $|\vartheta_x\rangle$ registers and register A of $|C_b\rangle$ are designated the commitment register, and the register B of $|C_b\rangle$ as well as the last $|x\rangle$ register are designated the reveal register.

Thus $(|\psi_0\rangle, |\psi_1\rangle)$ denotes a candidate commitment scheme. We first argue that it is strongly statistically hiding. The reduced state of $|\psi_b\rangle$ on the commitment register is

$$\rho_b = \sum_x D_x\,|x\rangle\!\langle x| \otimes |\vartheta_x\rangle\!\langle\vartheta_x| \otimes \mathrm{Tr}_{\mathsf{B}}(|C_b\rangle\!\langle C_b|)\;.$$

Then we have

$$\mathrm{F}(\rho_0,\rho_1) \geq \sum_x D_x\;\mathrm{F}(\mathrm{Tr}_{\mathsf{B}}(|C_0\rangle\!\langle C_0|), \mathrm{Tr}_{\mathsf{B}}(|C_1\rangle\!\langle C_1|)) \geq 1-\epsilon(n)$$

where we used that (C_0, C_1) is a $\textsc{DistUhlmann}_{1-\epsilon}$ instance. By Fuchs-van de Graaf we have that the trace distance is at most $\sqrt{\epsilon(n)}$ which is still negligibly small, and thus the strong statistical hiding property holds.

We now argue that it is weakly computationally binding. Let A be a quantum polynomial-time algorithm acting only on register R. Then

$$\begin{aligned}\mathrm{F}((\mathrm{id}_{\mathsf{C}} \otimes A_{\mathsf{R}})(\psi_0), \psi_1) &= \sum_x D_x\;\mathrm{F}((\mathrm{id}_{\mathsf{A}} \otimes A_{\mathsf{R}})(|C_0\rangle\!\langle C_0| \otimes |x\rangle\!\langle x|), |C_1\rangle\!\langle C_1| \otimes |x\rangle\!\langle x|) \\ &\leq (1-\alpha) + \alpha\cdot\left(1-\frac{1}{p(n)}\right) = 1-\frac{\alpha}{p(n)}\end{aligned}$$

where α is the probability

$$\Pr_{x \leftarrow D}\left[\mathrm{td}(A(|C_0\rangle\!\langle C_0| \otimes |x\rangle\!\langle x|), |C_1\rangle\!\langle C_1|) \geq \frac{1}{p(n)}\right]$$

which is guaranteed to be at least $1/p(n)$ by the definition of hardness on average. Thus the above is at most $1 - 1/p(n)^2$.

We now amplify the binding security. Consider the repeated commitment $(|\psi_0\rangle^{\otimes t}, |\psi_1\rangle^{\otimes t})$ for $t = np(n)$. It was shown by [BQSY24, Corollary 1.2] that any efficient algorithm for the amplified commitment that maps $|\psi_0\rangle^{\otimes t}$ to have fidelity non-negligibly greater than $(1-1/p(n))^t \leq \exp(-\Omega(n))$ can be converted into an efficient algorithm that maps $|\psi_0\rangle$ to have fidelity greater than $1 - 1/p(n)$ with $|\psi_1\rangle$, breaking the binding security of the original commitment, which is a contradiction. Therefore the amplified commitment scheme has strong computational binding security. Its hiding security is still strong, since we've only repeated the commitment a polynomial number of times. □

By flavor switching (Proposition 8.7), we also get the equivalence between the instance-average-case hardness of the Uhlmann Transformation Problem and the existence of commitments with strong computational hiding and strong statistical binding.

Commitments and Unitary Zero-Knowledge. Given the close relationship between the Uhlmann Transformation Problem and zero-knowledge protocols for unitary synthesis (as explored in Section 6), one might also expect an equivalence between the existence of a hard problem in $\mathsf{avgUnitaryHVSZK}$ and the existence of secure quantum commitments.

We show one direction: the instance-average-case hardness of $\mathsf{avgUnitaryHVSZK}$ also implies the existence of secure commitments. This can be viewed as a quantum analogue of the result of Ostrovsky [Ost91], who showed that a hard-on-average problem in (classical) SZK implies the existence of one-way functions. The intuition is that a hard distribution over instances of some unitary synthesis problem in $\mathsf{avgUnitaryHVSZK}$ implies the existence of a hard distribution over instances of DISTUHLMANN.

Theorem 8.11. Let $c, s : \mathbb{N} \times \mathbb{N} \to [0,1]$ be such that $c - s \geq \Omega(1)$. Let $\nu = \mathrm{negl}(n,r)$. If $\mathsf{avgUnitaryHVSZK}_{c,s,\nu}$ is instance-average-case hard for $\mathsf{avgUnitaryBQP}$, then quantum commitments with strong statistical hiding and strong computational binding exist.

Proof. Let $(\mathscr{U} = (U_x), \Psi = (\psi_x))$ denote a distributional unitary synthesis problem in $\mathsf{avgUnitaryHVSZK}_{c,s,\nu}$ with a distribution D of hard instances where $p(n)$ is the associated polynomial. By definition, there exists a $m(n)$-round zero knowledge protocol (for some polynomial $m(n)$) for $(\mathscr{U}, \Psi)$ with an honest prover P, an (honest) verifier $V = (V_{x,r})_{x,r}$ and a simulator S with negligible error $\nu(n,r)$. Let us recall the behavior of the simulator: on input (x,r,j), the simulator outputs a purification $|C_{x,j}\rangle$ that is $\nu(n,r)$-close to the state of the honest verifier immediately after receiving the j'th message of the honest prover. We assume that $|C_{x,0}\rangle = |\psi_x\rangle \otimes |0\cdots 0\rangle$.

In what follows we fix r to be $4p(n)$, and omit its mention for notational convenience. Thus we write $V_x, \nu(n), (x,j)$ instead of $V_{x,r}, \nu(n,r), (x,r,j)$, etc.

Define the uniform family of distributions $E = (E_n)_n$ where E_n outputs a string y sampled as follows:

- x is sampled from D_n and j is a uniformly random integer between 0 and $m(n) - 1$.
- $y = (B_{x,j}, C_{x,j+1})$ encodes a pair of circuit descriptions where $B_{x,j} = (V_x \otimes \mathrm{id}) C_{x,j}$ with $C_{x,j}$ corresponding to the purified circuits (i.e., meaning ignoring measurements and partial traces) of the simulator S on input (x,j); and $C_{x,j+1}$ is the purified circuit of the simulator S on input $(x, j+1)$.

Since the simulator can be implemented by a polynomial-size circuit, the distribution family $(E_n)_n$ can be sampled in polynomial time.

Thus the purifications $|B_{x,j}\rangle$ and $|C_{x,j+1}\rangle$ are approximately consistent in the following sense: the reduced density matrix of $|C_{x,j+1}\rangle$ on the verifier's system has fidelity at least $1 - 4\nu(n)$ with the reduced density matrix of $|C_{x,j}\rangle$, evolved by the verifier's unitary V_x. This implies that the pair $y = (B_{x,j}, C_{x,j+1})$ defines an instance of $\text{UHLMANN}_{1-4\nu}$.

We now argue that E is a distribution of hard instances for $\text{DISTUHLMANN}_{1-4\nu}$. Suppose not. Then by definition of instances (and applying Fuchs-van de Graaf), for the polynomial $q(n) = 4m(n)p(n)^2$ there exists a quantum polynomial time algorithm $A = (A_y)_y$, an integer n, and a channel completion Φ_y of the canonical Uhlmann transformation for instance $y = (B_{x,j}, C_{x,j+1})$, such that

$$\mathop{\mathbb{E}}_{\substack{x \leftarrow D \\ j \leftarrow \{0,1,\ldots,m(n)-1\}}} I_{x,j} \leq \frac{1}{q(n)}$$

where $I_{x,j}$ denotes the indicator variable for the event $\mathrm{td}((A_y \otimes \mathrm{id})(|B_{x,j}\rangle\!\langle B_{x,j}|), (\Phi_y \otimes \mathrm{id})(|B_{x,j}\rangle\!\langle B_{x,j}|)) \geq O(\frac{1}{q(n)})$. Multiplying both sides by $m(n)$ and applying Markov's inequality, we get that with probability at most $\sqrt{m(n)/q(n)}$ we have a *bad* x, i.e., one where

$$\sum_{0 \leq j < m(n)} I_{x,j} > \sqrt{\frac{m(n)}{q(n)}} \,.$$

Otherwise, if x is *good*, then $\sum_{0 \leq j < m(n)} I_{x,j} \leq \sqrt{m(n)/q(n)} < 1$, but since $I_{x,j}$ is either 0 or 1, this implies that $I_{x,j} = 0$ for *all* j.

Note that when $I_{x,j} = 0$, we have that for all j,

$$\begin{aligned}
&\mathrm{td}((A_y \otimes \mathrm{id})(|B_{x,j}\rangle\!\langle B_{x,j}|), |C_{x,j+1}\rangle\!\langle C_{x,j+1}|) \\
&\quad \leq \mathrm{td}((A_y \otimes \mathrm{id})(|B_{x,j}\rangle\!\langle B_{x,j}|), (\Phi_y \otimes \mathrm{id})(|B_{x,j}\rangle\!\langle B_{x,j}|)) + \mathrm{td}((\Phi_y \otimes \mathrm{id})(|B_{x,j}\rangle\!\langle B_{x,j}|), |C_{x,j+1}\rangle\!\langle C_{x,j+1}|) \\
&\qquad \leq O(\frac{1}{q(n)}) + \sqrt{4\nu(n)} =: \xi(n)
\end{aligned}$$

where we used that any channel completion Φ_y of the canonical Uhlmann transformation achieves the optimal fidelity, plus Fuchs-van de Graaf. Note that the error $\xi(n)$ is $O(1/q(n))$ because $\nu(n)$ is negligble.

We now describe an efficient procedure F that, when x is good, simulates the prover in the avgUnitaryHVSZK protocol to implement the unitary U_x on $|\psi_x\rangle$ with error smaller than $1/p(n)$. The idea is as follows: given input the target register of $|\psi_x\rangle$, evolve it forward by applying the verifier's circuit V_x along with some ancilla zeroes. The pure global state is $|B_{x,0}\rangle = V_x |\psi_x\rangle |0 \cdots 0\rangle$. Applying A_{y_0} for $y_0 = (B_{x,0}, C_{x,1})$ to the prover and message registers of $|B_{x,0}\rangle$ we get a state that is $\xi(n)$-close to $|C_{x,1}\rangle$. Apply V_x to the verifier and message register to get a state that is $\xi(n)$-close to $|B_{x,1}\rangle$, and apply A_{y_1} for $y_1 = (B_{x,1}, C_{x,2})$ to simulate the second prover action, and so on. After $m(n)$ iterations we have a state that is $m(n)\xi(n)$-close to the final state of the interaction between an honest verifier and honest prover. Thus the acceptance probability of this state is at least $c - m(n)\xi(n)$, which for large enough n, is greater than s. Therefore by the soundness of the protocol, this final state is $1/r(n)$-close to the desired output state $(\mathrm{id} \otimes U_x) |\psi_x\rangle$ (perhaps with some junk state attached). Thus overall this procedure implements the transformation U_x on $|\psi_x\rangle$ up to trace distance error $m(n)\xi(n) + 1/r(n) < 1/2p(n)$, or (by Fuchs-van de Graaf) equivalent with fidelity at least $1 - 1/p(n)$.

Thus when sampling x from D we get a good x with probability at least $1 - \sqrt{m(n)/q(n)} \geq 1 - 1/2p(n)$, and in this case the polynomial-time procedure F implements U_x on $|\psi_x\rangle$ with fidelity at least $1 - 1/p(n)$. This contradicts the definition of D being a hard distribution for the unitary synthesis problem $(\mathscr{U}, \Psi)$.

Therefore E is a hard distribution of instances for DistUhlmann$_{1-4\nu}$. Theorem 8.10 then implies the existence of commitments with the desired security properties. □

Remark 8.12. We suspect that the converse of Theorem 8.11 holds; however this is closely related to the question of whether DistUhlmann is a complete problem for avgUnitaryHVSZK, which we can show if a polarization lemma holds for the Uhlmann Transformation Problem (see Section 6.3 for a discussion of this).

8.2 Falsifiable quantum cryptographic assumptions

In this section, we show an avgUnitaryPSPACE upper bound for breaking *falsifiable quantum cryptographic assumptions*, which can be seen as a quantum analogue of the notion of falsifiable assumption considered by Naor [Nao03] as well as Gentry and Wichs [GW11]. Morally having a falsifiable assumption means that the challenger in the security game must be efficient, so that if an adversary claims to break the security game, it is possible to verify that they have done so. Roughly speaking, we show that a falsifiable assumption is either *information-theoretically* secure (in which case, not even a computationally unbounded prover can win at the security experiment beyond a certain threshold), or it can be reduced to DISTSUCCINCTUHLMANN, and hence it can broken in avgUnitaryPSPACE (as shown in Section 7).

Our notion of a *falsifiable quantum cryptographic assumption* captures most cryptographic assumptions in both classical and quantum cryptography. The definition is essentially a QIP protocol, albeit cast in a cryptographic language. Instead of a *verifier*, we have a *challenger*; instead of a *prover*, we have an *adversary*. We formally define falsifiable quantum cryptographic assumptions as follows. We refer the reader to Section 4 for the formal definitions of quantum verifiers and interactive protocols.

Definition 8.13 (Falsifiable quantum cryptographic assumption)**.** A *falsifiable quantum cryptographic assumption* (or *falsifiable assumption* for short) is a pair $(\mathcal{C}, c)$ consisting of a polynomial-time quantum verifier $\mathcal{C} = (\mathcal{C}_x)_x$ (which we call the *challenger*) and a constant $c \in [0, 1]$. Given a string $x \in \{0, 1\}^*$,[21] the challenger $\mathcal{C}_x$ engages in an interaction with a prover $\mathcal{A}$ (which also gets the input x) called the *adversary*. At the end of the protocol, the challenger accepts or rejects. If the challenger accepts, we say that the adversary *wins*.

See Figure 1 for a depiction of an interaction between a challenger and adversary. We now describe the security property corresponding to a falsifiable assumption.

Definition 8.14 (Security of a falsifiable assumption)**.** A falsifiable assumption $(\mathcal{C}, c)$ is *computationally secure* (resp. *information-theoretically secure*) if for all polynomial-time (resp. computationally unbounded) adversaries $\mathcal{A}$, there exists a negligible function ν such that for all $x \in \{0, 1\}^*$, the probability that the adversary is accepted is at most $c + \nu(|x|)$ over the randomness of the interaction $\mathcal{C}_x \leftrightarrows \mathcal{A}$. We say that a (possibly inefficient) adversary $\mathcal{A}$ *breaks instance x of the assumption* $(\mathcal{C}, c)$ *with advantage* δ if $\Pr\left(\mathcal{C}_x \leftrightarrows \mathcal{A} \text{ accepts}\right) \geq c + \delta$.

Here are some (informally-described) examples of falsifiable quantum cryptographic assumptions.

1. (*Public-key quantum money*) Consider a candidate public-key quantum money scheme (see [Aar16, Lectures 8 and 9] for a longer discussion of quantum money). The assumption here is the pair $(\mathcal{C}^{\$}, 0)$. The challenger $\mathcal{C}^{\$}$ first generates a random money state along with the serial number and sends both to the adversary (while remembering the serial number). The adversary wins if it can send back two states (which may be entangled) that both pass the money scheme's verification procedure.

2. (*Pseudorandom states*) Consider a candidate pseudorandom state generator G [JLS18]. The assumption here is $(\mathcal{C}^{\mathrm{PRS}}, \frac{1}{2})$ where the instances x specify the security parameter λ as well as a positive integer t. The challenger $\mathcal{C}^{\mathrm{PRS}}$, given $x = (1^\lambda, 1^t)$, either sends to the adversary t copies of a pseudorandom state or t copies of a Haar-random state (which can be done efficiently using, e.g., t-designs [AE07]). The adversary wins if it can guess whether it was given pseudorandom states or Haar-random states.

[21] Here, x should be taken as the security parameter in unary 1^λ, and perhaps in addition expected format of the interaction. This includes for example, the number of queries that the adversary wishes to make (in a CCA security game for an encryption scheme as an example), or an upper bound on the message length sent by the adversary (in a collision finding security game as an example). The point of having x is so that the overall running time of the challenger is upper bounded by a *fixed* polynomial in $|x|$. Furthermore, since we allow arbitrary bitstrings, this should be regarded as auxiliary input to the cryptosystem.

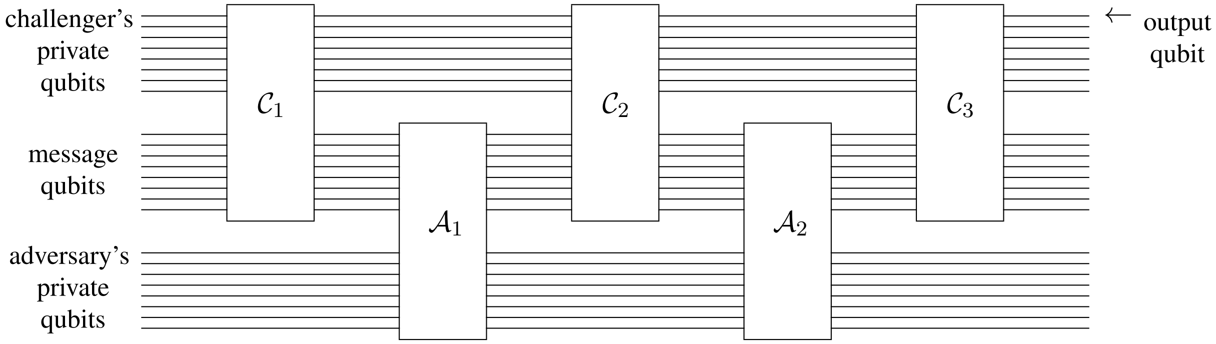

Figure 1: Quantum circuit representation of a 4-message interaction between an efficient challenger and an adversary who seeks to falsify a cryptrographic assumption $(\mathcal{C}, c)$.

3. (*Quantum EFI pairs*) Consider a candidate ensemble of EFI pairs $\{(\rho_{\lambda,0}, \rho_{\lambda,1})\}_\lambda$ [BCQ23]. The assumption here is $(\mathcal{C}^{\mathrm{EFI}}, \frac{1}{2})$. The challenge $\mathcal{C}^{\mathrm{EFI}}$ picks a random bit $b \in \{0,1\}$ and sends $\rho_{\lambda,b}$ to the adversary. The adversary wins if it can guess the bit b.

Theorem 8.15. A falsifiable quantum cryptographic assumption $(\mathcal{C}, c)$ is either information-theoretically secure, or breaking the assumption $(\mathcal{C}, c)$ can be reduced to $\textsc{DistSuccinctUhlmann}_1$.

Formally what we mean by "breaking the assumption can be reduced to $\textsc{DistSuccinctUhlmann}_1$" is the following: there exists an adversary A that is a polynomial time quantum query algorithm with access to a $\textsc{DistSuccinctUhlmann}_1$ oracle and breaks infinitely many instances x of the assumption $(\mathcal{C}, c)$ with advantage $1/p(|x|)$ for some polynomial p.

The proof of Theorem 8.15 is very similar to that of Theorem 6.5: again, the idea is that if we are considering a quantum interactive protocol, we can implement the prover's (or in this case adversary's) actions as Uhlmann unitaries. Hence, if there is any adversary that can break the falsifiable assumption, we can implement that adversary using a $\textsc{DistSuccinctUhlmann}_1$ oracle, so breaking the assumption reduces to $\textsc{DistSuccinctUhlmann}_1$. To make the paper more modular, we nonetheless spell out the details.

Proof of Theorem 8.15. Suppose that $(\mathcal{C}, c)$ is not in fact information-theoretically secure and there exists a possibly inefficient adversary $\mathcal{A}$ with at most $r = \mathrm{poly}(n)$ many rounds of interaction and a polynomial $p(n)$ such that

$$\Pr\left(\mathcal{C}_x \leftrightarrows \mathcal{A} \text{ accepts}\right) \geq c + 1/p(n)\,,$$

where $x \in \{0,1\}^*$ and $n = |x|$ for infinitely many x's. For each round $j \in \{1, \ldots, r\}$, we let

- $\rho^{(j)}_{\mathsf{M}^j_x \mathsf{W}^j_x}$ denote the state of the message register M^j_x and the private workspace W^j_x of the challenger $\mathcal{C}_x$ at the beginning of the challenger's j'th turn
- $\sigma^{(j)}_{\mathsf{M}^j_x \mathsf{W}^j_x}$ denote the state of the message register and the challenger's private workspace at the end of the challenger's j'th turn.

We now argue that the intermediate states on the message and challenger register in the interaction of $\mathcal{C}_x$ with $\mathcal{A}$ have purifications in $\mathsf{statePSPACE}$. From [MY23, Lemma 7.5], it follows that, for all x, there exists a prover $\mathcal{P}_x$ that is accepted with probability at least $c + 1/2p(n)$ for which the following property holds: there are families of pure states

$$(|\psi_{x,j}\rangle_{\mathsf{M}_x^j \mathsf{W}_x^j \mathsf{P}_x^j})_{x,j},\ |\varphi_{x,j}\rangle_{\mathsf{M}_x^j \mathsf{W}_x^j \mathsf{P}_x^j})_{x,j} \in \mathsf{statePSPACE}$$

for some purifying registers P_x^j that are purifications of intermediate states $\rho^{(j)}_{\mathsf{M}_x^j \mathsf{W}_x^j}$ and $\sigma^{(j)}_{\mathsf{M}_x^j \mathsf{W}_x^j}$ of the challenger $\mathcal{C}_x$ interacting with the prover $\mathcal{P}_x$. Moreover, there are polynomial-time Turing machines that, given as input a description of the verifier's actions in the protocol, output succinct classical descriptions of the quantum polynomial-space circuits for preparing $|\psi_{x,j}\rangle$ and $|\varphi_{x,j}\rangle$. This holds because [MY23, Lemma 7.5] only relies on the block-encoding transformations implemented in [MY23, Theorems 5.5 and 6.1], which have efficient (and explicit) descriptions.

This means that for each round j of the protocol, there exist polynomial-space quantum circuits C^j and D^j with efficiently computable succinct classical descriptions $\hat{C}^j$ and $\hat{D}^j$ such that $|\psi_{x,j}\rangle_{\mathsf{M_x^j W_x^j P_x^j}} = C^j |0 \dots 0\rangle$ and $|\varphi_{x,j}\rangle_{\mathsf{M_x^j W_x^j P_x^j}} = D^j |0 \dots 0\rangle$ are purifications of the reduced state on the message register $\mathsf{M_x^j}$ and challenger register $\mathsf{W_x^j}$ of the interactive protocol right before and after the prover's action in round j. Notice that because the challenger register in the interactive protocol is not acted upon by the prover, the reduced states on the challenger register are unchanged, i.e.

$$\mathrm{Tr}_{\mathsf{M_x^j P_x^j}}\left(|\psi_{x,j}\rangle\langle\psi_{x,j}|_{\mathsf{M_x^j W_x^j P_x^j}}\right) = \mathrm{Tr}_{\mathsf{M_x^j P_x^j}}\left(|\varphi_{x,j}\rangle\langle\varphi_{x,j}|_{\mathsf{M_x^j W_x^j P_x^j}}\right).$$

We can therefore interpret the circuit pair (C^j, D^j) as an instance of the SUCCINCTUHLMANN$_1$ problem, with $\mathsf{W^j}$ taking the role of the register that cannot be acted upon by the Uhlmann unitary. Hence, with access to a DISTSUCCINCTUHLMANN$_1$-oracle, we can apply an Uhlmann transformation mapping $|\psi_{x,j}\rangle_{\mathsf{M_x^j W_x^j P_x^j}}$ to $|\varphi_{x,j}\rangle_{\mathsf{M_x^j W_x^j P_x^j}}$ by acting only on registers $\mathsf{M_x^j P_x^j}$. This means that with the DISTSUCCINCTUHLMANN$_1$-oracle, we can efficiently implement the actions of a successful prover in the interactive protocol. □

9 Quantum Shannon Theory

We now relate the Uhlmann Transformation Problem to two fundamental tasks in quantum Shannon theory: decoding the output of quantum channels and compressing quantum information. We show that both of these tasks can be performed in polynomial time if the Uhlmann Transformation Problem can be implemented in polynomial time. We also prove that channel decoding is as hard as solving the Uhlmann transformation problem in the inverse polynomial error regime.

9.1 Decodable channels

We discuss the task of decoding the output of a channel (i.e. recovering the input to the channel from its output). We focus on channels that are *decodable*:

Definition 9.1 (Decodable channel)**.** Let $\epsilon > 0$. A channel $\mathcal{N}$ mapping register A to B is *ϵ-decodable* if there exists a (not necessarily efficient) quantum algorithm D that takes as input register B and outputs register A' isomorphic to A such that

$$\mathrm{F}\Big((D_{\mathsf{B}\to\mathsf{A}'} \circ \mathcal{N}_{\mathsf{A}\to\mathsf{B}})(|\Phi\rangle\langle\Phi|_{\mathsf{AR}}),\ |\Phi\rangle\langle\Phi|_{\mathsf{A}'\mathsf{R}}\Big) \geq 1 - \epsilon\,,$$

where $|\Phi\rangle_{\mathsf{AR}}$ is the maximally entangled state on registers AR.

Decodable channels naturally arise in the context of error corrected communication. Consider a noisy channel $\mathcal{C}$, and a encoder $\mathcal{E}$ corresponding to a quantum error correcting code. There are general situations when the concatenated channel $\mathcal{C} \circ \mathcal{E}$ is decodable, e.g., for example if $\mathcal{C}$ is a tensor-product Pauli channel and $\mathcal{E}$ is a random stabilizer code [Wil17, Theorem 24]. However, it is not clear whether the concatenated channel is efficiently decodable, even if the encoder $\mathcal{E}$ is efficient. In fact, it is known that decoding arbitrary classical linear codes and stabilizer codes is computationally intractable [Var97, BMV03, HL11, IP15].

Remark 9.2. We could also consider a generalization of Definition 9.1 where we consider states other than the maximally entangled state. However we focus on the maximally entangled state for simplicity, and it already illustrates the key ideas of our complexity result. It is known that using the maximally entangled state as the input to a coding scheme for a noisy channel is without loss of generality (up to small changes in capacity, see e.g. [Ren22, Chapter 15]).

We first show a sufficient and necessary condition for a channel $\mathcal{N} : \mathsf{A} \to \mathsf{B}$ to be decodable. Recall the definition of a Stinespring dilation of a channel: this is an isometry $V : \mathsf{A} \to \mathsf{BC}$ such that $\mathcal{N}(X) = \mathrm{Tr}_{\mathsf{C}}(VXV^\dagger)$. We introduce a condition about the *complementary channel* $\mathcal{N}^c(X) := \mathrm{Tr}_{\mathsf{B}}(VXV^\dagger)$, which maps register A to register C, defined relative to a Stinespring dilation V:

Definition 9.3 (Decoupling condition for channels)**.** We say a channel $\mathcal{N}_{\mathsf{A}\to\mathsf{B}}$ satisfies the *decoupling condition with error* ϵ if

$$\mathrm{F}\Big(\mathcal{N}^c_{\mathsf{A}\to\mathsf{C}}(|\Phi\rangle\langle\Phi|_{\mathsf{AR}}),\, \mathcal{N}^c_{\mathsf{A}\to\mathsf{C}}\Big(\frac{\mathrm{id}_{\mathsf{A}}}{\dim \mathsf{A}}\Big) \otimes \frac{\mathrm{id}_{\mathsf{R}}}{\dim \mathsf{R}}\Big) \geq 1-\epsilon\,,$$

where $\mathcal{N}^c$ is a complementary channel to $\mathcal{N}$ relative to any Stinespring dilation.

Proposition 9.4 (Necessary and sufficient conditions for decodability)**.** If a channel $\mathcal{N}$ satisfies the decoupling condition with error ϵ then it is ϵ-decodable. If it is ϵ-decodable, then it satisfies the decoupling condition with error $2\sqrt{\epsilon}$.

In other words, a channel is decodable if and only if the output of the complementary channel is close to unentangled with the reference register R of the maximally entangled state that was input to channel.

Proof. The first direction we prove is the following: if a channel $\mathcal{N}$ satisfies the decoupling condition, then it is decodable. Let V denote the Stinespring dilation of $\mathcal{N}$ which defines the complementary channel $\mathcal{N}^c$ satisfying the decoupling condition.

Let registers A', R' be isomorphic to A, R respectively. Consider the following pure states:

$$\begin{aligned}|E\rangle_{\mathsf{RBCA'R'}} &:= V_{\mathsf{A}\to\mathsf{BC}}\,|\Phi\rangle_{\mathsf{RA}} \otimes |0\rangle_{\mathsf{A'R'}}\\ |F\rangle_{\mathsf{RA'BCR'}} &:= |\Phi\rangle_{\mathsf{RA'}} \otimes V_{\mathsf{A}\to\mathsf{BC}}\,|\Phi\rangle_{\mathsf{AR'}}\ .\end{aligned}$$

Note that the reduced density matrices of $|E\rangle$ and $|F\rangle$ on registers C and R are, respectively, $\mathcal{N}^c_{\mathsf{A}\to\mathsf{C}}(|\Phi\rangle\langle\Phi|_{\mathsf{AR}})$ and $\mathcal{N}^c_{\mathsf{A}\to\mathsf{C}}\Big(\frac{\mathrm{id}_{\mathsf{A}}}{\dim \mathsf{A}}\Big) \otimes \frac{\mathrm{id}_{\mathsf{R}}}{\dim \mathsf{R}}$. Therefore by the decoupling condition and Uhlmann's theorem there exists a unitary U mapping registers $\mathsf{BA'R'}$ to registers $\mathsf{A'BR'}$ such that

$$\mathrm{F}\Big((\mathrm{id}\otimes U)\,|E\rangle\langle E|\,(\mathrm{id}\otimes U^\dagger), |F\rangle\langle F|\Big) \geq 1-\epsilon\,. \tag{9.1}$$

Define the decoding procedure D that maps register B to register A' and behaves as follows: it appends registers $\mathsf{A'R'}$ in the $|0\rangle$ state, applies the isometry U to registers $\mathsf{BA'R'}$, and then traces out registers $\mathsf{BR'}$

to obtain register A'. Since $|E\rangle$ is the result of applying the Stinespring dilation of $\mathcal{N}$ to $|\Phi\rangle$ and appending $|0\rangle_{\mathsf{A}'\mathsf{R}'}$, and using the fact that tracing out registers $\mathsf{B}\mathsf{R}'$ does not reduce the fidelity, Equation (9.1) implies that

$$\mathrm{F}\Big((D_{\mathsf{B}\to\mathsf{A}'}\circ\mathcal{N}_{\mathsf{A}\to\mathsf{B}})(|\Phi\rangle\langle\Phi|_{\mathsf{A}\mathsf{R}}),|\Phi\rangle\langle\Phi|_{\mathsf{A}'\mathsf{R}}\Big)\geq 1-\epsilon\,,$$

showing that $\mathcal{N}$ is ϵ-decodable, as desired.

Now we argue the other direction (if $\mathcal{N}$ is decodable, then the decoupling condition holds). The fact that it is decodable is equivalent to

$$\mathrm{Tr}\Big(\ |\Phi\rangle\langle\Phi|\ (D_{\mathsf{B}\to\mathsf{A}'}\circ\mathcal{N}_{\mathsf{A}\to\mathsf{B}})(|\Phi\rangle\langle\Phi|_{\mathsf{A}\mathsf{R}})\Big)\geq 1-\epsilon\ .$$

Considering the Stinespring dilation $V:\mathsf{A}\to\mathsf{B}\mathsf{C}$ of $\mathcal{N}$ this is equivalent to

$$\mathrm{Tr}\Big((|\Phi\rangle\langle\Phi|_{\mathsf{A}'\mathsf{R}}\otimes\mathrm{id}_{\mathsf{C}})\,D_{\mathsf{B}\to\mathsf{A}'}(V\ |\Phi\rangle\langle\Phi|_{\mathsf{A}\mathsf{R}}\,V^{\dagger})\Big)\geq 1-\epsilon\ . \tag{9.2}$$

Suppose we measure $D_{\mathsf{B}\to\mathsf{A}'}(V\ |\Phi\rangle\langle\Phi|_{\mathsf{A}\mathsf{R}}\,V^{\dagger})$ with the projector $|\Phi\rangle\langle\Phi|$ and succeed. The post-measurement state is thus $|\Phi\rangle\langle\Phi|\otimes\rho_{\mathsf{C}}$ for some density matrix ρ. Since the measurement succeeds with probability at least $1-\epsilon$, by the Gentle Measurement Lemma we get

$$\mathrm{F}\Big(D_{\mathsf{B}\to\mathsf{A}'}(V\ |\Phi\rangle\langle\Phi|_{\mathsf{A}\mathsf{R}}\,V^{\dagger}),|\Phi\rangle\langle\Phi|_{\mathsf{A}'\mathsf{R}}\otimes\rho_{\mathsf{C}}\Big)\geq 1-\epsilon\ . \tag{9.3}$$

Tracing out register A' from both sides, which does not reduce the fidelity, yields

$$\mathrm{F}\Big(\mathcal{N}^{c}_{\mathsf{A}\to\mathsf{C}}(|\Phi\rangle\langle\Phi|_{\mathsf{A}\mathsf{R}}),\ \rho_{\mathsf{C}}\otimes\frac{\mathrm{id}_{\mathsf{R}}}{\dim\mathsf{R}}\Big)\geq 1-\epsilon \tag{9.4}$$

as desired.

On the other hand, tracing out registers $\mathsf{A}'\mathsf{R}$ in Equation (9.3) also yields

$$\mathrm{F}\Big(\mathcal{N}^{c}_{\mathsf{A}\to\mathsf{C}}\Big(\frac{\mathrm{id}_{\mathsf{A}}}{\dim\mathsf{A}}\Big)\ ,\ \rho_{\mathsf{C}}\Big)\geq 1-\epsilon\ . \tag{9.5}$$

Combining Equations (9.4) and (9.5), tracing out register A', and using Fuchs-van de Graaf twice, and we get

$$\mathrm{F}\Big(\mathcal{N}^{c}_{\mathsf{A}\to\mathsf{C}}(|\Phi\rangle\langle\Phi|_{\mathsf{A}\mathsf{R}})\ ,\ \mathcal{N}^{c}_{\mathsf{A}\to\mathsf{C}}\Big(\frac{\mathrm{id}_{\mathsf{A}}}{\dim\mathsf{A}}\Big)\otimes\frac{\mathrm{id}_{\mathsf{R}}}{\dim\mathsf{R}}\Big)\geq 1-2\sqrt{\epsilon}\,,$$

which is the desired decoupling condition. □

9.1.1 Complexity of decoding quantum channels

Previously we identified necessary and sufficient conditions for when a channel is *information-theoretically* decodable. Now we investigate when a decodable channel can be *efficiently* decoded. First we define a computational problem corresponding to decoding a given channel.

Definition 9.5 (ϵ-Decodable Channel Problem)**.** Let $\epsilon,\delta:\mathbb{N}\to[0,1]$ be functions such that $\delta(n)\geq\epsilon(n)$. We say that D *solves the ϵ-Decodable Channel Problem with error δ* if for all $x=(1^m,1^n,C)$ where C is an explicit description of a quantum circuit that maps m qubits to n qubits and is a ϵ-decodable channel, the circuit D takes as input n qubits and satisfies

$$\mathrm{F}\Big((D_x\circ C)(|\Phi\rangle\langle\Phi|),|\Phi\rangle\langle\Phi|\Big)\geq 1-\delta(|x|)\,,$$

where $|\Phi\rangle$ is the maximally entangled state on m qubits.

Even though a channel $\mathcal{N}$ may be ϵ-decodable, it may be computationally intractable to decode it to ϵ error. The δ parameter quantifies the gap between the error achieved by the decoding algorithm and the information-theoretic limit.

The main result of this section is to show that the complexity of the Decodable Channel Problem is equivalent to the complexity of the (distributional) Uhlmann Transformation Problem.

Theorem 9.6. Let $\epsilon : \mathbb{N} \to [0, 1]$ be a negligible function. If $\textsc{DistUhlmann}_{1-2\sqrt{\epsilon}}$ can be solved in polynomial time with inverse polynomial error, then the ϵ-Decodable Channel Problem is solvable with inverse polynomial error. Conversely, if the $O(\sqrt{\epsilon})$-Decodable Channel Problem is solvable in polynomial time with inverse polynomial error then $\textsc{DistUhlmann}_{1-\epsilon}$ can be solved in polynomial time with inverse polynomial error.

Proof. **Upper bound.** We start by proving the the "only if" direction (if $\textsc{DistUhlmann}_{1-\epsilon}$ is easy, then the Decodable Channel Problem is easy). We present an algorithm D that solves the ϵ-Decodable Channel Problem, and is efficient under the assumption about $\textsc{DistUhlmann}$.

Let $x = (1^m, 1^n, C)$ be an instance of the ϵ-Decodable Channel Problem be such that C is a quantum circuit computing an ϵ-decodable channel mapping m qubits (which we label as register A) to n qubits (which we label as register B). Let V denote the unitary purification of C (see Definition 2.8) of C, which we view also as a Stinespring dilation of C that maps register A to registers BC. Let A', R' denote registers isomorphic to A, R, respectively. Consider the pure states $|E\rangle_{\mathsf{RBCA'R'}}$ and $|F\rangle_{\mathsf{RA'BCR'}}$ defined in the proof of Proposition 9.4 with respect to the dilation V. Note that these states can be computed by circuits E, F with size $\mathrm{poly}(|C|)$. By padding we can assume without loss of generality that E, F act on $2k$ qubits where $k \geq |x|$.

Since the channel C is ϵ-decodable, then by Proposition 9.4 it satisfies the decoupling condition with error $2\sqrt{\epsilon}$. Therefore it follows that $y = (1^k, E, F)$ is a valid $\textsc{Uhlmann}_{1-2\sqrt{\epsilon}}$ instance (where the registers are divided into two groups CR and $\mathsf{BA'R'}$). Thus by assumption there is a polynomial-time algorithm $M = (M_{y,r})_{y,r}$ that implements $\textsc{DistUhlmann}_{1-2\sqrt{\epsilon}} \in \mathsf{avgUnitaryBQP}$. By Proposition 5.8, it follows that for $y = (1^k, E, F)$ with $k = \mathrm{poly}(|x|)$, the algorithm M satisfies, for all precision r,

$$\mathrm{td}\Big((\mathrm{id} \otimes M_{y,r})(|E\rangle\langle E|), |F\rangle\langle F|\Big) \leq \frac{1}{r} + (4\epsilon(k))^{1/4} .$$

By Fuchs-van de Graaf this implies

$$\mathrm{F}\Big((\mathrm{id} \otimes M_{y,r})(|E\rangle\langle E|), |F\rangle\langle F|\Big) \geq \Big(1 - \frac{1}{r} - (4\epsilon(k))^{1/4}\Big)^2 . \tag{9.6}$$

Fix a polynomial q. The algorithm D behaves as follows on instance $x = (1^m, 1^n, C)$ of the ϵ-Decodable Channel Problem. It receives as input a register B. It first computes the description of the $\textsc{Uhlmann}_{1-2\sqrt{\epsilon}}$ instance $y = (1^k, E, F)$ described above. It initializes ancilla registers $\mathsf{A'R'}$ in the zero state, and then applies the algorithm $(M_{y,r})_{y,r}$ that solves the $\textsc{DistUhlmann}_{1-2\sqrt{\epsilon}}$-problem to registers $\mathsf{BA'R'}$ with the precision parameter $r = 1/4q(|x|)$. Finally, the algorithm D then traces out registers $\mathsf{BR'}$ and outputs the remaining register $\mathsf{A'}$.

Now we analyze the behavior of the algorithm D when it receives the B register of the state $C_{\mathsf{A}\to\mathsf{B}}(|\Phi\rangle\langle\Phi|_{\mathsf{AR}})$. Note that

$$\Big((D_x)_{\mathsf{B}\to\mathsf{A'}} \circ C_{\mathsf{A}\to\mathsf{B}}\Big)(|\Phi\rangle\langle\Phi|_{\mathsf{RA}}) = \mathrm{Tr}_{\mathsf{CBR'}}\Big((\mathrm{id} \otimes M_{y,r})(|E\rangle\langle E|)\Big)$$

$$|\Phi\rangle\langle\Phi|_{\mathsf{RA'}} = \mathrm{Tr}_{\mathsf{ABCR'}}\Big(\,|F\rangle\langle F|\,\Big) .$$

By Equation (9.6) and the fact that the fidelity does not decrease under partial trace we have

$$\begin{aligned}\mathrm{F}\Big(\big((D_x)_{\mathsf{B}\to\mathsf{A}'}\circ C_{\mathsf{A}\to\mathsf{B}}\big)(|\Phi\rangle\!\langle\Phi|_{\mathsf{RA}})\,,\,|\Phi\rangle\!\langle\Phi|_{\mathsf{RA}'}\Big) &\geq \mathrm{F}\Big((\mathrm{id}\otimes M_{y,r})(|E\rangle\!\langle E|),|F\rangle\!\langle F|\Big)\\ &\geq 1-\frac{2}{r}-2(4\epsilon(k))^{1/4}\geq 1-O(\frac{1}{q(|x|)})\,.\end{aligned}$$

In the last inequality we used that $O(\epsilon(k)^{1/4})$ is a negligible function of k and thus of $|x|$ (because $k=\mathrm{poly}(|x|)$). Thus we have shown that D solves the ϵ-Decodable Channel Problem up to error $1/q$ in time $\mathrm{poly}(|x|,r)=\mathrm{poly}(|x|)$ as desired. This concludes the "only if" direction.

Lower bound. We now prove the "if" part of the theorem (if the Decodable Channel Problem is easy, then DISTUHLMANN is easy). The intuition behind the proof is as follows: if DISTUHLMANN were hard, then we can construct a family of hard instances of the Decodable Channel Problem. These hard instances, intuitively, will be decodable channels $\mathcal{N}$ that take as input $b\in\{0,1\}$ and output an *encryption* ρ_b. The states ρ_0 and ρ_1 are far from each other, but are computationally indistinguishable (this is also known as an *EFI pair* [BCQ23]). Thus no efficient decoder can correctly recover the bit b, even though the channel $\mathcal{N}$ is information-theoretically decodable by construction.

We describe an efficient reduction from instances of the Uhlmann Transformation Problem to instances of the Decodable Channel Problem. Let $x=(1^n,C_0,C_1)$ be an instance of $\text{UHLMANN}_{1-\epsilon}$ for some negligible ϵ, where the circuits C_0,C_1 output a state on registers XY and the reduced density matrices of $|C_0\rangle\,,|C_1\rangle$ on register X have fidelity at least $1-\epsilon$. For $b\in\{0,1\}$ define the circuit E_b that prepares the state

$$|E_b\rangle:=\frac{1}{\sqrt{2}}\,|C_0\rangle_{\mathsf{XY}}\,|0\rangle_{\mathsf{E}}+(-1)^b\frac{1}{\sqrt{2}}\,|C_1\rangle_{\mathsf{XY}}\,|1\rangle_{\mathsf{E}}\ .$$

Define the channel $\mathcal{N}$ that takes as input a qubit $|b\rangle_{\mathsf{A}}$, maps it to $|E_b\rangle_{\mathsf{XYE}}$, and outputs the register YE. Let F denote the circuit that computes this channel. Note that F is a polynomial-sized circuit in the length of the Uhlmann instance x.

We first argue that the channel $\mathcal{N}$ is $O(\sqrt{\epsilon})$-decodable. By Uhlmann's theorem there exists a unitary V acting on register YE such that

$$\frac{1}{2}\Big(\langle C_1|\,\langle 1|\,(\mathrm{id}_{\mathsf{X}}\otimes V_{\mathsf{YE}})\,|C_0\rangle\,|0\rangle+\langle C_0|\,\langle 0|\,(\mathrm{id}_{\mathsf{X}}\otimes V_{\mathsf{YE}})\,|C_1\rangle\,|1\rangle\Big)\geq 1-\epsilon\,.$$

By the swapping-distinguishing equivalence of [AAS20, Theorem 2], this implies a (not necessarily efficient) measurement M on registers YE that distinguishes between $|E_0\rangle$ and $|E_1\rangle$ with bias $1-\epsilon$. Consider the following thought experiment: apply the channel $\mathcal{N}$ to register A of $|\Phi\rangle_{\mathsf{RA}}$ to obtain $\frac{1}{\sqrt{2}}\sum_b|b\rangle_{\mathsf{R}}\,|E_b\rangle_{\mathsf{XYE}}$. Trace out the registers YE; because we can imagine that the measurement M was performed on registers YE, the resulting density matrix must be $O(\epsilon)$-close in trace distance to

$$\frac{1}{2}\,|0\rangle\!\langle 0|\otimes\rho+\frac{1}{2}\,|1\rangle\!\langle 1|\otimes\sigma\ .$$

Since ρ,σ are $\sqrt{\epsilon}$-close in trace distance, this implies that the density matrix must be $O(\sqrt{\epsilon})$-close to $\frac{\mathrm{id}_{\mathsf{R}}}{2}\otimes\rho_{\mathsf{X}}$, which means that the channel $\mathcal{N}$ satisfies the decoupling condition with error $O(\sqrt{\epsilon})$. Proposition 9.4 implies that $\mathcal{N}$ is $O(\sqrt{\epsilon})$-decodable.

Let q be a polynomial and let $p(|x|) = O(1/q(|x|)^2)$. By assumption there exists a polynomial-time algorithm D that solves the $O(\sqrt{\epsilon})$-Decodable Channel Problem with error $1/p$. In particular, letting $y = (1^k, F)$ for the circuit F computing channel $\mathcal{N}$ described above, we have

$$\mathrm{F}\Big((D_y \circ F)(|\Phi\rangle\langle\Phi|), |\Phi\rangle\langle\Phi|\Big) \geq 1 - 1/p(|y|) \ .$$

By measuring the register R in the standard basis and using the monotonicity of the fidelity function under quantum operations, we get that

$$\frac{1}{2}\sum_b \mathrm{F}\Big((\mathrm{id}_{\mathsf{X}} \otimes D_y)(|E_b\rangle\langle E_b|)\, , \, |b\rangle\langle b|\Big) \geq 1 - 1/p(|y|) \ .$$

In other words, there is an efficient measurement on registers YE that distinguishes $|E_0\rangle, |E_1\rangle$ with bias at least $1 - O(1/p(|y|))$. Again by the swapping-distinguishing equivalence [AAS20, Theorem 2] we get that there is an efficient algorithm A acting on YE, plus some ancilla registers, that maps $|C_0\rangle$ to have overlap at least $1 - O(1/p(|y|))$ with $|C_1\rangle$.

By Proposition 5.8, this means that the algorithm A implements the canonical Uhlmann transformation corresponding to $(|C_0\rangle, |C_1\rangle)$ with error at most $O(\sqrt{1/p(|y|)} + \epsilon(|x|)^{1/4})$. Since $|y| \geq |x|$, the error function ϵ is negligible and we assume that all polynomials and error functions are monotonic, this is error bound asymptotically at most $O(\sqrt{1/p(|x|)}) \leq O(1/q(|x|))$. The running time of A is polynomial in $|x|$ as it runs the decoder D on input y, which has polynomial size in $|x|$. This concludes the "if" direction. □

9.2 Compressing quantum information

In this section we show that the computational complexity of performing optimal compression of a quantum state (that can be efficiently prepared) is related to the complexity of the Uhlmann Transformation Problem.

We consider the *one-shot* version of the information compression task, where one is given just one copy of a density matrix ρ (rather than many copies) and the goal is to compress it to as few qubits as possible while being able to recover the original state within some error. The task is defined formally as follows:

Definition 9.7 (Information compression task)**.** Let $\delta \geq 0$ and let ρ be an n-qubit density matrix. We say that a pair of (not necessarily efficient) quantum circuits (E, D) *compresses ρ to s qubits with error δ* if

1. E is a quantum circuit that takes as input n qubits and outputs s qubits,
2. D is a quantum circuit that takes as input s qubits and outputs n qubits,
3. For all purifications $|\psi\rangle_{\mathsf{AR}}$ of ρ (where R is the purifying register), we have

$$\mathrm{td}\Big((D \circ E)(\psi), \psi\Big) \leq \delta$$

where the composite channel $D \circ E$ acts on register A of $|\psi\rangle$.

Define the *δ-error communication cost of ρ*, denoted by $K^\delta(\rho)$, as the minimum integer s such that there exists a pair of quantum circuits (E, D) that compresses ρ to s qubits with error δ.

In this section, we first analyze what is information-theoretically achievable for one-shot compression. Then, we study the complexity of compressing quantum information to the information-theoretic limit; we will show that it is closely related to the complexity of the Uhlmann Transformation Problem.

9.2.1 Information-theoretic compression

It is well-known that n copies of a quantum state ρ can be compressed to n times the von Neumann entropy of ρ, in the limit of large n [Sch95]. In the one-shot setting the state ρ can be (information-theoretically) compressed to its *smoothed max entropy* and no further. The smoothed max entropy is defined as follows:

Definition 9.8 (Smoothed max-entropy)**.** Let $\epsilon \geq 0$ and let ψ_{AB} be a density matrix on registers AB. The *max-entropy of register* A *conditioned on register* B *of the state* ψ is

$$H_{\max}(\mathsf{A}|\mathsf{B})_\psi := \sup_{\sigma \in \mathrm{Pos}(\mathsf{B}) : \mathrm{Tr}(\sigma) \leq 1} \log \| \sqrt{\psi_{\mathsf{AB}}} \sqrt{\mathrm{id}_{\mathsf{A}} \otimes \sigma_{\mathsf{B}}} \|_1^2 \,.$$

The ϵ*-smoothed conditional max-entropy* is

$$H^\epsilon_{\max}(\mathsf{A}|\mathsf{B})_\psi := \inf_{\sigma : \mathrm{td}(\sigma,\psi) \leq \epsilon} H_{\max}(\mathsf{A}|\mathsf{B})_\sigma \,.$$

The following theorem shows that the smoothed max-entropy characterizes, up to additive constants and different smoothing parameters, the limits of one-shot compression.

Theorem 9.9 (Information-theoretic one-shot compression)**.** For all $\delta > 0$ and all density matrices ρ,

$$H^{\epsilon_1}_{\max}(\rho) \leq K^\delta(\rho) \leq H^{\epsilon_2}_{\max}(\rho) + 8 \log \frac{4}{\delta}$$

where $\epsilon_1 := 2\delta^{1/4}$ and $\epsilon_2 := (\delta/40)^4$.

We prove Theorem 9.9 in Appendix B. We note that for tensor product states $\rho^{\otimes k}$, the smoothed max-entropy converges to the well-known von Neumann entropy:

$$\lim_{\epsilon \to 0} \lim_{k \to \infty} \frac{1}{k} H^\epsilon_{\max}(\rho^{\otimes k}) = H(\rho) \,.$$

This is an instance of the *quantum asymptotic equipartition property*, which roughly states that the min, max, and Rényi entropies approach the von Neumann entropy in the limit of many copies of a state [TCR09].[22] Thus Theorem 9.9 applied to tensor product states $\rho^{\otimes k}$ recovers Schumacher compression [Sch95].

9.2.2 Complexity of near-optimal compression

We now study the computational complexity of compressing quantum information to the information-theoretic limit, i.e., to the smoothed max-entropy of a state. We begin by defining compression as a computational task.

Definition 9.10 (Compression as a computational task)**.** Let $\epsilon, \eta : \mathbb{N} \to [0,1]$ be functions. Let $E = (E_x)_x$ and $D = (D_x)_x$ be quantum algorithms. We say that (E, D) *compresses to the* ϵ*-smoothed max-entropy with error* η if for all $x = (1^n, C)$ where C is a quantum circuit that outputs n qubits, we have that (E_x, D_x) compresses $\rho_x := C(|0\rangle\langle 0|)$ to at most $H^{\epsilon(n)}_{\max}(\rho_x) + O(\log \frac{1}{\epsilon(n)})$ qubits with error at most $\eta(n)$. **Tony: Can we say why the additional $+O(\log \frac{1}{\epsilon(n)})$ is natural, e.g. by referring to the analogous term in Theorem 9.9?**

[22] In fact, one can give stronger quantitative bounds on the convergence to the von Neumann entropy as a function of the number of copies k and the error ϵ.

This brings us to the main result of the section, which are upper and lower bounds on the complexity of the compression task.

Theorem 9.11 (Near-optimal compression via Uhlmann transformations)**.** Let $\epsilon(n)$ be a negligible function. If $\textsc{DistUhlmann}_{1-\epsilon} \in \mathsf{avgUnitaryBQP}$, then for all polynomials $q(n)$ there exists a pair of polynomial-time algorithms (E, D) that compresses to the ϵ-smoothed max-entropy with error $\eta(n) = 1/q(n)$.

Proof. Let $x = (1^n, C)$ where C is a quantum circuit that outputs n qubits, and let $\rho_x = C(|0\rangle\langle 0|)$. Let $\epsilon = \epsilon(n)$. The proof of the upper bound of Theorem 9.9 involves the following two states:

$$|F\rangle := |\Phi\rangle_{\mathsf{EE}'} \otimes |\rho\rangle_{\mathsf{AR}} \;,$$
$$|G\rangle := \sum_y |y\rangle_{\mathsf{E}} \otimes (\Pi_y U \otimes \mathrm{id}_{\mathsf{R}}) \, |\rho\rangle_{\mathsf{AR}} \otimes |0\rangle_{\mathsf{F}} \;.$$

(The state $|G\rangle$ was called $|\theta\rangle$ in Theorem 9.9). Here, $|\Phi\rangle_{\mathsf{EE}'}$ denotes the maximally entangled state on EE', $|\rho\rangle_{\mathsf{AR}}$ is the pure state resulting from evaluating a purification of the circuit C on the all zeroes input, the projector Π_y denotes projecting the first $n-s$ qubits of register A onto $|y\rangle$, and U is a Clifford unitary. Note that $|F\rangle, |G\rangle$ can be prepared by circuits F, G whose sizes are polynomial in n and in the size of C; this uses the fact that Clifford unitaries can be computed by a circuit of size $O(n^2)$ [AG04].

The proof of Theorem 9.9 shows that the reduced density matrices of $|F\rangle, |G\rangle$ on registers EA have fidelity at least $1 - 2\nu = 1 - \epsilon^2/16 \geq 1 - \epsilon$. Thus $(1^m, F, G)$ is a valid $\textsc{Uhlmann}_{1-\epsilon}$ instance. Since $\textsc{DistUhlmann}_{1-\epsilon} \in \mathsf{avgUnitaryBQP}$ by assumption there exists $\mathrm{poly}(n, |C|)$-size circuit L mapping registers $\mathsf{E}'\mathsf{A}$ to $\mathsf{E}'\mathsf{CF}$ and a channel completion Ξ of the canonical Uhlmann transformation V corresponding to $(|F\rangle, |G\rangle)$ such that

$$\mathrm{td}\Big((\mathrm{id} \otimes L)(|F\rangle\langle F|),\; (\mathrm{id} \otimes \Xi)(|F\rangle\langle F|)\Big) \leq \frac{1}{r(n)}$$

where $r(n)$ is a polynomial such that $2/r(n) + \epsilon(n) \leq 1/q(n)$, which is possible because $\epsilon(n)$ is a negligible function. Similarly there exists a $\mathrm{poly}(n, |C|)$-size circuit M and a channel completion Λ of the Uhlmann transformation $V^\dagger$ corresponding to $(|G\rangle, |F\rangle)$ such that

$$\mathrm{td}\Big((\mathrm{id} \otimes M)(|G\rangle\langle G|),\; (\mathrm{id} \otimes \Lambda)(|G\rangle\langle G|)\Big) \leq \frac{1}{r(n)} \;.$$

The proof of Theorem 9.9 shows shows that there exists a pair of uniformly-computable circuits (E^*_x, D^*_x) that compresses ρ_x to $s = H^\epsilon_{\max}(\rho_x) + O(\log \frac{1}{\epsilon})$ qubits with error ϵ. Notice that the circuits E^*_x, D^*_x are $\mathrm{poly}(n)$-size circuits that make one call to channels Ξ, Λ, respectively. Now the idea is to "plug in" the circuits L, M to implement the call to the channel Ξ, Λ, respectively. Let E_x, D_x denote the resulting $\mathrm{poly}(n, |C|)$-sized circuits. Using L, M instead of the channels Ξ, Λ incurs at most $O(1/r(n))$ error, i.e., $\mathrm{td}\Big((D_x \circ E_x)(|\rho\rangle\langle\rho|_{\mathsf{AR}}), (D^*_x \circ E^*_x)(|\rho\rangle\langle\rho|_{\mathsf{AR}})\Big) \leq 2/r(n)$. Therefore

$$\mathrm{td}\Big((D_x \circ E_x)(|\rho\rangle\langle\rho|_{\mathsf{AR}}), |\rho\rangle\langle\rho|_{\mathsf{AR}}\Big) \leq 2/r(n) + \epsilon(n) \leq 1/q(n) \,.$$

Letting $E = (E_x)_x$ and $D = (D_x)_x$ we get the desired pair of uniform polynomial-time algorithms that compresses to the ϵ-smoothed max entropy with inverse polynomial error. □

We now turn to proving a hardness result for near-optimal compression; it cannot be performed in polynomial-time if *stretch pseudorandom state (PRS) generators* exist. Pseudorandom state generators are a quantum analogue of classical pseudorandom generators (PRGs) and in fact can be constructed from post-quantum pseudorandom generators [JLS18], but there is evidence that the assumption of PRS is less stringent than the assumption of post-quantum PRGs [Kre21, KQST23]. We first recall the definition of a PRS generator:

Definition 9.12 (Pseudorandom state generator [JLS18, Definition 3])**.** We say that a (uniform) polynomial-time algorithm $G = (G_\lambda)_\lambda$ is a *pseudorandom state (PRS) generator* if the following holds.

1. (*State generation*). For all λ, on input $k \in \{0,1\}^k$ the algorithm G outputs
$$G_\lambda(k) = |\psi_k\rangle\!\langle\psi_k|$$
for some $m(\lambda)$-qubit pure state $|\psi_k\rangle$.

2. (*Strong pseudorandomness*). For all polynomials $t(\lambda)$ and non-uniform polynomial-time distinguishers $A = (A_\lambda)_\lambda$ there exists a negligible function $\epsilon(\lambda)$ such that for all λ, we have
$$\left| \Pr_{k \leftarrow \{0,1\}^\lambda} \left[A_\lambda^{O_{\psi_k}}(G_\lambda(k)^{\otimes t(\lambda)}) = 1 \right] - \Pr_{|\vartheta\rangle \leftarrow \mathrm{Haar}_{m(\lambda)}} \left[A_\lambda^{O_\vartheta}(|\vartheta\rangle\!\langle\vartheta|^{\otimes t(\lambda)}) = 1 \right] \right| \le \epsilon(\lambda),$$
where $O_\psi := \mathrm{id} - 2\,|\psi\rangle\!\langle\psi|$ is the reflection oracle for $|\psi\rangle$.

We say that G is a *stretch* PRS generator if $m(\lambda) > \lambda$.

Here we use the strong pseudorandomness guarantee, which is known to be equivalent to the weaker (standard) pseudorandomness guarantee where the adversary does not get access to the reflection oracle [JLS18, Theorem 4]. We also note that PRS generators do not necessarily provide any *stretch*; there are nontrivial PRS generators where the output length $m(\lambda)$ can be smaller than the λ. Furthermore, unlike classical PRGs, it is not known whether PRS can be generically stretched (or shrunk); see [AQY22] for a longer discussion of this.

We now state our hardness result.

Theorem 9.13 (Hardness of near-optimal compression)**.** Let $\epsilon(n)$ be a function. Let $m(\lambda)$ be a function satisfying
$$m(\lambda) > \lambda + O\Big(\log \frac{1}{\epsilon(m(\lambda))}\Big) + 2$$
for all sufficiently large λ. If stretch pseudorandom state generators that output $m(\lambda)$ qubits exist, then there is no non-uniform polynomial-time algorithm (E, D) that compresses to the ϵ-smoothed max-entropy with error $\frac{1}{2}$.

Proof. Let G be a PRS generator that outputs $m(\lambda)$-qubit states for $m(\lambda)$ satisfying the conditions stated in Theorem 9.13, and fix a sufficiently large $\lambda \in \mathbb{N}$ for which the condition is satisfied. Define the pure state $|\varphi_\lambda\rangle$ that represents running a unitary purification of the generator G coherently with the keys k in superposition:
$$|\varphi_\lambda\rangle_{\mathsf{KQA}} := 2^{-\lambda/2} \sum_{k \in \{0,1\}^\lambda} |k\rangle_{\mathsf{K}} \otimes |\tau_k\rangle_{\mathsf{Q}} \otimes |\psi_k\rangle_{\mathsf{A}}$$
where $|\psi_k\rangle$ denotes the pseudorandom state output by G on key k, and $|\tau_k\rangle$ denotes the state of the ancilla qubits of G. Let $\mathsf{R} := \mathsf{KQ}$. The reduced density matrix of $|\varphi_\lambda\rangle$ on register A is the following mixed state:
$$\rho_\lambda := 2^{-\lambda} \sum_{k \in \{0,1\}^\lambda} |\psi_k\rangle\!\langle\psi_k| \ .$$

By the second item of Proposition B.2 we have $H^\epsilon_{\max}(\rho_\lambda) \leq \lambda$.

Assume for contradiction that there exists a polynomial-time pair of quantum algorithms (E, D) that compresses to the ϵ-smoothed max-entropy with error $\frac{1}{2}$. Let $x = (1^n, C)$ where C outputs the state ρ_λ by first synthesizing the state $|\varphi_\lambda\rangle$ and then tracing out register R. Clearly C is a $\mathrm{poly}(\lambda)$-sized circuit. Therefore (E_x, D_x) runs in $\mathrm{poly}(\lambda)$ time and compresses ρ_λ to $r_\lambda \coloneqq H^\epsilon_{\max}(\rho_\lambda) + O\Big(\log \frac{1}{\epsilon(m(\lambda))}\Big) \leq \lambda + O\Big(\log \frac{1}{\epsilon(m(\lambda))}\Big)$ qubits. By assumption we have

$$\mathrm{td}\Big((D_x \circ E_x)(|\varphi_\lambda\rangle\!\langle\varphi_\lambda|),\, |\varphi_\lambda\rangle\!\langle\varphi_\lambda|\Big) \leq \frac{1}{2}\,.$$

By measuring register K and tracing out register Q on both arguments (which does not increase the trace distance), we have that

$$\mathop{\mathbb{E}}_{k} \mathrm{td}\Big((D_x \circ E_x)(|\psi_k\rangle\!\langle\psi_k|)\,,\, |\psi_k\rangle\!\langle\psi_k|\Big) \leq \frac{1}{2}\,. \tag{9.7}$$

Now consider the following distinguisher $A = (A_\lambda)_\lambda$: it gets as input $|\theta\rangle$ where $|\theta\rangle$ is either $|\psi_k\rangle$ for a randomly sampled k or $|\vartheta\rangle$ sampled from the Haar measure; it also gets access to a (controlled) reflection oracle $O_\theta = \mathrm{id} - 2\,|\theta\rangle\!\langle\theta|$. It then

1. applies the channel $D_x \circ E_x$ to input $|\theta\rangle$;
2. measures $\{|\theta\rangle\!\langle\theta|\,, \mathrm{id} - |\theta\rangle\!\langle\theta|\}$ using the reflection oracle, and accept if measurement accepts.

From Equation (9.7) we have that, since the measurement step with respect to O_{ψ_k} accepts on $|\psi_k\rangle$ with probability 1, then A_λ with oracle access to O_{ψ_k} accepts $|\psi_k\rangle$ with probability at least $1 - \eta$ over the choice of key k and the randomness of A_λ.

Now consider what happens when we run A_λ with $|\vartheta\rangle$ as input where $|\vartheta\rangle$ is sampled from the Haar measure, as well as with the reflection oracle O_ϑ. Since A runs in $\mathrm{poly}(\lambda)$ time, by the pseudorandomness property of G the probability that A_λ accepts $|\vartheta\rangle$ is at least $\frac{1}{2} - \mathrm{negl}(\lambda)$.

On the other hand we show that since a Haar-random state cannot be compressed, A_λ cannot accept with high probability. Let $R \coloneqq 2^{r_\lambda}$ denote the dimensionality of the output of E_λ, and let $M = 2^{m(\lambda)}$ denote the dimensionality of register A. For brevity we abbreviate E_x, D_x as E, D respectively. The success probability of A_λ given a Haar-random state $|\vartheta\rangle$ and the reflection oracle O_ϑ can be calculated as follows. First, observe that

$$\int_\vartheta \mathrm{Tr}\Big((D \circ E)(|\vartheta\rangle\!\langle\vartheta|)\ |\vartheta\rangle\!\langle\vartheta|\Big)\,\mathrm{d}\vartheta = \int_\vartheta \mathrm{Tr}\Big(E(|\vartheta\rangle\!\langle\vartheta|)\, D^*(|\vartheta\rangle\!\langle\vartheta|)\Big)\,\mathrm{d}\vartheta$$

where D^* denotes the *adjoint channel* corresponding to D; it is the unique superoperator mapping register A' to B satisfying $\mathrm{Tr}(XD(Y)) = \mathrm{Tr}(D^*(X)Y)$ for all operators X, Y. Viewing $E \otimes D^*$ as a superoperator mapping registers $\mathsf{A}_1\mathsf{A}_2$ to $\mathsf{B}_1\mathsf{B}_2$ and letting $S_{\mathsf{B}_1\mathsf{B}_2}$ denote the swap operator on registers $\mathsf{B}_1\mathsf{B}_2$ the above is equal to

$$\mathrm{Tr}\Big(S_{\mathsf{B}_1\mathsf{B}_2}(E \otimes D^*)(\int_\vartheta |\vartheta\rangle\!\langle\vartheta|^{\otimes 2}\,\mathrm{d}\vartheta)\Big)\,.$$

Now, it is well-known [Har13] that the integral over two copies of an $m(\lambda)$-qubit Haar-random state is proportional to the projector $\frac{1}{2}(\mathrm{id} + S)$ onto the *symmetric subspace* of $(\mathbb{C}^M)^{\otimes 2}$. The dimension of the projector is $M(M+1)/2$. Thus the above is equal to

$$\begin{aligned}
&\frac{1}{M(M+1)}\mathrm{Tr}\Big(S_{\mathsf{B}_1\mathsf{B}_2}\,(E\otimes D^*)(\mathrm{id}_{\mathsf{A}_1\mathsf{A}_2}+S_{\mathsf{A}_1\mathsf{A}_2})\Big)\\
&\quad\leq \frac{1}{M(M+1)}\mathrm{Tr}\Big((E\otimes D^*)(\mathrm{id}_{\mathsf{A}_1\mathsf{A}_2}+S_{\mathsf{A}_1\mathsf{A}_2})\Big)\\
&\quad= \frac{1}{M(M+1)}\Big[\mathrm{Tr}\Big((E\otimes D^*)(\mathrm{id}_{\mathsf{A}_1\mathsf{A}_2})\Big)+\mathrm{Tr}\Big((E\otimes D^*)(S_{\mathsf{A}_1\mathsf{A}_2})\Big)\Big]\\
&\quad= \frac{1}{M(M+1)}\Big[\mathrm{Tr}\Big(\mathrm{id}_{\mathsf{A}_1}\otimes D^*(\mathrm{id}_{\mathsf{A}_2})\Big)+\mathrm{Tr}\Big((\mathrm{id}_{\mathsf{A}_1}\otimes D^*)(S_{\mathsf{A}_1\mathsf{A}_2})\Big)\Big]\\
&\quad= \frac{1}{M(M+1)}\Big[\mathrm{Tr}\Big(\mathrm{id}_{\mathsf{A}_1}\Big)\,\mathrm{Tr}\Big(D^*(\mathrm{id}_{\mathsf{A}_2})\Big)+\mathrm{Tr}\Big(D^*(\mathrm{id}_{\mathsf{A}_2})\Big)\Big]\\
&\quad= \frac{1}{M(M+1)}\Big[RM+R\Big]\\
&\quad= R/M = 2^{-(m(\lambda)-\lambda-O(\log 1/\epsilon))}\leq\frac{1}{4}\,.
\end{aligned}$$

The second line follows from the fact that $|\mathrm{Tr}(A^\dagger B)|\leq\|A\|_\infty\|B\|_1$ for all operators A,B and $\|S\|_\infty\leq 1$. The fourth line follows from the fact that E is a trace-preserving superoperator. The sixth line follows from the fact that since D is a channel that takes as input B, $\mathrm{Tr}(D^*(\mathrm{id}_{\mathsf{A}_2}))=\mathrm{Tr}(\mathrm{id}_{\mathsf{B}})=R$. The last line follows because our assumption about the stretch of the PRS. This shows that the acceptance probability of A_λ given a Haar random state and access to its reflection oracle is at most $\frac{1}{4}$, which is less than $\frac{1}{2}-\mathrm{negl}(\lambda)$ for sufficiently large λ.

Thus we have arrived at a contradiction. There is no polynomial-time pair of algorithms that compresses to the ϵ-smoothed max entropy. □

We compare our hardness result with the upper bound proved in Theorem 9.11. As an example, let $\epsilon(n)=2^{-\log^2(n)}$, which is a negligible function. Then roughly, if $\textsc{DistUhlmann}_{1-\epsilon}$ is easy, then compressing to $H^\epsilon_{\max}(\rho)+O(\log 1/\epsilon)=H^\epsilon_{\max}(\rho)+O(\log^2(n))$ is easy. On the other hand, the lower bound shows that if PRS generators with output length $m(\lambda)\geq\lambda+\Omega(\log^2(\lambda))$ exist, then compressing to $H^\epsilon_{\max}(\rho)+O(\log^2(n))$ is not easy.

We remark that it should be possible to base the lower bound on seemingly weaker assumptions, such as one-way state generators [MY22]. However, ideally we would be able to base the hardness on an assumption such as the existence of quantum commitments or the hardness of the Uhlmann transformation problem, which would give a true converse to the upper bound of Theorem 9.11. However the main issue is *verifiability*: with pseudorandom states or one-way state generators (with pure-state outputs), one can check whether the state has been compressed and decompressed; it is not clear whether this is possible with quantum commitments. We leave it as an open problem to prove matching upper and lower complexity bounds on compression.

Open Problem 12. Is the complexity of optimal compression equivalent to the complexity of the Uhlmann Transformation Problem?

There are many more that have been studied information-theoretically (including a whole family tree of them [ADHW09]), and one can ask about the complexity of each of these tasks.

Open Problem 13. What is the complexity of other quantum Shannon theory tasks, such as achieving capacity over a noisy channel, entanglement distillation, or quantum state redistribution?

10 Black-Hole Radiation Decoding

In this section, we discuss connections between the Uhlmann Transformation Problem and computational tasks motivated by questions in high-energy physics. We focus on the *black hole radiation decoding task*, which was introduced by Harlow and Hayden [HH13]. We argue that the complexity of this task is characterized by the complexity of the distributional Uhlmann Transformation Problem.

The black hole radiation decoding task is motivated by the following thought experiment of Almheiri, Marolf, Polchinski, Sully [AMPS13]: imagine that Alice creates a maximally entangled pair of qubits $|\mathrm{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and throws one half into a newly-formed black hole. After a long time, Alice could potentially decode the Hawking radiation of the black hole and recover the qubit she threw in. However, Alice could then jump into the black hole and find another qubit that is supposed to be maximally entangled with the qubit that was not thrown in – witnessing a violation of the monogamy of entanglement. These conclusions were derived assuming supposedly uncontroversial principles of quantum field theory and general relativity.

Harlow and Hayden proposed a resolution to this paradox via a computational complexity argument [HH13]: it may not be *feasible* for Alice to decode the black hole's Hawking radiation in any reasonable amount of time — by the time she decodes the qubit that she threw in, the black hole may have evaporated anyways! They argued that, assuming $\mathsf{SZK} \not\subseteq \mathsf{BQP}$ – note that these are classes of *decision* problems — a formulation of the black hole radiation decoding task cannot be done in polynomial time.

What about the converse? That is, does a traditional complexity class statement such as $\mathsf{SZK} \subseteq \mathsf{BQP}$ imply that the black hole radiation decoding task is solvable in polynomial time? As pointed out by Aaronson [Aar16], it is not even clear that the black hole radiation decoding task is easy even if we assume $\mathsf{P} = \mathsf{PSPACE}$. As with all the other "fully quantum" tasks considered in this paper, it appears difficult to characterize the complexity of the black hole decoding problem in terms of traditional notions from complexity theory.

Brakerski recently gave a characterization of the hardness of the black hole radiation task in terms of the existence of a cryptographic primitive known as *quantum EFI pairs* [Bra23], which are in turn equivalent to quantum commitments (as well as many other quantum cryptographic primitives, see [BCQ23] for an in-depth discussion). Given the discussion in Section 8 that connects quantum commitments with the Uhlmann Transformation Problem, one would then expect an equivalence between black hole radiation decoding and the Uhlmann Transformation Problem.

We spell out this equivalence by showing that the complexity of the black hole radiation decoding task is the same as the complexity of the Decodable Channel Problem, which we showed to be equivalent to the (distributional) Uhlmann Transformation Problem in Section 9.1. We believe that the direct reduction to and from the Decodable Channel Problem is natural, and may be useful to those who are more comfortable with quantum Shannon theory.

We first describe a formulation of the black hole radiation decoding task, which is an adaptation of the formulations of [HH13, Bra23].

Definition 10.1 (Decodable black hole states)**.** Let P denote a unitary quantum circuit mapping registers AG to HR where A is a single qubit register. Consider the state

$$|\psi\rangle_{\mathsf{BHR}} \coloneqq (\mathrm{id}_{\mathsf{B}} \otimes P_{\mathsf{AG}\to\mathsf{HR}})\, |\mathrm{EPR}\rangle_{\mathsf{BA}} \otimes |0\rangle_{\mathsf{G}} \ .$$

We say that $|\psi\rangle$ *is an ϵ-decodable black hole state* if there exists a quantum circuit D that takes as input register R and outputs a qubit labelled A, such that letting ρ_{HBA} denote the state $(\mathrm{id} \otimes D)(|\psi\rangle\!\langle\psi|)$, we have

$$\mathrm{F}\Big(|\mathrm{EPR}\rangle\!\langle\mathrm{EPR}|_{\mathsf{AB}} \ , \rho_{\mathsf{AB}}\Big) \geq 1 - \epsilon$$

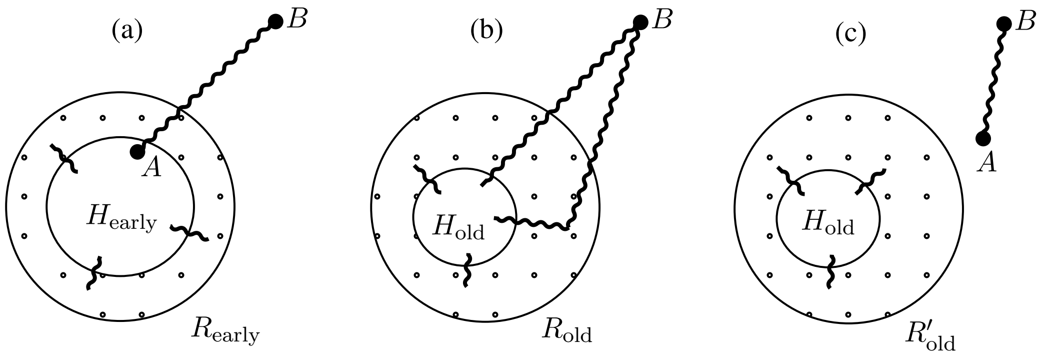

Figure 2: Decoding black hole radiation. (a) Qubit A, maximally entangled with qubit B, falls into an early black hole H_{early}, which is entangled with some early Hawking radiation R_{early}. (b) After evaporating much of its mass, the old black hole H_{old} is entangled with the radiation R_{old} which is entangled with the qubit B. (c) By performing a computation on the radiation only, the partner qubit A can be decoded.

i.e., measuring the registers BA in the Bell basis yields the state $|\mathrm{EPR}\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ with probability at least $1 - \epsilon$. We say that the circuit D is a *ϵ-decoder* for the state $|\psi\rangle$.

The circuit P generating the decodable black hole state can be thought of as a unitary that encodes the laws of black hole evolution: given a qubit in register A and a fixed number of ancilla qubits, it forms a black hole in register H as well as the outgoing Hawking radiation in register R. The decodability condition implies that, by acting on the radiation only, it is information-theoretically possible to decode the original qubit that was input. See Figure 2 for an illustration of black hole radiation decoding. We formalize black hole radiation decoding as a computational task.

Definition 10.2 (Black hole radiation decoding task)**.** Let $\epsilon(n), \delta(n)$ be functions. We say that a quantum algorithm $D = (D_x)_x$ solves the *ϵ-black hole radiation decoding task with error δ* if for all $x = (1^n, P)$ where P is a unitary quantum circuit acting on n qubits and gives rise to an $\epsilon(n)$-decodable black hole state $|\psi\rangle$, the circuit D_x is a $\delta(n)$-decoder for $|\psi\rangle$.

We now prove that the task of black hole radiation decoding in Definition 10.2 is equivalent to the Decodable Channel Problem in Definition 9.5, which results in the following theorem.

Theorem 10.3. *Let $\epsilon(n)$ be a negligible function. $\textsc{DistUhlmann}_{1-\epsilon}$ is solvable in polynomial-time with inverse polynomial error if and only if the $\epsilon(n)$-black hole radiation decoding task is solvable in polynomial-time with inverse polynomial error.*

Proof. We prove this via reduction to the Decodable Channel Problem described in Section 9.1. First, observe (from the proof) that the statement in Theorem 9.6 still holds when considering instances of the ϵ-Decodable Channel Problem of the form $y = (1^1, 1^r, C)$, i.e., where we restrict C to single qubit inputs only. Define the following bijection φ: for every $x = (1^n, P)$, where $P : \mathsf{AG} \to \mathsf{HR}$ is a unitary quantum circuit acting on n qubits and where r is the size of the register R, define $\varphi(x) = (1^1, 1^r, \tilde{P})$, where $\tilde{P}$ is the quantum circuit first appends $n - 1$ qubits initialized to $|0\rangle$ to its input and then runs P.

It is clear that x corresponds to an ϵ-decodable black hole state if and only if $\varphi(x)$ corresponds to an ϵ-decodable channel: the channel can be viewed as taking the input qubit, dumping it in the black hole, and the outputting the radiation emitted by the black hole. Decoding the EPR pair from the channel associated with $\tilde{P}$ exactly corresponds to decoding the EPR pair from the black hole associated with P. Therefore, the claim follows from Theorem 9.6, which shows that the complexity of the Decodable Channel Problem is equivalent to the complexity of DISTUHLMANN. □

Remark 10.4. We remark that Brakerski proved a stronger theorem by relating the black hole radiation task to EFI [BCQ23]. For simplicity, we focus on the task of decoding the EPR pair with fidelity $1 - \epsilon$, for a small ϵ, whereas Brakerski [Bra23] used amplification to boost weak decoders that succeed with fidelity much smaller than 1.

Part IV
Appendix

A Weak polarization for Uhlmann transformations

In this section we prove the following weak polarization lemma, which we can interpret as evidence for a stronger polarization statement, Conjecture 6.8.

Theorem 6.10. Let $p(n)$ be a polynomial. Suppose there is a polynomial-time algorithm Q that implements $\textsc{DistUhlmann}_{1-2^{-p(n)}}$ with average-case error at most $1/32$. Then for all $0 < \epsilon < 1$ there exists a quantum algorithm $A = (A_x)_{x\in\{0,1\}^*}$ that runs in $n^{O(1/\epsilon)}$ time, makes queries to the unitary purification of Q and its inverse, such that for all valid instances $x = (1^n, C, D)$ of $\textsc{Uhlmann}_{1/2}$,

$$\mathrm{F}((\mathrm{id} \otimes A_x)(|C\rangle\!\langle C|), |D\rangle\!\langle D|) \geq \frac{1}{2} - \epsilon\,.$$

At a high level, the algorithm operates as follows. Given a $\textsc{Uhlmann}_\kappa$ instance $x = (1^n, C, D)$, it computes the description of an instance $y = (1^k, F_+, F_-)$ of $\textsc{Uhlmann}_{1-2^{-p(n)}}$, resulting from applying parallel repetition, XOR repetition, and then parallel repetition again to the original instance x. We show that an algorithm that approximately implements the Uhlmann transform for y can be transformed into an algorithm that approximately implements the Uhlmann transform for x. This makes use of reductions from the following results.

The first is a parallel repetition theorem for Uhlmann transforms, which is a special case of the parallel repetition theorem for 3-message arguments proved by [BQSY24]:

Theorem A.1 (Efficient parallel repetition of Uhlmann transformations [BQSY24])**.** Let $0 < \delta < 1$ and $|C\rangle$ and $|D\rangle$ be a pair of bipartite states prepared by circuits C and D respectively. Suppose that there is a quantum algorithm Q such that

$$\mathrm{F}(Q(|C\rangle\!\langle C|^{\otimes t}), |D\rangle\!\langle D|^{\otimes t}) \geq \delta^t\,.$$

Then there is a $\mathrm{poly}(\delta^{-t}, \epsilon^{-1})$-time query algorithm R acting only on B (and additional ancilla), makes queries to the unitary purification of Q and its inverse, $C^\dagger$, and D, such that

$$\mathrm{F}(R(|C\rangle\!\langle C|), |D\rangle\!\langle D|) \geq \delta - \epsilon\,.$$

The second result is the so-called "swapping-distinguishing duality" theorem of Aaronson, Atia, and Susskind [AAS20]:

Theorem A.2 (Swapping-distinguishing duality, Theorem 1 from [AAS20])**.**

1. Let $|x\rangle, |y\rangle$ be orthogonal states, and suppose that $\langle y| U |x\rangle = a$ and $\langle x| U |y\rangle = b$. Then using a single black-box call to controlled-U, plus $O(1)$ additional gates, we can distinguish $|\psi\rangle = \frac{1}{\sqrt{2}}(|x\rangle + |y\rangle)$ and $|\phi\rangle = \frac{1}{\sqrt{2}}(|x\rangle - |y\rangle)$ with bias $\Delta = \frac{1}{2}|a + b|$.

2. Let $|\psi\rangle, |\phi\rangle$ be orthogonal states, and suppose that a quantum circuit A accepts $|\psi\rangle$ with probability p and accepts $|\phi\rangle$ with probability $p - \Delta$. Then using a single black-box call to A and $A^\dagger$, plus $O(1)$ additional gates, we can apply a unitary U such that

$$\frac{1}{2}\Big(|\langle y| U |x\rangle| + |\langle x| U |y\rangle|\Big) = \Delta$$

where $|x\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle + |\phi\rangle)$ and $|y\rangle = \frac{1}{\sqrt{2}}(|\psi\rangle - |\phi\rangle)$.

Proof of Theorem 6.10. We present the following argument for general κ, even though the theorem is only specified for $\kappa = 1/2$. Set parameters

$$m = \left\lceil \frac{\ln 8p(n)}{\ln \frac{1}{1-\epsilon/2}} \right\rceil \quad \text{and} \quad t = \left\lceil \frac{8p(n)}{\kappa^m} \right\rceil .$$

Note that this setting of parameters satisfies

$$\kappa^m \geq \frac{2p(n)}{t} \quad \text{and} \quad (\kappa - \epsilon/2)^m \leq \frac{1}{4t} .$$

We now describe the states $|F_\pm\rangle$ in more detail, and analyze their properties. First, define the pair of states

$$\begin{aligned} |E_+\rangle &= \frac{1}{\sqrt{2}} \left(|C\rangle^{\otimes m} |0\rangle + |D\rangle^{\otimes m} |1\rangle \right)_{\mathsf{A}^m \mathsf{B}^m \mathsf{O}} \\ |E_-\rangle &= \frac{1}{\sqrt{2}} \left(|C\rangle^{\otimes m} |0\rangle - |D\rangle^{\otimes m} |1\rangle \right)_{\mathsf{A}^m \mathsf{B}^m \mathsf{O}} . \end{aligned}$$

Note that $|E_+\rangle, |E_-\rangle$ are orthogonal. Then define

$$\begin{aligned} |F_+\rangle &= \frac{1}{\sqrt{2}} \Big(|E_+\rangle^{\otimes t} + |E_-\rangle^{\otimes t} \Big)_{\mathsf{A}^{m\times t} \mathsf{B}^{m \times t} \mathsf{O}^t} \\ |F_-\rangle &= \frac{1}{\sqrt{2}} \Big(|E_+\rangle^{\otimes t} - |E_-\rangle^{\otimes t} \Big)_{\mathsf{A}^{m\times t} \mathsf{B}^{m \times t} \mathsf{O}^t} . \end{aligned}$$

Index the registers by A_{ij}, B_{ij}, and O_j where $1 \leq i \leq m$ and $1 \leq j \leq t$. Let $k = t(m+1)$ denote the number of qubits of $|F_\pm\rangle$.

Let F_+, F_- denote the circuits that prepare the states $|F_+\rangle, |F_-\rangle$, respectively. Note that given the instance $x = (1^n, C, D)$, the instance $(1^k, F_+, F_-)$ can be computed in $\mathrm{poly}(m, t, n)$ time.

Claim A.3. $(1^k, F_+, F_-)$ is an instance of $\textsc{Uhlmann}_{1-2^{-p(n)}}$.

Proof. Let σ_0, σ_1 denote the reduced density matrices of $|C\rangle$ and $|D\rangle$ on A respectively. Then the observe that reduced density matrices of $|C\rangle^{\otimes m}$ and $|D\rangle^{\otimes m}$ on register A^m are $\sigma_0^{\otimes m}$ and $\sigma_1^{\otimes m}$, respectively.

Let $\tau_\pm$ denote the reduced density matrices of $|F_\pm\rangle$ on registers $\mathsf{A}^{m\times n}$ (i.e., the collection of registers A_{ij}). A simple calculation shows that

$$\begin{aligned} \tau_+ &= \frac{1}{2^{t-1}} \sum_{x:|x| \text{ even}} \sigma_{x_1}^{\otimes m} \otimes \sigma_{x_2}^{\otimes m} \otimes \cdots \otimes \sigma_{x_t}^{\otimes m} \\ \tau_- &= \frac{1}{2^{t-1}} \sum_{x:|x| \text{ odd}} \sigma_{x_1}^{\otimes m} \otimes \sigma_{x_2}^{\otimes m} \otimes \cdots \otimes \sigma_{x_t}^{\otimes m} . \end{aligned}$$

Watrous [Wat02, Proposition 6] showed that $\mathrm{td}(\tau_+, \tau_-) = \mathrm{td}(\sigma_0^{\otimes m}, \sigma_1^{\otimes m})^t$. Since $(1^n, C, D)$ is an instance of $\textsc{Uhlmann}_\kappa$ and by Fuchs-van de Graaf, we have $\mathrm{F}(\sigma_0^{\otimes m}, \sigma_1^{\otimes m}) \geq \kappa^m$ and therefore

$$\mathrm{td}(\tau_+, \tau_-) \leq (1 - \kappa^m)^{t/2} .$$

By Fuchs-van de Graaf again we have

$$\mathrm{F}(\tau_+, \tau_-) \geq (1 - \mathrm{td}(\tau_+, \tau_-))^2 \geq 1 - 2\mathrm{td}(\tau_+, \tau_-) \geq 1 - 2(1 - \kappa^m)^{t/2} .$$

Using that $1 - x \leq e^{-x}$ and our choice of m, t we have that

$$\mathrm{F}(\tau_+, \tau_-) \geq 1 - \exp\Big(- \frac{t}{2}\kappa^m \Big) \geq 1 - e^{-p(n)} .$$

□

Claim A.4. Suppose there was a quantum algorithm Q acting only on registers $\mathsf{B}_{ij}\mathsf{O}_j$ such that

$$\mathrm{td}((\mathrm{id} \otimes Q)(|F_+\rangle\langle F_+|), |F_-\rangle\langle F_-|) \leq \frac{1}{32} .$$

Then there exists a quantum algorithm A that for all ϵ can runs in $\mathrm{poly}(t, m, 1/\epsilon)$ time, makes queries to the unitary purification of Q and its inverse, acts on B (plus ancillas), such that

$$\mathrm{F}((\mathrm{id} \otimes A)(|C\rangle\langle C|), |D\rangle\langle D|) \geq (4t)^{-1/m} - \epsilon/2 .$$

Proof. Let $\delta = 1/32$. Let $\widetilde{Q}$ denote the unitary purification of Q. By Uhlmann's theorem and Fuchs-van de Graaf, there exists a pure state $|\eta\rangle$ such that

$$\Big(\langle F_-| \otimes \langle \eta| \, (\mathrm{id} \otimes \widetilde{Q}) \, |F_+\rangle \otimes |0\rangle \Big)^2 \geq (1 - \delta)^2 .$$

Here, the circuit $\widetilde{Q}$ acts on the registers $\mathsf{B}_{ij}\mathsf{O}_j$ as well as the ancilla zeroes. Translating to Euclidean distance, we have

$$\Big\| (\mathrm{id} \otimes \widetilde{Q}) \, |F_+\rangle \, |0\rangle - |F_-\rangle \, |\eta\rangle \Big\| \leq \sqrt{2\delta} .$$

The state $|\eta\rangle$ can be (approximately) prepared by using the circuit $\widetilde{Q}$, its inverse, and the circuits F_+, F_- for preparing $|F_+\rangle, |F_-\rangle$ respectively. Therefore there exists a circuit R such that

$$\Big| \langle F_-| \otimes \langle 0| \, (\mathrm{id} \otimes R) \, |F_+\rangle \otimes |0\rangle \Big|^2 \geq 1 - 8\delta \geq 3/4$$

where we used $\delta = 1/32$. By Theorem A.2, since $|E_\pm\rangle^{\otimes t} = \frac{1}{\sqrt{2}}\Big(|F_+\rangle \pm |F_-\rangle \Big)$ there exists an efficient quantum operation S that makes a single call to R and $R^\dagger$ that acts only on registers $\mathsf{B}_{ij}\mathsf{O}_j$ (plus ancillas) and distinguishes between $|E_+\rangle^{\otimes t}$ and $|E_-\rangle^{\otimes t}$ with advantage at least $3/8 \geq 1/4$.

By a hybrid argument, there exists a quantum operation S' (whose complexity is that of S plus the complexity of preparing $t-1$ copies of $|E_+\rangle$ or $|E_-\rangle$) that acts only on registers $\mathsf{B}^m\mathsf{O}$ and distinguishes between $|E_+\rangle$ and $|E_-\rangle$ with advantage at least $1/4t$.

By Theorem A.2 again, there exists an operation U acting only on registers $\mathsf{B}^m\mathsf{O}$ (plus ancillas) and makes a single call to S' to transform $|C\rangle^{\otimes m} |0\rangle$ to have overlap at least $1/4t$ with $|D\rangle^{\otimes m} |1\rangle$. By Theorem A.1, there exists an algorithm A acting only on register B (plus ancillas) with running time $\mathrm{poly}(m, 1/\epsilon)$, makes queries to U and $U^\dagger$, and maps $|C\rangle$ to have squared overlap at least $(4t)^{-1/m} - \epsilon/2$ with $|D\rangle$.

Taking into account the complexity of $\tilde{Q}, \tilde{R}, S, S', U$, we get that A runs in time $\mathrm{poly}(m, t, 1/\epsilon)$. □

Thus weak polarization theorem follows immediately from Claims A.3 and A.4. The algorithm A_x behaves as follows: it computes the description of $y = (1^k, F_+, F_-)$ in $\mathrm{poly}(m, t, n)$ time. By Claim A.3, this is an instance of $\textsc{Uhlmann}_{1-2^{-p(n)}}$. Then, invoke the algorithm A from Claim A.4 that queries the algorithm Q_y which implements the Uhlmann transform corresponding to y with error at most $1/32$. The resulting fidelity is at least $(4t)^{-1/m} - \epsilon/2$, which by our choice of parameters is at least $\kappa - \epsilon$. □

B Information-theoretic one-shot compression

In this section we prove Theorem 9.9, which for convenience we restate here:

Theorem 9.9 (Information-theoretic one-shot compression)**.** For all $\delta > 0$ and all density matrices ρ,

$$H_{\max}^{\epsilon_1}(\rho) \leq K^{\delta}(\rho) \leq H_{\max}^{\epsilon_2}(\rho) + 8 \log \frac{4}{\delta}$$

where $\epsilon_1 := 2\delta^{1/4}$ and $\epsilon_2 := (\delta/40)^4$.

This theorem shows that the smoothed max-entropy of a quantum state characterizes the extent to which it can be compressed in the one-shot setting.

The smoothed max entropy is just one of a rich zoo of entropy measures that are used in the setting of non-asymptotic quantum information theory [Tom13]. To prove Theorem 9.9 we employ the following entropy measures:

Definition B.1 (Min-, max-, and Rényi 2-entropy)**.** Let $\epsilon \geq 0$ and let ψ_{AB} be a density matrix on registers AB.

- The *min-entropy of register* A *conditioned on register* B *of the state* ψ is

  $$H_{\min}(\mathsf{A}|\mathsf{B})_{\psi} := -\log \inf_{\sigma \in \mathrm{Pos}(\mathsf{B}) : \psi_{\mathsf{AB}} \leq \mathrm{id}_{\mathsf{A}} \otimes \sigma_{\mathsf{B}}} \mathrm{Tr}(\sigma)$$

  The ϵ-*smoothed conditional min-entropy* is

  $$H_{\min}^{\epsilon}(\mathsf{A}|\mathsf{B})_{\psi} := \sup_{\sigma : P(\sigma,\psi) \leq \epsilon} H_{\min}(\mathsf{A}|\mathsf{B})_{\sigma} ,$$

  where $P(\sigma, \psi)$ is the purified distance (whose definition need not concern us, see [Tom13, Definition 3.15]).

- The *max-entropy of register* A *conditioned on register* B *of the state* ψ is

  $$H_{\max}(\mathsf{A}|\mathsf{B})_{\psi} := \sup_{\sigma \in \mathrm{Pos}(\mathsf{B}) : \mathrm{Tr}(\sigma) \leq 1} \log \| \sqrt{\psi_{\mathsf{AB}}} \sqrt{\mathrm{id}_{\mathsf{A}} \otimes \sigma_{\mathsf{B}}} \|_1^2 .$$

  The ϵ-*smoothed conditional max-entropy* is

  $$H_{\max}^{\epsilon}(\mathsf{A}|\mathsf{B})_{\psi} := \inf_{\sigma : \mathrm{td}(\sigma,\psi) \leq \epsilon} H_{\max}(\mathsf{A}|\mathsf{B})_{\sigma} .$$

- The *Rényi* 2-*entropy of register* A *conditioned on register* B *of the state* ψ is [Dup09, Definition 2.11]

  $$H_2(\mathsf{A}|\mathsf{B})_{\psi} := -\log \inf_{\sigma > 0} \mathrm{Tr}\Big(\big((\mathrm{id}_{\mathsf{A}} \otimes \sigma_{\mathsf{B}})^{-1/2} \psi_{\mathsf{AB}} \big)^2 \Big)$$

  where the infimum is over all positive definite density operators σ acting on register B. The ϵ-*smoothed conditional Rényi* 2-*entropy* is

  $$H_2^{\epsilon}(\mathsf{A}|\mathsf{B})_{\psi} := \sup_{\sigma : \mathrm{td}(\sigma,\psi) \leq \epsilon} H_2(\mathsf{A}|\mathsf{B})_{\sigma} .$$

We do not elaborate further on the meaning or motivation for the definitions of these entropy measures (we refer the reader to [Tom13, KRS09] for deeper discussions); we will only use the following properties of them:

Proposition B.2 (Relations between the entropy measures)**.** Let $\epsilon \geq 0$ and let $|\psi\rangle_{\mathsf{ABC}}$ be a tripartite pure state. The following relationships hold:

- (*Duality relation*) $H^{\epsilon}_{\min}(\mathsf{A}|\mathsf{B})_{\psi} = -H^{\epsilon}_{\max}(\mathsf{A}|\mathsf{C})_{\psi}$. We note that this duality relation only holds when ψ is a pure state on registers ABC.
- (*Bounds for conditional min/max-entropy*) Both $H^{\epsilon}_{\min}(\mathsf{A}|\mathsf{B})_{\psi}$ and $H^{\epsilon}_{\max}(\mathsf{A}|\mathsf{B})_{\psi}$ are bounded below by $-\log \mathrm{rank}(\psi_{\mathsf{A}})$, and bounded above by $\log \mathrm{rank}(\psi_{\mathsf{A}})$.
- (*Isometric invariance*) For all isometries V mapping register A to A' we have $H_{\min}(\mathsf{A}|\mathsf{B})_{\psi} = H_{\min}(\mathsf{A}'|\mathsf{B})_{V\psi V^{\dagger}}$.
- (*Min- versus* 2*-entropy*) $H_{\min}(\mathsf{A}|\mathsf{B})_{\psi} \leq H_2(\mathsf{A}|\mathsf{B})_{\psi}$.
- (*Operational interpretation of min-entropy*) When ψ_{AB} is diagonal (i.e., it corresponds to a bipartite probability distribution $p(a,b)$), $2^{-H_{\min}(\mathsf{A}|\mathsf{B})_{\psi}} = \sum_b p(b)\ \max_a p(a|b)$, i.e., the maximum probability of guessing the state of A given the state of B.
- (*Max-entropy does not decrease after appending a state*) For all density matrices $\sigma \in \mathrm{S}(\mathsf{D})$, we have $H^{\epsilon}_{\max}(\mathsf{A})_{\psi} \leq H^{\epsilon}_{\max}(\mathsf{AD})_{\psi\otimes\sigma}$.

Proof. A proof of the duality relation can be found in [Tom13, Theorem 5.4]. The bounds for the conditional min-entropy can be found in [Tom13, Proposition 4.3]; the bounds on the conditional max-entropy follow via the duality relation. The isometric invariance property follows directly from the definition of the (smoothed) conditional min-entropy. The min- versus 2-entropy bound is proved in [Dup09, Lemma 2.3]. The operational interpretation of min-entropy is given in [KRS09]. The fact that the max-entropy does not decrease after appending a state follows from [Tom13, Theorem 5.7], which states that the smoothed max-entropy is non-decreasing under trace-preserving quantum operations; consider the quantum operation $\psi_{\mathsf{A}} \mapsto \psi_{\mathsf{A}} \otimes \sigma_{\mathsf{D}}$, which is clearly trace-preserving. □

Having established the definitions and properties of these entropy measures, we now prove the characterization of the fundamental limits on one-shot compression for quantum states.

Proof of Theorem 9.9. **Lower bound.** We first prove the lower bound $H^{2\delta^{1/4}}_{\max}(\rho) \leq K^{\delta}(\rho)$. Let (E, D) denote a pair of quantum circuits that compresses ρ to $s = K^{\delta}(\rho)$ qubits with error δ. Let $|\psi\rangle_{\mathsf{AR}}$ denote a purification of ρ. Then using the Fuchs-van de Graaf inequality we get that

$$\mathrm{F}\Big((D \circ E)(\psi), \psi\Big) \geq 1 - 2\delta\ . \tag{B.1}$$

Let $\hat{E} : \mathsf{A} \to \mathsf{CE}, \hat{D} : \mathsf{C} \to \mathsf{AF}$ denote the unitary purifications of the channels corresponding to E and D, respectively. Then by Uhlmann's theorem, since $(\hat{D}\hat{E} \otimes \mathrm{id}_{\mathsf{R}})\,|\psi\rangle_{\mathsf{RA}}$ is a purification of $(D \circ E)(\psi)$ and $|\psi\rangle_{\mathsf{AR}}$ is pure, Equation (B.1) implies that there exists a pure state $|\theta\rangle_{\mathsf{EF}}$ such that

$$1 - 2\delta \leq \mathrm{F}\Big((D \circ E)(\psi), \psi\Big) = \mathrm{F}\Big((\hat{D} \circ \hat{E})(\psi), \psi_{\mathsf{AR}} \otimes \theta_{\mathsf{EF}}\Big) \leq \mathrm{F}\Big(\mathrm{Tr}_{\mathsf{BC}}\Big(\hat{D} \circ \hat{E}(\psi)\Big), \rho_{\mathsf{A}} \otimes \theta_{\mathsf{F}}\Big)\ .$$

The last inequality follows from monotonicity of the fidelity under partial trace. By Fuchs-van de Graaf we have

$$\mathrm{td}\Big(\mathrm{Tr}_{\mathsf{BC}}(\hat{D} \circ \hat{E}(\psi)), \rho_{\mathsf{A}} \otimes \theta_{\mathsf{F}}\Big) \leq \sqrt{2\delta}\,. \tag{B.2}$$

Next consider the following entropy bounds using the properties given by Proposition B.2:

$$\begin{aligned} s = \dim(\mathsf{C}) &\geq -H_{\min}(\mathsf{C}|\mathsf{RE})_{\hat{E}|\psi\rangle} \\ &= -H_{\min}(\mathsf{AF}|\mathsf{RE})_{\hat{D}\hat{E}|\psi\rangle} \\ &= H_{\max}(\mathsf{AF})_{\hat{D}\hat{E}|\psi\rangle} \\ &\geq H_{\max}^{2\delta^{1/4}}(\mathsf{AF})_{\rho_{\mathsf{B}}\otimes\theta_{\mathsf{R}}} \\ &\geq H_{\max}^{2\delta^{1/4}}(\mathsf{A})_{\rho}. \end{aligned}$$

The first item follows from the bounds on min-entropy. The second line follows from the isometric invariance of the min-entropy. The third line follows from the duality relation between min- and max-entropy. The fourth line follows from the definition of the smoothed max-entropy (B.2) and the relationship between the purified distance and trace distance [Tom13, Lemma 3.17]. The last line follows from the fact that the smoothed max-entropy does not decrease when appending a state. Putting everything together we have $H_{\max}^{2\delta^{1/4}}(\rho) \leq s = K^{\delta}(\rho)$ as desired.

Upper bound. We now prove the upper bound, i.e., show that there exists a pair of circuits (E, D) that compresses ρ to $s := H_{\max}^{\epsilon}(\rho) + 4\log\frac{8}{\delta}$ qubits with error δ, where $\epsilon = \delta^2/512$. Let ρ_{AR} be an arbitrary purification of ρ (with purifying register R).

We leverage the following *decoupling theorem*, which has been a ubiquitous tool in quantum information theory. Informally, a decoupling theorem states that applying a Haar-random unitary to the A system of a bipartite state ρ_{AR} and then tracing out an appropriately large subsystem of A will result in the remainder of A being *decoupled* (i.e., in tensor product) from the reference register R. There have been many decoupling theorems proved over the years (see, e.g., [HHWY08, Dup09, DBWR14, BCT16]); we use the following one due to Dupuis (together with the standard fact that Clifford unitaries form a 2-design).

Theorem B.3 (Decoupling Theorem [Dup09, Theorem 3.8])**.** Let ρ_{AB} be a density matrix, $\mathcal{T} : \mathsf{S}(\mathsf{A}) \to \mathsf{S}(\mathsf{E})$ be a completely positive superoperator, $\omega_{\mathsf{EA}'} = (\mathcal{T} \otimes \mathrm{id}_{\mathsf{A}'})(\Phi_{\mathsf{AA}'})$ (where Φ denotes the maximally entangled state), and $\epsilon \geq 0$. Then

$$\int \|(\mathcal{T} \circ U)(\rho_{\mathsf{AB}}) - \omega_{\mathsf{E}} \otimes \rho_{\mathsf{B}}\|_1 \, \mathrm{d}U \leq 2^{-\frac{1}{2}H_2^{\epsilon}(\mathsf{A}'|\mathsf{E})_{\omega} - \frac{1}{2}H_2^{\epsilon}(\mathsf{A}|\mathsf{B})_{\rho}} + 8\epsilon$$

where the integral is over the uniform measure on Clifford unitary matrices acting on B, and $\mathcal{T} \circ U$ denotes the superoperator where the input state is conjugated by U first, and then $\mathcal{T}$ is applied.

Define the following channel $\mathcal{T}$ that acts on A: it measures the first $n - s$ qubits of A in the standard basis to obtain a classical outcome $y \in \{0,1\}^{n-s}$, traces out A, and outputs y in register E. We now evaluate the state $\omega_{\mathsf{EA}'} = (\mathcal{T} \otimes \mathrm{id}_{\mathsf{A}'})(\Phi_{\mathsf{AA}'})$. This can be seen to be

$$\omega_{\mathsf{EA}'} = \sum_{y \in \{0,1\}^{n-s}} |yy\rangle\!\langle yy|_{\mathsf{EA}'_1} \otimes 2^{-s}\, \mathrm{id}_{\mathsf{A}'_2}$$

where A' is subdivided into two registers $\mathsf{A}'_1\mathsf{A}'_2$ with A'_1 isomorphic to E. The entropy $H_2^\epsilon(\mathsf{A}'|\mathsf{E})_\omega$ can be calculated as follows:

$$H_2^\epsilon(\mathsf{A}'|\mathsf{E})_\omega \geq H_2(\mathsf{A}'|\mathsf{E})_\omega \geq H_{\min}(\mathsf{A}'|\mathsf{E})_\omega \ .$$

The first inequality follows from the definition of the smoothed 2-entropy. The second inequality follows from Proposition B.2. Note that $\omega_{\mathsf{A}'\mathsf{E}}$ is a classical state (i.e., it is diagonal in the standard basis); using the operational definition of the min-entropy in this case we see that $H_{\min}(\mathsf{A}'|\mathsf{E}) = s$.

Now we bound the entropy $H_2^\epsilon(\mathsf{A}|\mathsf{R})_\rho$. Since ρ_{AR} is pure, Proposition B.2 gives us

$$-H_2^\epsilon(\mathsf{A}|\mathsf{R})_\rho \leq -H_{\min}^\epsilon(\mathsf{A}|\mathsf{R})_\rho = H_{\max}^\epsilon(\mathsf{A})_\rho \ .$$

By Theorem B.3, by averaging there exists a Clifford unitary U such that

$$\|(\mathcal{T} \circ U)(\rho_{\mathsf{AR}}) - \omega_{\mathsf{E}} \otimes \rho_{\mathsf{R}}\|_1 \leq 2^{-\frac{1}{2}(s - H_{\max}^\epsilon(\mathsf{A})_\rho)} + 8\epsilon := \nu \ .$$

Consider the following two purifications:

1. $|\Phi\rangle_{\mathsf{EE}'} \otimes |\rho\rangle_{\mathsf{AR}}$ where $|\Phi\rangle_{\mathsf{EE}'}$ denotes the maximally entangled state on two isomorphic registers E, E'. This is a purification of the density matrix $\omega_{\mathsf{E}} \otimes \rho_{\mathsf{R}}$.

2. $|\theta\rangle_{\mathsf{EE}'\mathsf{CRF}} := \sum_y |y\rangle_{\mathsf{E}} \otimes (\Pi_y U \otimes \mathrm{id}_{\mathsf{R}}) |\rho\rangle_{\mathsf{AR}} \otimes |0\rangle_{\mathsf{F}}$ where Π_y is the projection that maps A into $\mathsf{E}'\mathsf{C}$ with C being an s qubit register and E' being $n-s$ qubit register, projecting the first $n-s$ qubits of A into the $|y\rangle$ state. The register F is isomorphic to E and is used to ensure that the dimensions of both purifications are the same. This is a purification of $(\mathcal{T} \circ U)(\rho_{\mathsf{AR}})$.

By Fuchs-van de Graaf and Uhlmann's theorem there exist a partial isometry V mapping registers $\mathsf{E}'\mathsf{A}$ to $\mathsf{CE}'\mathsf{F}$ such that

$$\mathrm{td}\Big(V(\Phi_{\mathsf{EE}'} \otimes \rho_{\mathsf{AR}})V^\dagger \, , \, \theta_{\mathsf{EE}'\mathsf{CRF}}\Big) \leq \sqrt{2\nu} \ .$$

Let Ξ be an arbitrary channel completion of V. We show that Ξ can be used in place of V with small error. Let P denote the projection onto the support of V. Then we have

$$\Big|\mathrm{Tr}(P(\Phi_{\mathsf{EE}'} \otimes \rho_{\mathsf{AR}})) - 1\Big| \leq \mathrm{td}\Big(P(\Phi_{\mathsf{EE}'} \otimes \rho_{\mathsf{AR}})P, \theta_{\mathsf{EE}'\mathsf{CRF}}\Big) \leq \mathrm{td}\Big(V(\Phi_{\mathsf{EE}'} \otimes \rho_{\mathsf{AR}})V^\dagger, \theta_{\mathsf{EE}'\mathsf{CRF}}\Big) \leq \sqrt{2\nu} \, .$$

Let τ denote the post-measurement state of $\Phi_{\mathsf{EE}'} \otimes \rho_{\mathsf{AR}}$ after measuring the projector P; by the Gentle Measurement Lemma [Win99] we have $\mathrm{td}(\tau, \Phi_{\mathsf{EE}'} \otimes \rho_{\mathsf{AR}}) \leq 4\nu^{1/4}$. Thus

$$\begin{aligned}\mathrm{td}\Big(\Xi(\Phi_{\mathsf{EE}'} \otimes \rho_{\mathsf{AR}}) \, , \, \theta_{\mathsf{EE}'\mathsf{CRF}}\Big) &\leq \mathrm{td}\Big(\Xi(\Phi_{\mathsf{EE}'} \otimes \rho_{\mathsf{AR}}) \, , \, \Xi(\tau)\Big) + \mathrm{td}\Big(\Xi(\tau), V\tau V^\dagger\Big) \\ &\quad + \mathrm{td}\Big(V\tau V^\dagger, V(\Phi_{\mathsf{EE}'} \otimes \rho_{\mathsf{AR}})V^\dagger\Big) + \mathrm{td}\Big(V(\Phi_{\mathsf{EE}'} \otimes \rho_{\mathsf{AR}})V^\dagger \, , \, \theta_{\mathsf{EE}'\mathsf{CRF}}\Big) \\ &\leq 4\nu^{1/4} + 4\nu^{1/4} + \sqrt{2\nu} \leq 10\nu^{1/4} \, , \end{aligned} \tag{B.3}$$

where we used that $\Xi(\tau) = V\tau V^\dagger$ by definition of channel completion.

Similarly, let Λ be an arbitrary channel completion of the partial isometry $V^\dagger$. A similar argument shows that

$$\mathrm{td}\Big(\Phi_{\mathsf{EE}'} \otimes \rho_{\mathsf{AR}} \, , \, \Lambda(\theta_{\mathsf{EE}'\mathsf{CRF}})\Big) \leq 10\nu^{1/4} \ .$$

We now continue with Ξ instead of V and Λ instead of $V^\dagger$. Applying the channel that measures the register E in the standard basis to both arguments of the left-hand side of Equation (B.3) and using that the trace distance is non-increasing under quantum operations we have

$$\mathop{\mathbb{E}}_y \mathrm{td}\Big(\Xi(|y\rangle\langle y|_{\mathsf{E}'} \otimes |\rho\rangle\langle\rho|_{\mathsf{AR}})\,,\, 2^{n-s}\alpha_y\, |y\rangle\langle y|_{\mathsf{E}'} \otimes |\rho_{U,y}\rangle\langle\rho_{U,y}|_{\mathsf{CR}} \otimes |0\rangle\langle 0|_{\mathsf{F}}\Big) \leq 10\nu^{1/4}\,,$$

where the expectation is over a uniformly random y, and $\alpha_y := \|\Pi_y U\,|\rho\rangle_{\mathsf{AR}}\|^2$ and the pure state $|\rho_{U,y}\rangle_{\mathsf{RC}}$ is defined so that

$$\alpha_y^{-1/2}\,\Pi_y U\,|\rho\rangle_{\mathsf{AR}} = |y\rangle_{\mathsf{E}'} \otimes |\rho_{U,y}\rangle_{\mathsf{CR}}\ .$$

By monotonicity of the trace distance this implies that $\mathbb{E}_y\,|2^{n-s}\alpha_y - 1| \leq 10\nu^{1/4}$. Therefore by triangle inequality we have

$$\mathop{\mathbb{E}}_y \mathrm{td}\Big(\Xi(|y\rangle\langle y|_{\mathsf{E}'} \otimes |\rho\rangle\langle\rho|_{\mathsf{AR}})\,,\, |y\rangle\langle y|_{\mathsf{E}'} \otimes |\rho_{U,y}\rangle\langle\rho_{U,y}|_{\mathsf{CR}} \otimes |0\rangle\langle 0|_{\mathsf{F}}\Big) \leq 20\nu^{1/4}\,, \tag{B.4}$$

Define the following quantum circuits:

1. The circuit E acts on register A and behaves as follows: it appends a randomly chosen $|y\rangle$ in register E', applies the channel Ξ, and then traces out registers $\mathsf{E}'\mathsf{F}$. In other words, it implements the following channel:
$$E(\sigma_{\mathsf{A}}) = \mathop{\mathbb{E}}_y \mathrm{Tr}_{\mathsf{E}'\mathsf{F}}\Big(\Xi(|y\rangle\langle y|_{\mathsf{E}'} \otimes \sigma_{\mathsf{A}})\Big)\ .$$

2. The circuit D takes as input register C and behaves as follows: it appends a randomly chosen $|y\rangle$ in register E' and $|0\rangle$ in register F, applies the channel Λ, and then traces out register E'. In other words, it implements the following channel:
$$D(\tau_{\mathsf{C}}) = \mathop{\mathbb{E}}_y \mathrm{Tr}_{\mathsf{E}'}\Big(\Lambda(|y\rangle\langle y|_{\mathsf{E}'} \otimes \tau_{\mathsf{C}} \otimes |0\rangle\langle 0|_{\mathsf{F}})\Big)\ .$$

Then Equation (B.4) implies that

$$\mathop{\mathbb{E}}_y \mathrm{td}\Big(E(|\rho\rangle\langle\rho|_{\mathsf{AR}}),\ |\rho_{U,y}\rangle\langle\rho_{U,y}|_{\mathsf{CR}}\Big) \leq 20\nu^{1/4}$$
$$\mathop{\mathbb{E}}_y \mathrm{td}\Big(\ |\rho\rangle\langle\rho|_{\mathsf{AR}}\ ,\ D(|\rho_{U,y}\rangle\langle\rho_{U,y}|_{\mathsf{CR}})\Big) \leq 20\nu^{1/4}\ .$$

Put together this means

$$\mathop{\mathbb{E}}_y \mathrm{td}\Big((D \circ E)(|\rho\rangle\langle\rho|_{\mathsf{AR}}), |\rho\rangle\langle\rho|_{\mathsf{AR}}\Big) \leq 40\nu^{1/4}\ .$$

Although we have defined the circuits E, D in terms of the purification $|\rho\rangle_{\mathsf{AR}}$, observe that Uhlmann's theorem implies that the same circuits works for *all* purifications of ρ_{A}. Thus, since the output of channel E is register C which has size s qubits, this shows that (E, D) compresses ρ to s qubits with error $40\nu^{1/4}$. By our choice of $s = H^{\epsilon}_{\max}(\mathsf{B})_\rho + 8\log\frac{4}{\delta}$ and $\epsilon = (\delta/40)^4$, this error is at most δ. □

References

[AA24] Anurag Anshu and Srinivasan Arunachalam. “A survey on the complexity of learning quantum states”. In: *Nature Reviews Physics* 6.1 (2024), pp. 59–69. DOI: 10.1038/s42254-023-00662-4 (cit. on p. 14).

[Aar07] Scott Aaronson. “The learnability of quantum states”. In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 463.2088 (2007), pp. 3089–3114. DOI: 10.1098/rspa.2007.0113 (cit. on p. 14).

[Aar14] Scott Aaronson. “The Equivalence of Sampling and Searching”. In: *Theory of Computing Systems* 55.2 (2014), pp. 281–298. DOI: 10.1007/s00224-013-9527-3 (cit. on p. 30).

[Aar16] Scott Aaronson. *The Complexity of Quantum States and Transformations: From Quantum Money to Black Holes*. 2016. arXiv: 1607.05256 (cit. on pp. 4, 66, 79).

[Aar23] Scott Aaronson. *The Complexity Zoo*. https://complexityzoo.net/Complexity_Zoo. Accessed: 2023-04-01. 2023 (cit. on p. 7).

[AAS20] Scott Aaronson, Yosi Atia, and Leonard Susskind. *On the Hardness of Detecting Macroscopic Superpositions*. 2020. arXiv: 2009.07450 (cit. on pp. 72, 73, 82).

[ABK23] Scott Aaronson, Harry Buhrman, and William Kretschmer. “A qubit, a coin, and an advice string walk into a relational problem”. In: *arXiv preprint arXiv:2302.10332* (2023) (cit. on pp. 30, 31).

[ABV23] Rotem Arnon-Friedman, Zvika Brakerski, and Thomas Vidick. *Computational Entanglement Theory*. 2023. arXiv: 2310.02783 (cit. on p. 12).

[ACQ22] Dorit Aharonov, Jordan Cotler, and Xiao-Liang Qi. “Quantum algorithmic measurement”. In: *Nature Communications* 13.1 (2022), p. 887. DOI: 10.1038/s41467-021-27922-0 (cit. on p. 4).

[ADHW09] Anura Abeyesinghe, Igor Devetak, Patrick Hayden, and Andreas Winter. “The Mother of All Protocols: Restructuring Quantum Information’s Family Tree”. In: *Proceedings: Mathematical, Physical and Engineering Sciences* 465.2108 (2009), pp. 2537–2563. DOI: 10.1098/rspa.2009.0202 (cit. on pp. 4, 78).

[AE07] Andris Ambainis and Joseph Emerson. “Quantum t-designs: t-wise independence in the quantum world”. In: *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC’07)*. 2007, pp. 129–140. DOI: 10.1109/CCC.2007.26 (cit. on p. 66).

[AG04] Scott Aaronson and Daniel Gottesman. “Improved simulation of stabilizer circuits”. In: *Physical Review A* 70 (5 2004), p. 052328. DOI: 10.1103/PhysRevA.70.052328 (cit. on p. 75).

[AJW18] Anurag Anshu, Rahul Jain, and Naqueeb Ahmad Warsi. “A One-Shot Achievability Result for Quantum State Redistribution”. In: *IEEE Transactions on Information Theory* 64.3 (2018), pp. 1425–1435. DOI: 10.1109/TIT.2017.2776112 (cit. on p. 4).

[AK07] Scott Aaronson and Greg Kuperberg. “Quantum Versus Classical Proofs and Advice”. In: *Theory of Computing* 3.7 (2007), pp. 129–157. DOI: 10.4086/toc.2007.v003a007 (cit. on pp. 6, 15, 59).

[AMPS13] Ahmed Almheiri, Donald Marolf, Joseph Polchinski, and James Sully. “Black holes: complementarity or firewalls?” In: *Journal of High Energy Physics* 2013.2 (2013), p. 62. DOI: 10.1007/JHEP02(2013)062 (cit. on pp. 13, 79).

[AQY22] Prabhanjan Ananth, Luowen Qian, and Henry Yuen. “Cryptography from Pseudorandom Quantum States”. In: *Advances in Cryptology – CRYPTO 2022*. 2022, pp. 208–236. DOI: 10.1007/978-3-031-15802-5_8 (cit. on pp. 4, 10, 11, 76).

[BCQ23] Zvika Brakerski, Ran Canetti, and Luowen Qian. “On the Computational Hardness Needed for Quantum Cryptography”. In: *14th Innovations in Theoretical Computer Science Conference (ITCS 2023)*. Vol. 251. 2023. DOI: 10.4230/LIPIcs.ITCS.2023.24 (cit. on pp. 10, 11, 67, 72, 79, 81).

[BCR11] Mario Berta, Matthias Christandl, and Renato Renner. “The Quantum Reverse Shannon Theorem Based on One-Shot Information Theory”. In: *Communications in Mathematical Physics* 306.3 (2011), pp. 579–615. DOI: 10.1007/s00220-011-1309-7 (cit. on p. 4).

[BCT16] Mario Berta, Matthias Christandl, and Dave Touchette. “Smooth Entropy Bounds on One-Shot Quantum State Redistribution”. In: *IEEE Transactions on Information Theory* 62.3 (2016), pp. 1425–1439. DOI: 10.1109/TIT.2016.2516006 (cit. on p. 87).

[BFL91] László Babai, Lance Fortnow, and Carsten Lund. “Non-deterministic exponential time has two-prover interactive protocols”. In: *computational complexity* 1.1 (1991), pp. 3–40. DOI: 10.1007/BF01200056 (cit. on p. 38).

[BFV20] Adam Bouland, Bill Fefferman, and Umesh Vazirani. “Computational Pseudorandomness, the Wormhole Growth Paradox, and Constraints on the AdS/CFT Duality (Abstract)”. In: *11th Innovations in Theoretical Computer Science Conference (ITCS 2020)*. Vol. 151. 2020. DOI: 10.4230/LIPIcs.ITCS.2020.63 (cit. on p. 13).

[BMV03] Elwyn Berlekamp, Robert McEliece, and Henk Van Tilborg. “On the inherent intractability of certain coding problems (corresp.)” In: *IEEE Transactions on Information theory* 24.3 (2003), pp. 384–386 (cit. on p. 69).

[BO21] Costin Bădescu and Ryan O’Donnell. “Improved Quantum Data Analysis”. In: *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*. 2021, pp. 1398–1411. DOI: 10.1145/3406325.3451109 (cit. on p. 14).

[BQSY24] John Bostanci, Luowen Qian, Nicholas Spooner, and Henry Yuen. “An Efficient Quantum Parallel Repetition Theorem and Applications”. In: *Proceedings of the 56th Annual ACM SIGACT Symposium on Theory of Computing*. 2024. DOI: 10.1145/3618260.3649603 (cit. on pp. 62, 63, 82).

[Bra23] Zvika Brakerski. “Black-Hole Radiation Decoding Is Quantum Cryptography”. In: *Advances in Cryptology – CRYPTO 2023*. 2023, pp. 37–65. DOI: 10.1007/978-3-031-38554-4_2 (cit. on pp. 5, 13, 79, 81).

[BRS^{+}16] Adam R Brown, Daniel A Roberts, Leonard Susskind, Brian Swingle, and Ying Zhao. “Complexity, action, and black holes”. In: *Physical Review D* 93 (8 2016), p. 086006. DOI: 10.1103/PhysRevD.93.086006 (cit. on p. 13).

[BT06] Andrej Bogdanov and Luca Trevisan. “Average-case complexity”. In: *Foundations and Trends® in Theoretical Computer Science* 2.1 (2006), pp. 1–106 (cit. on p. 30).

[CCLY21] Nai-Hui Chia, Kai-Min Chung, Qipeng Liu, and Takashi Yamakawa. "On the Impossibility of Post-Quantum Black-Box Zero-Knowledge in Constant Round". In: *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*. 2021, pp. 59–67. DOI: 10.1109/FOCS52979.2021.00015 (cit. on p. 31).

[CLS01] Claude Crépeau, Frédéric Légaré, and Louis Salvail. "How to Convert the Flavor of a Quantum Bit Commitment". In: *Advances in Cryptology - EUROCRYPT 2001*. Vol. 2045. 2001, pp. 60–77. DOI: 10.1007/3-540-44987-6_5 (cit. on p. 61).

[CY13] Matthew Coudron and Henry Yuen. "Infinite randomness expansion and amplification with a constant number of devices". In: *arXiv preprint arXiv:1310.6755* (2013) (cit. on p. 55).

[DBWR14] Frédéric Dupuis, Mario Berta, Jürg Wullschleger, and Renato Renner. "One-Shot Decoupling". In: *Communications in Mathematical Physics* 328.1 (2014), pp. 251–284. DOI: 10.1007/s00220-014-1990-4 (cit. on p. 87).

[Dup09] Frédéric Dupuis. "The decoupling approach to quantum information theory". PhD thesis. Université de Montréal, 2009. HDL: 1866/3363 (cit. on pp. 13, 85–87).

[FR21] Bill Fefferman and Zachary Remscrim. "Eliminating intermediate measurements in space-bounded quantum computation". In: *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*. 2021, pp. 1343–1356 (cit. on p. 28).

[GJMZ23] Sam Gunn, Nathan Ju, Fermi Ma, and Mark Zhandry. "Commitments to Quantum States". In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. 2023, pp. 1579–1588. DOI: 10.1145/3564246.3585198 (cit. on p. 61).

[GMR89] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. "The Knowledge Complexity of Interactive Proof Systems". In: *SIAM Journal on Computing* 18.1 (1989), pp. 186–208 (cit. on pp. 7, 35).

[GR21] Uma Girish and Ran Raz. "Eliminating intermediate measurements using pseudorandom generators". In: *arXiv preprint arXiv:2106.11877* (2021) (cit. on p. 28).

[GSV98] Oded Goldreich, Amit Sahai, and Salil Vadhan. "Honest-Verifier Statistical Zero-Knowledge Equals General Statistical Zero-Knowledge". In: *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*. 1998, pp. 399–408. DOI: 10.1145/276698.276852 (cit. on p. 38).

[GW11] Craig Gentry and Daniel Wichs. "Separating Succinct Non-Interactive Arguments from All Falsifiable Assumptions". In: *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing*. 2011, pp. 99–108. DOI: 10.1145/1993636.1993651 (cit. on pp. 11, 65).

[Har13] Aram W. Harrow. *The Church of the Symmetric Subspace*. 2013. arXiv: 1308.6595 (cit. on p. 77).

[Haw76] Stephen W Hawking. "Breakdown of predictability in gravitational collapse". In: *Physical Review D* 14 (10 1976), pp. 2460–2473. DOI: 10.1103/PhysRevD.14.2460 (cit. on p. 4).

[HH13] Daniel Harlow and Patrick Hayden. "Quantum computation vs. firewalls". In: *Journal of High Energy Physics* 2013.6 (2013), p. 85. DOI: 10.1007/JHEP06(2013)085 (cit. on pp. 5, 13, 79).

[HHWY08] Patrick Hayden, Michał Horodecki, Andreas Winter, and Jon Yard. “A Decoupling Approach to the Quantum Capacity”. In: *Open Systems & Information Dynamics* 15.01 (2008), pp. 7–19. DOI: 10.1142/S1230161208000043 (cit. on pp. 4, 87).

[HKP20] Hsin-Yuan Huang, Richard Kueng, and John Preskill. “Predicting many properties of a quantum system from very few measurements”. In: *Nature Physics* 16.10 (2020), pp. 1050–1057. DOI: 10.1038/s41567-020-0932-7 (cit. on pp. 14, 31).

[HL11] Min-Hsiu Hsieh and François Le Gall. “NP-hardness of decoding quantum error-correction codes”. In: *Physical Review A—Atomic, Molecular, and Optical Physics* 83.5 (2011), p. 052331 (cit. on p. 69).

[HMY23] Minki Hhan, Tomoyuki Morimae, and Takashi Yamakawa. “From the Hardness of Detecting Superpositions to Cryptography: Quantum Public Key Encryption and Commitments”. In: *Advances in Cryptology – EUROCRYPT 2023*. 2023, pp. 639–667. DOI: 10.1007/978-3-031-30545-0_22 (cit. on p. 61).

[IL89] Russell Impagliazzo and Michael Luby. “One-way functions are essential for complexity based cryptography”. In: *30th Annual Symposium on Foundations of Computer Science*. 1989, pp. 230–235. DOI: 10.1109/SFCS.1989.63483 (cit. on pp. 11, 14).

[Imp95] Russell Impagliazzo. “A personal view of average-case complexity”. In: *Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference*. 1995, pp. 134–147. DOI: 10.1109/SCT.1995.514853 (cit. on pp. 11, 14).

[IP15] Pavithran Iyer and David Poulin. “Hardness of decoding quantum stabilizer codes”. In: *IEEE Transactions on Information Theory* 61.9 (2015), pp. 5209–5223 (cit. on p. 69).

[JJUW11] Rahul Jain, Zhengfeng Ji, Sarvagya Upadhyay, and John Watrous. “QIP = PSPACE”. In: *Journal of the ACM* 58.6 (2011). DOI: 10.1145/2049697.2049704 (cit. on pp. 5, 9, 20).

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. “Pseudorandom Quantum States”. In: *Advances in Cryptology – CRYPTO 2018*. 2018, pp. 126–152. DOI: 10.1007/978-3-319-96878-0_5 (cit. on pp. 9, 13, 14, 52, 53, 66, 76).

[JNV$^+$21] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. “MIP* = RE”. In: *Communications of the ACM* 64.11 (2021), pp. 131–138. DOI: 10.1145/3485628 (cit. on p. 38).

[KA04] Elham Kashefi and Carolina Moura Alves. *On the Complexity of Quantum Languages*. 2004. arXiv: quant-ph/0404062 (cit. on p. 4).

[KLL$^+$17] Shelby Kimmel, Cedric Yen-Yu Lin, Guang Hao Low, Maris Ozols, and Theodore J. Yoder. “Hamiltonian simulation with optimal sample complexity”. In: *npj Quantum Information* 3.1 (2017). DOI: 10.1038/s41534-017-0013-7 (cit. on pp. 31, 34).

[KQST23] William Kretschmer, Luowen Qian, Makrand Sinha, and Avishay Tal. “Quantum Cryptography in Algorithmica”. In: *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*. 2023, pp. 1589–1602. DOI: 10.1145/3564246.3585225 (cit. on pp. 4, 10, 11, 76).

[Kre21] William Kretschmer. “Quantum Pseudorandomness and Classical Complexity”. In: *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*. Vol. 197. 2021. DOI: 10.4230/LIPIcs.TQC.2021.2 (cit. on pp. 4, 10, 11, 76).

[KRS09] Robert Konig, Renato Renner, and Christian Schaffner. “The Operational Meaning of Min- and Max-Entropy”. In: *IEEE Transactions on Information Theory* 55.9 (2009), pp. 4337–4347. DOI: 10.1109/TIT.2009.2025545 (cit. on p. 86).

[KT23] Dakshita Khurana and Kabir Tomer. *Commitments from Quantum One-Wayness*. 2023. arXiv: 2310.11526 (cit. on p. 11).

[KW00] Alexei Kitaev and John Watrous. “Parallelization, Amplification, and Exponential Time Simulation of Quantum Interactive Proof Systems”. In: *Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing*. 2000, pp. 608–617. DOI: 10.1145/335305.335387 (cit. on pp. 5, 8).

[KW20] Sumeet Khatri and Mark M. Wilde. *Principles of Quantum Communication Theory: A Modern Approach*. 2020. arXiv: 2011.04672 (cit. on p. 11).

[LC98] Hoi-Kwong Lo and H.F. Chau. “Why quantum bit commitment and ideal quantum coin tossing are impossible”. In: *Physica D: Nonlinear Phenomena* 120.1 (1998). Proceedings of the Fourth Workshop on Physics and Consumption, pp. 177–187. DOI: 10.1016/S0167-2789(98)00053-0 (cit. on pp. 4, 10, 61, 62).

[LFKN92] Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. “Algebraic methods for interactive proof systems”. In: *Journal of the ACM* 39.4 (1992), pp. 859–868. DOI: 10.1145/146585.146605 (cit. on p. 20).

[LMR14] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost. “Quantum principal component analysis”. In: *Nature Physics* 10.9 (2014), pp. 631–633. DOI: 10.1038/nphys3029 (cit. on pp. 31, 34).

[LMW23] Alex Lombardi, Fermi Ma, and John Wright. *A one-query lower bound for unitary synthesis and breaking quantum cryptography*. 2023. arXiv: 2310.08870 (cit. on pp. 4, 11, 15).

[LP20] Yanyi Liu and Rafael Pass. “On One-way Functions and Kolmogorov Complexity”. In: *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*. 2020, pp. 1243–1254. DOI: 10.1109/FOCS46700.2020.00118 (cit. on p. 14).

[May97] Dominic Mayers. “Unconditionally Secure Quantum Bit Commitment is Impossible”. In: *Physical Review Letters* 78 (17 1997), pp. 3414–3417. DOI: 10.1103/PhysRevLett.78.3414 (cit. on pp. 4, 10, 61, 62).

[MY22] Tomoyuki Morimae and Takashi Yamakawa. “Quantum Commitments and Signatures Without One-Way Functions”. In: *Advances in Cryptology – CRYPTO 2022*. 2022, pp. 269–295. DOI: 10.1007/978-3-031-15802-5_10 (cit. on pp. 4, 10, 11, 14, 78).

[MY23] Tony Metger and Henry Yuen. “$\mathsf{stateQIP} = \mathsf{statePSPACE}$”. In: *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*. 2023, pp. 1349–1356. DOI: 10.1109/FOCS57990.2023.00082 (cit. on pp. 7, 9, 20, 21, 31, 35, 40, 56–58, 68).

[Nao03] Moni Naor. “On Cryptographic Assumptions and Challenges”. In: *Advances in Cryptology – CRYPTO 2003*. 2003, pp. 96–109. DOI: 10.1007/978-3-540-45146-4_6 (cit. on pp. 10, 11, 65).

[Nao91] Moni Naor. “Bit commitment using pseudorandomness”. In: *Journal of Cryptology* 4 (1991), pp. 151–158 (cit. on p. 11).

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: 10.1017/CBO9780511976667 (cit. on p. 17).

[Oka96] Tatsuaki Okamoto. "On Relationships between Statistical Zero-Knowledge Proofs". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. 1996, pp. 649–658. DOI: 10.1145/237814.238016 (cit. on p. 38).

[Ost91] Rafail Ostrovsky. "One-Way Functions, Hard on Average Problems, and Statistical Zero-Knowledge Proofs." In: *SCT*. Citeseer. 1991, pp. 133–138 (cit. on pp. 11, 64).

[OW16] Ryan O'Donnell and John Wright. "Efficient quantum tomography". In: *Proceedings of the forty-eighth annual ACM symposium on Theory of Computing*. 2016, pp. 899–912 (cit. on p. 31).

[Pap97] Christos H. Papadimitriou. "NP-completeness: A retrospective". In: *Automata, Languages and Programming*. 1997, pp. 2–6. DOI: 10.1007/3-540-63165-8_160 (cit. on p. 14).

[Pre92] John Preskill. "Do Black Holes Destroy Information?" In: *Proceedings of the International Symposium on Black Holes, Membranes, Wormholes and Superstrings*. World Scientific. 1992, pp. 22–39. DOI: 10.1142/9789814536752 (cit. on p. 13).

[Ren22] Joseph M. Renes. *Quantum Information Theory. Concepts and Methods*. De Gruyter Oldenbourg, 2022. DOI: 10.1515/9783110570250 (cit. on pp. 11, 69).

[Ros24] Gregory Rosenthal. "Efficient quantum state synthesis with one query". In: *Proceedings of the 2024 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*. SIAM. 2024, pp. 2508–2534 (cit. on pp. 9, 52–54).

[RY22] Gregory Rosenthal and Henry Yuen. "Interactive Proofs for Synthesizing Quantum States and Unitaries". In: *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*. Vol. 215. 2022. DOI: 10.4230/LIPIcs.ITCS.2022.112 (cit. on pp. 5, 7, 9, 19–21, 31, 33–35, 37, 52, 58).

[Sch95] Benjamin Schumacher. "Quantum coding". In: *Physical Review A* 51 (4 1995), pp. 2738–2747. DOI: 10.1103/PhysRevA.51.2738 (cit. on pp. 13, 74).

[Sha48] Claude E. Shannon. "A mathematical theory of communication". In: *The Bell System Technical Journal* 27.3 (1948), pp. 379–423. DOI: 10.1002/j.1538-7305.1948.tb01338.x (cit. on p. 13).

[Sha92] Adi Shamir. "IP = PSPACE". In: *Journal of the ACM* 39.4 (1992), pp. 869–877. DOI: 10.1145/146585.146609 (cit. on p. 20).

[Sus16] Leonard Susskind. "Computational complexity and black hole horizons". In: *Fortschritte der Physik* 64.1 (2016), pp. 24–43. DOI: 10.1002/prop.201500092 (cit. on p. 13).

[SV03] Amit Sahai and Salil Vadhan. "A Complete Problem for Statistical Zero Knowledge". In: *Journal of the ACM* 50.2 (2003), pp. 196–249. DOI: 10.1145/636865.636868 (cit. on pp. 9, 44, 50).

[TCR09] Marco Tomamichel, Roger Colbeck, and Renato Renner. "A Fully Quantum Asymptotic Equipartition Property". In: *IEEE Transactions on Information Theory* 55.12 (2009), pp. 5840–5847. DOI: 10.1109/TIT.2009.2032797 (cit. on p. 74).

[Tom13] Marco Tomamichel. *A Framework for Non-Asymptotic Quantum Information Theory*. 2013. arXiv: 1203.2142 (cit. on pp. 13, 85–87).

[Uhl76] Armin Uhlmann. "The "transition probability" in the state space of a $*$-algebra". In: *Reports on Mathematical Physics* 9.2 (1976), pp. 273–279. DOI: 10.1016/0034-4877(76)90060-4 (cit. on pp. 4, 39).

[Var97] Alexander Vardy. "The intractability of computing the minimum distance of a code". In: *IEEE Transactions on Information Theory* 43.6 (1997), pp. 1757–1766 (cit. on p. 69).

[Vaz01] Vijay V Vazirani. *Approximation algorithms*. Vol. 1. Springer, 2001 (cit. on p. 30).

[VW16] Thomas Vidick and John Watrous. "Quantum Proofs". In: *Foundations and Trends® in Theoretical Computer Science* 11.1-2 (2016), pp. 1–215. DOI: 10.1561/0400000068 (cit. on p. 18).

[Wat02] John Watrous. "Limits on the power of quantum statistical zero-knowledge". In: *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.* 2002, pp. 459–468. DOI: 10.1109/SFCS.2002.1181970 (cit. on pp. 8, 35, 50, 83).

[Wat06] John Watrous. "Zero-Knowledge against Quantum Attacks". In: *Proceedings of the Thirty-Eighth Annual ACM Symposium on Theory of Computing*. 2006, pp. 296–305. DOI: 10.1145/1132516.1132560 (cit. on pp. 7, 35, 38).

[Wat99] John Watrous. "Space-Bounded Quantum Complexity". In: *Journal of Computer and System Sciences* 59.2 (1999), pp. 281–326. DOI: 10.1006/jcss.1999.1655 (cit. on p. 35).

[Wil17] Mark M. Wilde. *Quantum Information Theory*. 2nd ed. Cambridge University Press, 2017. DOI: 10.1017/CBO9781139525343 (cit. on pp. 11, 17, 40, 45, 69).

[Win99] Andreas Winter. "Coding theorem and strong converse for quantum channels". In: *IEEE Transactions on Information Theory* 45.7 (1999), pp. 2481–2485. DOI: 10.1109/18.796385 (cit. on p. 88).

[Yan22] Jun Yan. "General Properties of Quantum Bit Commitments (Extended Abstract)". In: *Advances in Cryptology – ASIACRYPT 2022*. 2022, pp. 628–657. DOI: 10.1007/978-3-031-22972-5_22 (cit. on pp. 10, 60, 61).

[YE23] Lisa Yang and Netta Engelhardt. *The Complexity of Learning (Pseudo)random Dynamics of Black Holes and Other Chaotic Systems*. 2023. arXiv: 2302.11013 (cit. on p. 13).