

Unitary Complexity and the Uhlmann Transformation Problem

John Bostanci¹, Yuval Efron¹, Tony Metger²,
Alexander Poremba³, Luowen Qian⁴, and Henry Yuen¹

¹Columbia University

²ETH Zürich

³Caltech

⁴Boston 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	4
1.1	A fully quantum complexity theory	5
1.2	Structural results about the Uhlmann Transformation Problem	8
1.3	Centrality of the Uhlmann Transformation Problem	11
1.4	Summary and future directions	16
2	Preliminaries	18
2.1	Notation	18
2.2	Partial isometries and channel completions	19
2.3	Quantum circuits	20
2.4	Quantum state complexity classes	20
I	Unitary Complexity Theory	22
3	Unitary Synthesis Problems and Unitary Complexity Classes	22
3.1	Unitary synthesis problems	22
3.2	Unitary complexity classes	24
3.3	Reductions	27
3.4	Discussion and open problems	30
4	Interactive Proofs for Unitary Synthesis	31
4.1	Quantum interactive protocols	31
4.2	Interactive proofs for unitary synthesis	32
4.3	Zero-knowledge protocols for state and unitary synthesis	34
II	Uhlmann Transformation Problem: Definitions and Structural Results	37
5	Definition of the Uhlmann Transformation Problem	37
5.1	Uhlmann’s theorem and canonical isometries	37
5.2	Worst-case Uhlmann transformation problem	40
5.3	Distributional Uhlmann transformation problem	41
6	Structural Results about the Uhlmann Transformation Problem	44
6.1	Completeness for unitary zero knowledge	44
6.2	Hardness amplification	52
6.3	The padding trick	60
6.4	A polarization lemma for unitary zero knowledge?	62
7	Structural Results about the Succinct Uhlmann Transformation Problem	63
7.1	Completeness for avgUnitaryQIP	63
7.2	Completeness for avgUnitaryPSPACE	74
7.3	Completeness for worst-case unitaryPSPACE	76
7.4	Relationship between avgUnitaryPSPACE and PSPACE	78

III	Uhlmann Transformation Problem: Applications	81
8	Applications to Quantum Cryptography	81
8.1	Quantum commitment schemes	81
8.2	Unclonable state generators	86
8.3	Falsifiable quantum cryptographic assumptions	91
8.4	Open problems	94
9	Applications to Quantum Shannon Theory	95
9.1	Decoding channels	95
9.2	Compressing quantum information	102
9.3	Complexity of classical Shannon tasks?	112
9.4	Open problems	112
10	Applications to Computational Tasks in High-Energy Physics	113
10.1	Black hole radiation decoding	113
10.2	Interference detection	115
10.3	Open problems	119

1 Introduction

Uhlmann’s theorem [Uhl76] is 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

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

where $F(\rho, \sigma)$ 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

Transforming entangled states via local operations is a ubiquitous task 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, MY22b, 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 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 QIP = 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.

These examples motivate investigating a computational task we call the *Uhlmann Transformation Problem* (denoted by the shorthand UHLMANN): given the classical description of quantum circuits C, D acting on $2n$ qubits and an n -qubit quantum system (in some unknown state), apply the Uhlmann transformation U for the state pair $(|C\rangle, |D\rangle)$ to the given quantum system, where $|C\rangle = C |0^{2n}\rangle$ and $|D\rangle = D |0^{2n}\rangle$.

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

What is the complexity of UHLMANN? What are the implications for the complexity of the tasks mentioned in the examples above? For instance, many protocols developed in quantum Shannon theory achieve asymptotically optimal communication rates, but are not known to be computationally efficient due to the use of Uhlmann transformations for decoding. Could solving UHLMANN be *necessary* for these protocols? What would that mean for quantum cryptography or quantum gravity? Despite the prevalence of Uhlmann transformations in quantum information processing, these questions have not been studied systematically.

The goal of this paper is to study these questions formally. Since Uhlmann transformations are inherently quantum operations and cannot meaningfully be phrased as decision or function problems, we need to extend the language of complexity theory to *unitary synthesis problems*, i.e. computational problems that involve implementing a unitary operation on a quantum system in an unknown state. The first main contribution of this paper 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 the setting of unitary synthesis problems. 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 `unitaryPSPACE` and `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, unclonable state generators, quantum state compression, decoding of noisy quantum channels, and more.

1.1 A fully quantum complexity theory

The complexity of Uhlmann transformations deals with the hardness of implementing a unitary *transformation*, where the inputs and outputs of the task are quantum states. Traditional complexity classes deal with tasks with classical inputs and outputs (e.g., solving a decision problem or computing a Boolean function) — which appears inadequate for capturing the complexity of Uhlmann transformations, or more generally of implementing unitaries on unknown input states. To study the hardness of problems with quantum inputs or outputs, we need a new framework.

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]. Indeed, the oracle separations mentioned above [Kre21, KQST23, LMW23] demonstrate 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 $P = NP$, certain quantum cryptographic primitives could still remain secure. In fact, [LMW23] gives evidence that the ability to solve *any* decision problem (even undecidable ones!) would not help with breaking quantum cryptography.

Recently, Rosenthal and Yuen initiated the study of complexity classes for *state synthesis* and *unitary synthesis* problems [RY22]. 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 `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*. A unitary synthesis problem is a sequence of unitary² operators $(U_x)_{x \in \{0,1\}^*}$ and a unitary complexity class is a collection of unitary synthesis problems. For example the class `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 `unitaryBQP`, since given x , the algorithm A can just execute the circuit specified 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 formulate questions and conjectures about the computational hardness of inherently quantum problems. For example, we can ask whether `unitaryPSPACE` is contained in `unitaryBQPPSPACE` — 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 $\mathcal{U} = (U_x)_x$ polynomial-time reduces to $\mathcal{V} = (V_x)_x$ if an efficient algorithm for implementing \mathcal{V} implies an efficient algorithm for implementing \mathcal{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 the natural generalisation of traditional average-case complexity statements to the unitary setting. This notion

²In 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.

³We remark that this question is open — this is related to the “Unitary Synthesis Problem” raised by Aaronson and Kuperberg [\[AK07\]](#). Recent work [\[LMW23\]](#) gives evidence that the Unitary Synthesis Problem has a negative answer: they show that the complexity of unitary transformations cannot be generically reduced to making a single query to an arbitrary Boolean function.

turns out to be particularly natural in the context of entanglement transformation problems because it is equivalent to implementing the unitary on one half of a fixed larger 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.

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 $\mathcal{U} = (U_x)_x$, a polynomial-time verifier receives an instance x and a quantum system \mathbf{B} as input, and interacts with an all-powerful but untrusted prover to try to apply U_x to system \mathbf{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 generalizes 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 \mathbf{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. This model gives rise to the unitary complexity class `avgUnitarySZKHV`,⁵ which is a unitary synthesis analogue of the decision class `QSZKHV` in traditional complexity theory. Interestingly, for reasons that we explain in more detail in [Section 4.3](#), the average-case aspect of `avgUnitarySZKHV` 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’s sake, 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, nor do we distinguish between uniform and non-uniform unitary complexity classes. After each informal result statement we point the reader to where the formal result is stated and proved.

⁴The class `unitaryQIP` was also briefly discussed informally by Rosenthal and Yuen [\[RY22\]](#).

⁵The “HV” modifier signifies that the zero-knowledge property is only required to hold with respect to verifiers that honestly follow the protocol.

1.2 Structural results about the Uhlmann Transformation Problem

Equipped with the proper language to talk about unitary synthesis problems, we now turn to the Uhlmann Transformation Problem. 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 $\kappa \leq \kappa'$. We provide formal definitions of UHLMANN, 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 $\kappa = 1 - \epsilon$ for negligibly small ϵ as a function of the length of the string specifying an instance x) *exactly characterizes* the complexity of the unitary complexity class $\text{avgUnitarySZK}_{\text{HV}}$, which is the unitary synthesis version of QSZK_{HV} [[Wat02](#)].

Theorem 1.2 (Informal). *UHLMANN $_{1-\epsilon}$ for negligibly small ϵ is complete for $\text{avgUnitarySZK}_{\text{HV}}$ 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 if one can efficiently solve UHLMANN $_{1-\epsilon}$ in the average case (meaning that one can approximately map the input state $|C\rangle$ to $|D\rangle$ by acting locally), then one can efficiently solve any other distributional unitary synthesis problem in $\text{avgUnitarySZK}_{\text{HV}}$. This uses a characterization of quantum interactive protocols due to Kitaev and Watrous [[KW00](#)].

The second direction is to show that UHLMANN $_{1-\epsilon}$ is in $\text{avgUnitarySZK}_{\text{HV}}$ 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.

Hardness amplification for UHLMANN. We then prove a *hardness amplification* result for the Uhlmann Transformation Problem. The unitary complexity classes we define can be parameterized by an error parameter δ . For example, unitaryBQP_δ denotes the set of unitary synthesis problems where the transformation can be implemented up to error δ on all input states; when the error parameter is not specified we assume that the transformation can be implemented with any error that is an arbitrarily small inverse polynomial. It is clear that if $\mathcal{U} \in \text{unitaryBQP}_\delta$, then $\mathcal{U} \in \text{unitaryBQP}_\eta$ for all $\eta \geq \delta$ (i.e., problems cannot get any harder if we are allowed to incur larger error).

Although we do not expect UHLMANN to be solvable in polynomial time, we show that *if* Uhlmann transformations can generally be efficiently implemented with large error (even with error approaching 1), then they can be efficiently implemented with arbitrarily small inverse polynomial error. We prove this by analysing parallel repetitions of instances of the Uhlmann transformation problem using ideas inspired by “quantum rewinding” techniques from quantum cryptography [Wat06]. Written in terms of unitary classes, we have:

Theorem 1.3 (Informal). *Let ϵ be negligibly small. Then $\text{UHLMANN}_{1-\epsilon} \in \text{avgUnitaryBQP}$ if and only if $\text{UHLMANN}_{1-\epsilon} \in \text{avgUnitaryBQP}_{1-\xi}$ where $\xi(n) = n^{-1/16}$. Here, n refers to the number of qubits of the UHLMANN instance.*

This is formally stated and proved as [Theorem 6.8](#). In other words, being able to solve UHLMANN (with the guarantee that the fidelity between the reduced states is negligibly close to 1) with very large error is no easier (up to polynomial factors) than solving it with very small error. We prove the more interesting direction (that $\text{UHLMANN} \in \text{avgUnitaryBQP}_{1-\xi}$ implies that $\text{UHLMANN} \in \text{avgUnitaryBQP}$) as follows: given an instance $(|C\rangle, |D\rangle)$ of UHLMANN for which it is hard to implement the corresponding Uhlmann transformation U with error δ , we show that it is hard to implement the Uhlmann transformation $U^{\otimes k}$ for the k -fold repetition $(|C\rangle^{\otimes k}, |D\rangle^{\otimes k})$ even with error $1 - \frac{1}{\delta k^2}$. The proof uses ideas inspired by “quantum rewinding” techniques from quantum cryptography [Wat06].

A natural question is whether one can prove a *strong* hardness amplification result, where one shows that hardness of an Uhlmann transformation U implies the hardness of implementing the

repeated transformation $U^{\otimes k}$ with error $1 - \exp(-\Omega(k))$. Strong hardness amplification results are known in classical complexity theory and cryptography [Raz98, Hai09, HPWP10]; we conjecture that an analogous result holds for the Uhlmann Transformation Problem.

Conjecture 1.4. *Let ϵ be negligibly small. Then $\text{UHLMANN}_{1-\epsilon} \in \text{avgUnitaryBQP}$ if and only if $\text{UHLMANN}_{1-\epsilon} \in \text{avgUnitaryBQP}_{1-\exp(-\Omega(n))}$.*

Our hardness amplification result for the Uhlmann Transformation Problem immediately implies hardness amplification for quantum commitments, which answers an open question of Yan [Yan22]. We give more details when discussing the applications to quantum cryptography later in this introduction and in Section 8.

The succinct Uhlmann Transformation Problem. We also define a *succinct* version of the Uhlmann Transformation Problem (denoted by 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 1.5 (Informal). *SUCCINCTUHLMANN is complete for avgUnitaryPSPACE under polynomial-time reductions.*

This is formally stated and proved as Theorem 7.12. 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 $\text{SUCCINCTUHLMANN} \in \text{avgUnitaryPSPACE}$ 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 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 $|\omega_x\rangle$ representing the distribution to $(\text{id} \otimes U_x)|\omega_x\rangle$. This is nothing but an instance of the SUCCINCTUHLMANN transformation problem. We refer to the proof of Theorem 7.12 for details.

We then show another completeness result for SUCCINCTUHLMANN :

Theorem 1.6 (Informal). *SUCCINCTUHLMANN is complete for avgUnitaryQIP under polynomial-time reductions.*

This is formally stated and proved as Theorem 7.6. Here, the class avgUnitaryQIP is like $\text{avgUnitarySZK}_{\text{HV}}$ except there is no requirement that the protocol between the honest verifier and prover can be efficiently simulated. The proof starts similarly to the proof of the $\text{avgUnitarySZK}_{\text{HV}}$ -completeness of UHLMANN , but requires additional ingredients, such as the state synthesis protocol of [RY22] and the density matrix exponentiation algorithm of [LMR14]. Putting together Theorems 1.5 and 1.6 we get the following unitary complexity analogue of the $\text{QIP} = \text{PSPACE}$ theorem [JJUW11] and the $\text{stateQIP} = \text{statePSPACE}$ theorem [RY22, MY23]:

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

Corollary 1.7. $\text{avgUnitaryQIP} = \text{avgUnitaryPSPACE}$.

This partially answers an open question of [RY22, MY23], who asked whether $\text{unitaryQIP} = \text{unitaryPSPACE}$ (although they did not formalize this question to the same level as we do here). Using the Uhlmann Transformation Problem as a complete problem, we resolve this question in the average case, and leave it as an interesting open question to prove the same statement for the worst-case complexity classes unitaryPSPACE and unitaryQIP .

We can also relate the traditional decision complexity class PSPACE to the unitary synthesis problem SUCCINCTUHLMANN with the following theorem.

Theorem 1.8. $\text{PSPACE} \subseteq \text{BQP}^{\text{SUCCINCTUHLMANN}}$.

This is formally proved as [Theorem 7.15](#). In other words, all languages in PSPACE can be decided by a quantum polynomial time algorithm that can query an oracle that solves SUCCINCTUHLMANN . Since it is believed that $\text{PSPACE} \not\subseteq \text{BQP}$, this gives evidence from “traditional” complexity theory that SUCCINCTUHLMANN is a very difficult unitary synthesis problem. Our proof of this relies on the random self-reducibility of PSPACE -complete languages [FF93].

We note that it is an interesting question whether the “converse” direction holds: can SUCCINCTUHLMANN be synthesized in polynomial time given oracle access to the decision class PSPACE ? We conjecture that the answer is “no”, and that in general a given unitary complexity class is much harder than its corresponding decision class.

1.3 Centrality of the Uhlmann Transformation Problem

We now 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 *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.

1.3.1 Quantum cryptography applications

We begin by exploring connections between the Uhlmann Transformation Problem and several concepts in quantum cryptography.

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, MY22b, KQST23] or EFI pairs [BCQ23].

In an in-depth study of the properties of quantum commitment schemes, Yan [Yan22] suggested connecting the hardness of Uhlmann transformations to the existence of quantum commitments. We formalize this connection within the unitary complexity framework and show the following:

Theorem 1.9 (Informal). *If $\text{UHLMANN}_{1-\epsilon} \in \text{avgUnitaryBQP}$ for all negligible ϵ , then quantum commitments do not exist. On the other hand, if $\text{UHLMANN}_{1-\epsilon} \notin \text{avgUnitaryBQP}$ for some negligible ϵ , and furthermore hard instances of $\text{UHLMANN}_{1-\epsilon}$ can be uniformly and efficiently generated, then quantum commitments with strong statistical hiding and weak computational binding exist.*

Here, *strong statistical hiding* means that no adversary (even a computationally unbounded one) can distinguish commitments to $b = 0$ from commitments to $b = 1$ with more than negligible advantage, and *weak computational binding* means that no computationally bounded adversary can swap the committed bit with fidelity greater than $1 - 1/p(\lambda)$ for some polynomial $p(\lambda)$ in the security parameter. This theorem is formally stated and proved as [Theorem 8.10](#).

We also show that the proof of hardness amplification for the Uhlmann Transformation Problem ([Theorem 1.3](#)) can be used to amplify the security of the binding property of quantum commitments: roughly speaking, if there is a commitment scheme where it is hard for a malicious sender to transform the 0-commitment to have fidelity more than $1 - 1/p(\lambda)$ with the 1-commitment for some polynomial $p(\lambda)$, then there exists another commitment scheme where it is hard for an adversary to transform the 0-commitment to have more than $\frac{1}{q(\lambda)}$ overlap with the 1-commitment for all polynomials $q(\lambda)$. This answers an open question of Yan [Yan22], who asked whether hardness amplification for commitments is possible.

Theorem 1.10 (Informal). *Quantum commitments with strong statistical hiding and weak computational binding exist if and only if quantum commitments with strong statistical hiding and $1/q(\lambda)$ -computational binding exist for all $q(\lambda)$.*

This theorem is formally stated and proved as [Theorem 8.8](#). Furthermore, since we can generically perform *flavor switching* of quantum commitments (i.e. swap which security property holds statistically and which computationally) [HMY23, GJMZ23, Yan22], both [Theorems 1.9](#) and [1.10](#) can be extended to quantum commitments with computational hiding and statistical binding.

Assuming [Conjecture 1.4](#) about strong amplification for the Uhlmann Transformation Problem, we also obtain a stronger statement, which is that if $\text{UHLMANN}_{1-\epsilon} \notin \text{avgUnitaryBQP}$ for some negligibly small ϵ and hard instances can be uniformly and efficiently generated, then quantum commitments with strong hiding and strong binding properties exist (whereas [Theorem 1.9](#) only guarantees commitments with weak binding). These strong commitments are in turn equivalent to a number of quantum cryptographic primitives, such as EFI pairs [BCQ23], oblivious transfer [BCQ23], (secretly-verifiable and statistically-invertible) one-way state generators [MY22a], and secure quantum multi-party quantum computation scheme for any classical functionality [BCQ23, AQY22].

Breaking unclonable state generators. We consider the cryptographic notion of *unclonable state generators*, which is an efficiently computable map from a classical key k to a quantum state

$|\phi_k\rangle$ that is intractable to clone (without the classical key). This abstractly captures the security of unclonable cryptographic primitives like quantum money [Wie83, AC12] or quantum copy-protection [ALL⁺21, CLLZ21]. We show the following relation between unclonable state generators and UHLMANN (stated formally as [Theorem 8.18](#)):

Theorem 1.11 (Informal). *A real-valued, clean-output unclonable state generator is either information-theoretically secure, or the task of cloning its output can be efficiently reduced to UHLMANN $_{\kappa}$ for $\kappa = 1/\text{poly}(n)$.*

Being *real-valued* means that the output state of the one-way state generator is represented as a real vector. The *clean-output* property means that the one-way state generator, on input key k , only outputs $|\phi_k\rangle$ and no other residual state depending on k . We argue in [Section 8.2](#) that most existing constructions of unclonable state generators are real-valued and clean-output.

Note that this theorem uses a regime where $\kappa \ll 1$. This marks our first application of UHLMANN $_{\kappa}$ for small κ ; most of the applications in this paper are connected to UHLMANN $_{1-\epsilon}$ for a negligible function $\epsilon(n)$. The class UHLMANN $_{\kappa}$ for small κ is at least as hard as UHLMANN $_{1-\epsilon}$, and *a priori* it could be harder.

Remark 1.12. Recent work of Khurana and Tomer [KT23] shows that breaking *one-way state generators* (OWSGs) with $t(\lambda)$ -copy security can be efficiently reduced to UHLMANN $_{1-\text{negl}}$, provided that $t(\lambda)$ is a sufficiently large polynomial. One-way state generators and unclonable state generators are closely related, but have different security properties. We elaborate on the comparison between OWSGs and unclonable state generators in [Section 8.2](#).

Breaking falsifiable quantum cryptographic assumptions. Finally, 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 8.21](#) for the formal statement):

Theorem 1.13 (Informal). *A falsifiable quantum cryptographic assumption is either information-theoretically secure, or the task of breaking security reduces to SUCCINCTUHLMANN.*

Since SUCCINCTUHLMANN is complete for avgUnitaryPSPACE ([Theorem 1.5](#)), this means that avgUnitaryBQP \neq 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, MY22b, 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 [Wil13, 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. 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.

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 $\mathcal{D}_{B \rightarrow A'}(\mathcal{N}_{A \rightarrow B}(\Phi_{AR})) \approx \Phi_{A'R}$, where $|\Phi\rangle_{AR}$ 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 $(\mathcal{N} \otimes \text{id})(\Phi_{AR})$, decode and output a register $A' \equiv A$ such that the final joint state of $A'R$ 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 provide a precise characterisation of the complexity of the Decodable Channel Problem:

Theorem 1.14 (Informal). *The Decodable Channel Problem can be solved in polynomial-time if and only if $\text{UHLMANN} \in \text{avgUnitaryBQP}$.*

This theorem is formally stated and proved as [Theorem 9.6](#); since we do not expect that $\text{UHLMANN} \in \text{avgUnitaryBQP}$, this suggests that the Decodable Channel Problem is hard to solve 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*⁷ \mathcal{N}^c , when given register A of the maximally entangled state $|\Phi\rangle_{AR}$, 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 $\text{UHLMANN} \in \text{avgUnitaryBQP}$, 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 strong statistical hiding and weak computational binding quantum commitments. 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

⁷The 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.

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 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 1.15 (Informal). *Quantum states can be optimally compressed to their smoothed max entropy in polynomial-time if $\text{UHLMANN}_{1-\epsilon} \in \text{avgUnitaryBQP}$ 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 9.15](#) and [9.17](#). The upper bound (i.e., compression is easy if UHLMANN is easy) is proved using a powerful technique in quantum information theory known as *decoupling* [Dup10]. 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 Theoretical physics applications

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 two computational tasks arising from this research.

First, 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 $|\psi\rangle_{\text{BHR}}$ 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 $|\text{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ 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 $\text{SZK} \not\subseteq \text{BQP}$. 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 $\text{UHLMANN} \in \text{avgUnitaryBQP}$.

Secondly, we consider the complexity of detecting interference between orthogonal states (i.e. distinguish $(|\psi\rangle + |\varphi\rangle)/\sqrt{2}$ from $(|\psi\rangle - |\varphi\rangle)/\sqrt{2}$), which was recently studied in the context of physically detecting interference between superpositions of spacetime geometries in the AdS/CFT correspondence in [AAS20]. We show that a suitably formalised version of this task polynomial-time reduces to SUCCINCTUHLMANN .

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 lay the foundations for a rich theory of the complexity of “fully quantum” problems. A lot of questions in this direction are completely unexplored. 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 indispensable 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 [MY22b] 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 Kolmogorov 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, AA23]. 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 $P = PSPACE$ does not imply $\text{unitaryBQP} = \text{unitaryPSPACE}$? One would likely have to show this in a *relativized* setting, i.e., exhibit an oracle O relative to which $P^O = PSPACE^O$ but $\text{unitaryBQP}^O \neq \text{unitaryPSPACE}^O$. 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 (Section 4) and the hardness amplification result (Section 6.2).
- **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, and Renato Renner for helpful discussions. We thank Fred Dupuis for his help with understanding

the decoupling results in his thesis. We also thank Tomoyuki Morimae for their helpful comments on a preliminary version of this work. 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 $\delta : \mathbb{N} \rightarrow [0, 1]$ is an *inverse polynomial* if $\delta(n) \leq 1/p(n)$ for all sufficiently large n . A function $\epsilon : \mathbb{N} \rightarrow [0, 1]$ is *negligible* if for every polynomial $p(n)$, for all sufficiently large n we have $\epsilon(n) \leq 1/p(n)$.

A *register* R is a named finite-dimensional complex Hilbert space. If A, B, 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 $\text{Tr}(\cdot)$ to denote trace, and $\text{Tr}_R(\cdot)$ to denote the partial trace over a register R .

We denote the set of linear transformations on R by $L(R)$, and linear transformations from R to another register S by $L(R, S)$. We denote the set of positive semidefinite operators on a register R by $\text{Pos}(R)$. The set of density matrices on R is denoted $S(R)$. 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 $X \in L(R)$, we define $\|X\|_\infty$ to be its operator norm, and $\|X\|_1 = \text{Tr}(|X|)$ to denote its trace norm, where $|X| = \sqrt{X^\dagger X}$. We write $\text{td}(\rho, \sigma) = \frac{1}{2}\|\rho - \sigma\|_1$ to denote the trace distance between two density matrices ρ, σ , and $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$ for the fidelity between ρ, σ .⁸ 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*

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

A *quantum channel* from register A to B is a completely positive trace-preserving (CPTP) map from $L(A)$ to $L(B)$. For simplicity, we often write $\mathcal{N} : A \rightarrow B$ instead of $\mathcal{N} : L(A) \rightarrow L(B)$ when it is clear that \mathcal{N} is a channel. We denote the set of quantum channels as $\text{CPTP}(A, B)$. We also call a channel a *superoperator*. For a channel Φ , we write $\text{supp}(\Phi)$ to denote the number of qubits it takes as input. We call a channel unitary (isometric) if it conjugates its input state with a unitary (isometry).

⁸We note that in the literature there are two versions of fidelity that are commonly used; here we use the *squared* version of it.

The diamond norm of a channel $\Phi \in \text{CPTP}(\mathbf{A}, \mathbf{B})$ is defined as $\|\Phi\|_\diamond = \max_\rho \|(\Phi \otimes \text{id}_{\mathbf{C}})(\rho)\|_1$ where the maximization is over all density matrices $\rho \in \mathbf{S}(\mathbf{A} \otimes \mathbf{C})$ where \mathbf{C} is an arbitrary register.

Another important type of quantum operation that can be performed on a quantum state is a *measurement*. In general a quantum measurement is described by a finite set of positive semidefinite matrices $\mathcal{M} = \{M_i\}_i$ satisfying $\sum_i M_i = \text{id}$. Performing a measurement on a state ρ results in an *output* i , where each i occurs with probability $\text{Tr}[M_i\rho]$, and conditioned on the outcome being i , the resulting state is

$$\rho|_{M_i} = \frac{\sqrt{M_i}\rho\sqrt{M_i}}{\text{Tr}(M_i\rho)}. \quad (2.1)$$

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.

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

A proof of this can be found in, e.g., [Wil13, 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 $U \in \mathbf{L}(\mathbf{A}, \mathbf{B})$ is called a partial isometry if there exists a projector $\Pi \in \mathbf{L}(\mathbf{A})$ and an isometry $\tilde{U} \in \mathbf{L}(\mathbf{A}, \mathbf{B})$ 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: 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 $U \in \mathbf{L}(\mathbf{A}, \mathbf{B})$ be a partial isometry. A channel completion of U is a quantum channel $\Phi \in \text{CPTP}(\mathbf{A}, \mathbf{B})$ such that for any input state $\rho \in \mathbf{S}(\mathbf{A})$,*

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

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

2.3 Quantum circuits

For convenience we assume that all quantum circuits use gates from the universal gate set $\{H, CNOT, T\}$ [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 uses space s if the total number of qubits involved at any 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 $C|0\dots 0\rangle$.

Definition 2.5 (Polynomial size and space circuit families). *We say that $(C_x)_{x \in \{0,1\}^*}$ is a family of polynomial-size general quantum circuits if there exists a polynomial p such that C_x has size (i.e. number of gates) at most $p(|x|)$. We say that $(C_x)_{x \in \{0,1\}^*}$ is a family of polynomial-space general quantum circuits if there exists a polynomial p such that C_x uses at most $p(|x|)$ space.*

Definition 2.6 (Uniform circuit families). *A family of general quantum circuits $(C_x)_{x \in \{0,1\}^*}$ is called time-uniform (or simply uniform) if $(C_x)_{x \in \{0,1\}^*}$ is polynomial-size and there exists a classical polynomial-time Turing machine that on input x outputs the description of C_x . Similarly, a family of general quantum circuits $(C_x)_{x \in \{0,1\}^*}$ is called space-uniform if $(C_x)_{x \in \{0,1\}^*}$ is polynomial-space and there exists a classical polynomial-space Turing machine that on input (x, i) outputs the i 'th gate of C_x . For brevity, we also call a time-uniform (resp. space-uniform) family of quantum circuits a polynomial time (resp. polynomial space) quantum algorithm.*

Definition 2.7 (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 2.8. *Let C be a size- m general quantum circuit acting on n qubits, and let \tilde{C} be its unitary purification where 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 ,*

$$C(\rho) = \text{Tr}_R(\tilde{C} \rho \tilde{C}^\dagger).$$

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

2.4 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 2.9 (stateBQP, statePSPACE). Let $\delta : \mathbb{N} \rightarrow [0, 1]$ be a function. Then stateBQP_δ (resp. $\text{statePSPACE}_\delta$) is the class of all sequences of density matrices $(\rho_x)_{x \in \{0,1\}^*}$ such that each ρ_x is a state on $\text{poly}(|x|)$ qubits, and there exists a time-uniform (resp. space-uniform) family of general quantum circuits $(C_x)_{x \in \{0,1\}^*}$ such that for all $x \in \{0,1\}^*$ with sufficiently large length $|x|$, the circuit C_x takes no inputs and C_x outputs a density matrix σ_x such that

$$\text{td}(\sigma_x, \rho_x) \leq \delta(|x|).$$

We define

$$\text{stateBQP} = \bigcap_q \text{stateBQP}_{1/q(n)} \quad \text{and} \quad \text{statePSPACE} = \bigcap_q \text{statePSPACE}_{1/q(n)}$$

where the intersection is over all polynomials $q : \mathbb{N} \rightarrow \mathbb{R}$.

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.

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 $\mathcal{U} = (U_x)_{x \in \{0,1\}^*}$ of partial isometries.*⁹

One should think of $x \in \{0,1\}^*$ as an encoding of the particular partial isometry in the sequence \mathcal{U} . The precise form of this encoding can differ between unitary synthesis problems. Some examples of encodings include: x describes a polynomial-length sequence of quantum gates; or x describes a classical circuit that, on input i , outputs the i -th gate of a (potentially exponentially long) quantum circuit implementing a unitary. We call the latter a *succinct description* of the unitary.

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 $\Pi_x = \text{id}$). A partial isometry is only required to be unitary on some subspace, and does not specify any action on the orthogonal complement of the subspace. This is analogous to the idea of a “promise” on the inputs in standard complexity theory: the unitary synthesis problem includes a “promised subspace” on which all input states to that unitary are supposed to lie; if an input state has support on the orthogonal complement to this subspace, the behaviour is not specified by the unitary synthesis problem.

Examples. We present some examples of unitary synthesis problems.

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 $U_x = 0$. Then we define $\text{TIMEEVOLUTION} = (U_x)_{x \in \{0,1\}^*}$.
2. (*Decision languages*) Let $L \subseteq \{0,1\}^*$ be a decision language. Define $\text{UNITARYDECIDER}_L = (U_x)_{x \in \{0,1\}^*}$ as follows: interpreting x as the binary representation of an integer $n \in \mathbb{N}$, the unitary U_n acts on $n + 1$ qubits and for all $y \in \{0,1\}^n, b \in \{0,1\}$, we define $U_n |y\rangle |b\rangle = |y\rangle |b \oplus L(y)\rangle$ where $L(y) = 1$ iff $y \in L$. In other words, the unitary U_n coherently decides whether $y \in L$ or not.

⁹We 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”.

3. (*State preparation*) Let $(|\psi_x\rangle)_{x \in \{0,1\}^*}$ be a family of states where $|\psi_x\rangle$ is on n_x qubits. Then the partial isometries $U_x = |\psi_x\rangle\langle 0^{n_x}|$ form a unitary synthesis problem. In other words, these partial isometries map the zero state to $|\psi_x\rangle$.

We now define what it means to *implement* a unitary synthesis problem. Intuitively, an implementation of a unitary synthesis problem is just a sequence of (not necessarily unitary) quantum circuits that implement the corresponding partial isometries. The only subtlety is that a quantum circuit is trace-preserving on all inputs, so it cannot map states in the orthogonal complement of the support of the partial isometry to 0. Therefore, we require that the quantum circuit implements any channel completion of the partial isometry (Definition 2.4). 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, instead of being e.g. required to abort.

Definition 3.2 (Worst-case implementation of unitary synthesis problems). *Let $\mathcal{U} = (U_x)_{x \in \{0,1\}^*}$ denote a unitary synthesis problem and $\delta : \mathbb{N} \rightarrow \mathbb{R}$ a function. Let $C = (C_x)_{x \in \{0,1\}^*}$ denote a (not necessarily uniform) family of quantum circuits, where C_x implements a channel whose input and output registers are the same as those of U_x . We say that C implements \mathcal{U} with **worst-case error** δ if for all $x \in \{0,1\}^*$, there exists a channel completion Φ_x of U_x such that*

$$\left\| C_x - \Phi_x \right\|_{\diamond} \leq \delta(|x|),$$

where $\|\cdot\|_{\diamond}$ denotes the diamond norm.

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.

Remark 3.3. For a unitary synthesis problem $\mathcal{U} = (U_x)_{x \in \{0,1\}^*}$ we call x an *instance*, and U_x the transformation of \mathcal{U} corresponding to instance x . We call the register that U_x or its implementation C_x acts on the *quantum input* to the unitary synthesis problem.

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 to act; note, however, that this is very different from a state synthesis problem, as we discuss in Remark 3.12. We first give the formal definition and then explain why this is a reasonable notion of a distributional unitary synthesis problem.

Definition 3.4 (Distributional unitary synthesis problem). *We say that a pair (\mathcal{U}, Ψ) is a distributional unitary synthesis problem if $\mathcal{U} = (U_x)_x$ is a unitary synthesis problem with $U_x \in \mathcal{L}(\mathbf{A}_x, \mathbf{B}_x)$ for some registers $\mathbf{A}_x, \mathbf{B}_x$, and $\Psi = (|\psi_x\rangle)_x$ is a family of bipartite pure states on registers $\mathbf{A}_x \mathbf{R}_x$. We call $|\psi_x\rangle$ the distribution state with target register \mathbf{A}_x and ancilla register \mathbf{R}_x .*

Definition 3.5 (Average-case implementation of distributional unitary synthesis problems). *Let (\mathcal{U}, Ψ) denote a distributional unitary synthesis problem, where $\mathcal{U} = (U_x)_x$ and $\Psi = (|\psi_x\rangle)_x$, and let $\delta : \mathbb{N} \rightarrow \mathbb{R}$ be a function. Let $C = (C_x)_x$ denote a family of quantum circuits, where C_x implements a channel whose input and output registers are the same as those of U_x . We say that C implements (\mathcal{U}, Ψ) with **average-case error** δ if for all $x \in \{0,1\}^*$, there exists a channel completion Φ_x of U_x such that*

$$\text{td}\left((C_x \otimes \text{id})(\psi_x), (\Phi_x \otimes \text{id})(\psi_x)\right) \leq \delta(|x|),$$

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

The term “distributional” may seem a bit odd at first; for example, where is the distribution in [Definition 3.4](#)? 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 (\mathcal{U}, Ψ) can be viewed as a *purification* of a distribution over pure states: by the Schmidt decomposition, we can always write

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

for orthonormal states $\{|\phi_{x,j}\rangle\}_j$ on \mathbf{A}_x and $\{|j\rangle\}_j$ on \mathbf{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 (\mathcal{U}, Ψ) with average-case error δ is equivalent to the following: for all $x \in \{0, 1\}^*$ there exists a channel completion Φ_x of U_x such that

$$\mathbb{E}_{j \sim \mathcal{D}_x} \text{td}(C_x(\phi_{x,j}), \Phi_x(\phi_{x,j})) \leq \delta(|x|). \quad (3.2)$$

Conversely, any distribution over pure states can be purified into a state of the form [Equation \(3.1\)](#), so the condition in [Equation \(3.2\)](#) is equivalent to [Definition 3.5](#). We will find it more convenient to simply specify (for each x) one pure state $|\psi_x\rangle_{\mathbf{A}_x \mathbf{R}_x}$ instead of a set of pure states on \mathbf{A}_x and a distribution over them.

One might also wonder about specifying a distribution over the strings x that label the partial isometries U_x . However this can be “folded” into the state distribution by consider a larger unitary U_n that takes as input $|x\rangle \otimes |\psi\rangle$.

Remark 3.6. Comparing [Definition 3.2](#) and [Definition 3.5](#), we see that we can also define the worst-case error in terms of the average-case error: a circuit family $C = (C_x)_{x \in \{0,1\}^*}$ implements a unitary synthesis problem $\mathcal{U} = (U_x)_{x \in \{0,1\}^*}$ with worst case error δ if and only if it implements the distributional unitary synthesis problem (\mathcal{U}, Ψ) with average-case error δ for all state sequences $\Psi = (|\psi_x\rangle)_x$.

3.2 Unitary complexity classes

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

Definition 3.7 (unitaryBQP, unitaryPSPACE). *Let $\delta : \mathbb{N} \rightarrow \mathbb{R}$ be a function. Define the unitary complexity class unitaryBQP_δ (resp. $\text{unitaryPSPACE}_\delta$) to be the set of unitary synthesis problems $\mathcal{U} = (U_x)_x$ for which there exists a uniform polynomial-time (resp. polynomial-space) quantum algorithm C that implements \mathcal{U} with worst-case error δ . We define unitaryBQP (resp. unitaryPSPACE) to be the intersection of $\text{unitaryBQP}_{1/q(n)}$ (resp. $\text{unitaryPSPACE}_{1/q(n)}$) over all polynomials $q(n)$.*

A natural question about unitary complexity classes such unitaryBQP_δ and $\text{unitaryPSPACE}_\delta$ is whether the error δ can be generically reduced, in analogy to how the completeness/soundness errors can be generically reduced in randomized complexity classes like BPP or BQP. In particular, is it true that $\text{unitaryBQP}_{1/3}$ is the same as $\text{unitaryBQP}_{n^{-1}}$ or even $\text{unitaryBQP}_{\exp(-n)}$? We first present a simple argument for why error reduction for unitary synthesis classes is not possible in general.

Proposition 3.8 (Impossibility of error reduction for unitary synthesis problems). *Let α, β be such that $0 < \alpha < \beta < 1$ and $\beta > 2\sqrt{3\alpha}$. Then $\text{unitaryBQP}_\alpha \neq \text{unitaryBQP}_\beta$.*

Proof. Define $\mathcal{U} = (U_x)_{x \in \{0,1\}^*}$ as follows. If x is the description of a Turing machine that halts on the empty input, then U_x is the single-qubit unitary $\begin{pmatrix} \sqrt{1-3\alpha} & -\sqrt{3\alpha} \\ \sqrt{3\alpha} & \sqrt{1-3\alpha} \end{pmatrix}$. Otherwise, U_x is the identity matrix on a single qubit. It is clear that $\mathcal{U} \in \text{unitaryBQP}_\beta$: this is because in the case that x represents a halting Turing machine, the identity matrix approximates U_x in diamond norm with error $2\sqrt{3\alpha} < \beta$.

On the other hand, $\mathcal{U} \notin \text{unitaryBQP}_\alpha$. Suppose for contradiction there was a uniform quantum algorithm $C = (C_x)_x$ that implements \mathcal{U} with worst-case error α . Then we can use C to decide the Halting Problem as follows. Given an input x , repeatedly run the circuit C_x on $|0\rangle$, and then measure in the standard basis. Since C_x implements U_x with worst-case error α , this means that if x represents a halting Turing machine, then each trial results in $|1\rangle$ with probability at least $3\alpha - \alpha \geq 2\alpha$, and if x represents a non-halting Turing machine, then each trial results in $|1\rangle$ with probability at most α . Since α is constant, after a constant number of trials one can distinguish with high confidence whether x represents a halting Turing machine or not. Thus this implies the Halting problem can be decided by a quantum algorithm in polynomial time, which is a contradiction. \square

Remark 3.9. It is interesting that a simple argument can prove separations between unitary complexity classes, whereas in contrast it is much harder to prove analogous separations between traditional complexity classes. For example, it remains unknown whether $\text{BPP} \neq \text{BQP}$. However we also point out that this has nothing to do with the fact that we're dealing with quantum complexity classes; one could also prove similar separations between *classical sampling complexity classes* (see, e.g., [Aar14]).

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

Definition 3.10 (avgUnitaryBQP , avgUnitaryPSPACE). *Let $\delta : \mathbb{N} \rightarrow \mathbb{R}$ be a function. Define the unitary complexity class $\text{avgUnitaryBQP}_\delta$ (resp. $\text{avgUnitaryPSPACE}_\delta$) to be the set of distributional unitary synthesis problems $(\mathcal{U} = (U_x)_x, \Psi = (|\psi\rangle_x)_x)$ where $\Psi \in \text{stateBQP}$ (resp. $\Psi \in \text{statePSPACE}$) and there exists a uniform polynomial-time (resp. polynomial-space) quantum algorithm C that implements (\mathcal{U}, Ψ) with average-case error δ . We define avgUnitaryBQP (resp. avgUnitaryPSPACE) to be the intersection of $\text{avgUnitaryBQP}_{1/q(n)}$ (resp. $\text{avgUnitaryPSPACE}_{1/q(n)}$) over all polynomials $q(n)$.*

Remark 3.11. In our definition of avgUnitaryBQP and 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. stateBQP and 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 4.2). This is in analogy to classical average case complexity classes, where it is common to require that the distribution over which the problem is defined can be sampled from with reasonable complexity. As we will see e.g. in Theorem 7.12, this assumption will be necessary to prove several natural results about average unitary complexity.

Remark 3.12. 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 just a complicated way of stating the state synthesis problem for the state $U_x|\psi_x\rangle$. This, however, is not the case: the state $|\psi_x\rangle$ is defined on register A_xR_x , but the unitary U_x is only allowed to act on A_x . Therefore, if we imagine that we hand a unitary synthesis problem to some black box to implement, we should imagine that we provide as input the string x as well as register A_x of $|\psi_x\rangle$. With sufficient computational resources, the black box can of course synthesise many more copies of $|\psi_x\rangle$ because the state is in the corresponding state complexity class. However, to solve the unitary synthesis problem, it has to apply the unitary on register A_x of the state that we provided as input, not any other copy of $|\psi_x\rangle$ it created itself. This is because otherwise the output state would not be entangled with our register R_x (which the black box does not have access to) in the correct way. This has the important consequence that in contrast to state synthesis problems, in average unitary synthesis problems the black box cannot re-run the synthesis algorithm many times and post-select on success, as it is only provided with a single copy of a register of the input state $|\psi_x\rangle$. We therefore see that solving an average-case unitary synthesis problem $(\mathcal{U} = (U_x)_x, \Psi = (|\psi_x\rangle)_x)$ is potentially much harder than the state synthesis problem for the sequence $\Psi' := (U_x|\psi_x\rangle)_x$. Conversely, if we can show that (\mathcal{U}, Ψ) is in some average unitary complexity class, it immediately follows that the state synthesis problem Ψ' is in the corresponding state complexity class.

Non-uniform unitary synthesis classes. The classes `unitaryBQP` and `unitaryPSPACE` are *uniform* complexity classes in the sense that a unitary synthesis problem $\mathcal{U} = (U_x)_x$ in either class must be implemented by a *uniform* quantum algorithm, i.e. a collection of circuits $C = (C_x)_x$ that are uniformly generated by a single (classical) Turing machine.

However one can also consider *nonuniform* variants of these classes, where the circuits C_x are not required to be uniformly generated by a Turing machine. These are analogous to nonuniform complexity classes like `P/poly` in classical complexity theory, but there is one key difference: the implementation algorithm can have a different circuit for each instance x , whereas the definition of `P/poly` only allows the circuit to depend on the *input length*. If the circuits in the definition of `P/poly` could depend on the instance, then all languages would trivially be in `P/poly`: the circuit could just output 1 or 0 depending on whether the instance were in the language.

As we will see in [Section 8](#), this notion of nonuniformity allows us to establish a tight connection between the (non-uniform) complexity of unitary synthesis problems and the hardness of breaking various quantum cryptographic primitives.

Definition 3.13 (`unitaryBQP/poly`). *Let $\delta : \mathbb{N} \rightarrow \mathbb{R}$ be a function. Define the unitary complexity class `unitaryBQP/poly $_\delta$` to be the set of unitary synthesis problems $\mathcal{U} = (U_x)_x$ for which there exists a non-uniform polynomial-size family of quantum algorithms C_x that implements \mathcal{U} with worst-case error δ . We define `unitaryBQP/poly` to be the intersection of `unitaryBQP/poly $_{1/q(n)}$` for all polynomials $q(n)$.*

We also define an nonuniform variant of `avgUnitaryBQP`.

Definition 3.14 (`avgUnitaryBQP/poly`). *Let $\delta : \mathbb{N} \rightarrow \mathbb{R}$ be a function. Define the unitary complexity class `avgUnitaryBQP/poly $_\delta$` to be the set of distributional unitary synthesis problems $(\mathcal{U} = (U_x)_x, \Psi = (|\psi_x\rangle)_x)$ where $\Psi \in \text{stateBQP}$ and there exists a non-uniform polynomial-size family of quantum circuits $(C_x)_x$ that implements (\mathcal{U}, Ψ) with average-case error δ . We define `avgUnitaryBQP/poly` to be the intersection of `avgUnitaryBQP/poly $_{1/q(n)}$` for all polynomials $q(n)$.*

One can also define non-uniform versions of these classes with *quantum* advice, e.g., unitaryBQP/qpoly, but we leave that for future work.

3.3 Reductions

Notions of reductions are crucial in complexity theory and theoretical computer science. We introduce a basic notion of reduction that allows one 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 3.15 (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 $y \in \{0,1\}^*$; 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.*

Section 3.3 depicts an example of a quantum query circuit.

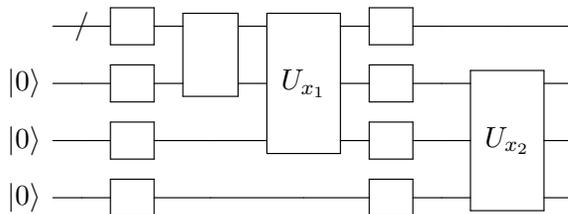


Figure 1: An example of a quantum query circuit that calls members of a unitary synthesis problem \mathcal{U} ; the subscripts x_1, x_2 denote instances that are hardcoded in the query circuit.

Definition 3.16 (Instantiations of quantum query circuits). *An instantiation of a quantum query circuit C^* with a unitary synthesis problem $\mathcal{U} = (U_x)$, denoted $C^{\mathcal{U}}$, is a quantum channel obtained from C^* by replacing all the oracle gates with label y by some channel completion of U_y (which can be different each time U_y is called). Whenever we write $C^{\mathcal{U}}$, we implicitly require that \mathcal{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 in C^* .*

Definition 3.17 (Uniformity of quantum query circuits). *We say that a family $(C_x^*)_x$ of quantum query circuits is time-uniform (resp. space-uniform) if there exists a classical polynomial time (resp. polynomial space) Turing machine that on input x outputs a description of C_x and furthermore all labels y in an oracle gate in C_x^* satisfy $|y| = \text{poly}(|x|)$. For brevity, we also call a time-uniform (resp. space-uniform) family of quantum query circuits a polynomial time (resp. polynomial space) quantum query algorithm. If $C^* = (C_x^*)_x$ is a quantum query algorithm, then we write $C^{\mathcal{Y}}$ to denote a family of instantiations $(C_x^{\mathcal{Y}})_x$. Just like for individual query circuits, for families of query circuits we call $C^{\mathcal{Y}}$ an instantiation of C^* .*

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.¹⁰ To accommodate situations when the oracle circuit may want to query different oracles $\mathcal{U} = (U_x)_x$ (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.

We also note that the instantiation $C^\mathcal{V}$ is not unique because the oracle gates can implement any channel completion of the partial isometries $V_x \in \mathcal{V}$. Whenever we say that a statement holds for $C^\mathcal{V}$, we mean that it holds for all possible instantiations, i.e. for all possible choices of channel completions.

Using quantum query circuits, we can define reductions between unitary synthesis problems.

Definition 3.18 (Reductions between unitary synthesis problems). *Let $\mathcal{U} = (U_x)_x$ and $\mathcal{V} = (V_x)_x$ denote unitary synthesis problems. Then \mathcal{U} (polynomial-time) reduces to \mathcal{V} if for all polynomials $q(n)$ there exists a polynomial-time quantum query algorithm C^* such all instantiations $C^\mathcal{V}$ of C^* implement \mathcal{U} with worst-case error $1/q(|x|)$.*

Just like one can define oracle complexity classes like $\text{P}^{3\text{SAT}}$ (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 $\text{unitaryBQP}^\mathcal{V}$ to be the set of all unitary synthesis problems that are polynomial-time reducible to a unitary synthesis problem \mathcal{V} .*

We can also define reductions between distributional unitary synthesis problems, analogously to how reductions between distributional problems are defined in classical average case complexity.

First, we need to define what it means for a query circuit to be instantiated with an average-case implementation of an oracle.

Definition 3.20 (Average-case instantiation of a query circuit). *Let $(\mathcal{U} = (U_x)_x, \Psi = (|\psi_x\rangle)_x)$ denote a distributional unitary synthesis problem. Let $\epsilon(n)$ be a function and let C^* denote a quantum query circuit that queries $U_{x_1}, U_{x_2}, \dots, U_{x_m}$. An ϵ -error average-case instantiation of C^* with (\mathcal{U}, Ψ) , denoted by $C^{(\mathcal{U}, \Psi)}$, is a quantum channel obtained from C^* by replacing all the oracle gates with label x by some quantum algorithm (which can be different each time U_x is called) that implements U_x on the distribution ψ_x with average-case error $\epsilon(|x|)$.*

Furthermore, whenever we write $C^{(\mathcal{U}, \Psi)}$, we implicitly require that \mathcal{U} is such that the input and output registers of U_x match the input and output registers of any oracle gate with label x in C^* .

We note that the error ϵ in an “ ϵ -error average-case instantiation” only refers to the error with which the oracle gates are implemented, not the error of the output of the overall quantum query circuit. The latter will of course depend on ϵ , but also on other factors, e.g. how many oracle queries are made and how sensitive the overall output is to errors in the oracle implementation.

We now define reductions between distributional problems.

¹⁰Of course, for a family of query circuits (C_x^*) , the labels y used by C_x^* can depend on the index x ; the point here is that a given C_x^* cannot compute the labels y as a function of the quantum input it is given.

Definition 3.21 (Reductions between distributional problems). Let $(\mathcal{U} = (U_x)_x, \Psi = (|\psi_x\rangle)_x)$ and $(\mathcal{V} = (V_x)_x, \Omega = (|\omega_x\rangle)_x)$ denote distributional unitary synthesis problems. Then (\mathcal{U}, Ψ) (polynomial-time) reduces to (\mathcal{V}, Ω) if for all polynomials $q(n)$ there exists a polynomial-time quantum query algorithm C^* and a polynomial $r(n)$ such that all $1/r(n)$ -error average-case instantiations $C^{(\mathcal{V}, \Omega)}$ implement (\mathcal{U}, Ψ) with average-case error $1/q(n)$.

Next we aim to define the oracle class $\text{avgUnitaryBQP}^{(\mathcal{V}, \Omega)}$. For this, we will have to specify a state complexity class which the distributional states are required to be from. For avgUnitaryBQP , we required that the distributional states be from stateBQP . However, if we give the avgUnitaryBQP oracle access to (\mathcal{V}, Ω) , it is natural to allow the same oracle access for the preparation of the distributional states, too. Therefore, we have to specify a notion “oracle state complexity class”, which we will naturally denote by $\text{stateBQP}^{(\mathcal{V}, \Omega)}$. Similar definitions can be made for other state classes in addition to stateBQP .

Definition 3.22 (Oracle state complexity classes). Let $(\mathcal{V} = (V_x)_x, \Omega = (|\omega_x\rangle)_x)$ be a distributional unitary synthesis problem. We define the oracle state complexity class $\text{stateBQP}^{(\mathcal{V}, \Omega)}$ to be the set of state families $\Psi = (|\psi_x\rangle)_x$ where for all polynomials $q(n)$ there exists a polynomial-time quantum query algorithm $C^* = (C_x^*)_x$ and a polynomial $r(n)$ such that for all x , all $1/r(n)$ -error average-case instantiations $C_x^{(\mathcal{V}, \Psi)}$ on the all zeroes input outputs a state that is $1/q(n)$ -close to $|\psi_x\rangle$.

In other words, a state family $\Psi = (|\psi_x\rangle)_x$ is in $\text{stateBQP}^{(\mathcal{V}, \Omega)}$ if it can be synthesized by polynomial-sized circuits that also have the ability to query algorithms that solve \mathcal{V} in the average case. We now define the oracle class $\text{avgUnitaryBQP}^{(\mathcal{V}, \Omega)}$:

Definition 3.23 (Average-case oracle unitary complexity classes). We define the oracle class $\text{avgUnitaryBQP}^{(\mathcal{V}, \Omega)}$ to be the set of all distributional problems (\mathcal{U}, Ψ) that are polynomial-time reducible to the distributional unitary synthesis problem (\mathcal{V}, Ω) and for which $\Psi \in \text{stateBQP}^{(\mathcal{V}, \Omega)}$.

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

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

As would be expected, unitaryBQP and avgUnitaryBQP are closed under polynomial-time reductions.

Lemma 3.25. unitaryBQP is closed under polynomial-time reductions, i.e. for all $\mathcal{V} \in \text{unitaryBQP}$, we have that $\text{unitaryBQP}^{\mathcal{V}} \subseteq \text{unitaryBQP}$.

Likewise, avgUnitaryBQP is closed under polynomial-time reductions, i.e. for all $(\mathcal{V}, \Omega) \in \text{avgUnitaryBQP}$, we have that $\text{avgUnitaryBQP}^{(\mathcal{V}, \Omega)} \subseteq \text{avgUnitaryBQP}$.

Proof. Consider a unitary synthesis problem $\mathcal{U} = (U_x)_x \in \text{unitaryBQP}^{\mathcal{V}}$. By definition, for all polynomials q there exists a polynomial-time quantum query algorithm $C^* = (C_x^*)_x$ such that all instantiations $C_x^{\mathcal{V}}$ implement U_x with worst-case error $1/q(|x|)$. Since $\mathcal{V} \in \text{unitaryBQP}$, for all polynomials p there exists a polynomial-size circuit family \tilde{C}_y such that \tilde{C}_y is $1/p(|y|)$ -close to a channel completion of V_y . Since C_x^* can include $r(|x|) = \text{poly}(|x|)$ many oracle gates with labels y such that $|y| = \text{poly}(|x|)$, we can simply replace each oracle gate by the polynomial-time circuit \tilde{C}_y ; this will yield another polynomial-size circuit, and this circuit will be $(r(|x|)/p(\text{poly}(|x|)) + 1/q(|x|))$ -close to a channel completion of U_x by the triangle inequality and monotonicity property of the diamond norm. Since p, q can be chosen arbitrarily large, we get that $\mathcal{U} \in \text{unitaryBQP}$. The statement for avgUnitaryBQP follows analogously after noting that for $(\mathcal{V}, \Omega) \in \text{avgUnitaryBQP}$, $\text{stateBQP}^{(\mathcal{V}, \Omega)} \subseteq \text{stateBQP}$. \square

The same statement holds for unitaryPSPACE and avgUnitaryPSPACE , too.

Lemma 3.26. *unitaryPSPACE is closed under polynomial-time reductions, i.e. for all $\mathcal{V} \in \text{unitaryPSPACE}$, we have that $\text{unitaryBQP}^{\mathcal{V}} \subseteq \text{unitaryPSPACE}$.*

Similarly, avgUnitaryPSPACE is closed under polynomial-time reductions, i.e. for all $(\mathcal{V}, \Omega) \in \text{avgUnitaryPSPACE}$, we have that $\text{avgUnitaryBQP}^{(\mathcal{V}, \Omega)} \subseteq \text{avgUnitaryPSPACE}$.

Proof. The proof for the worst-case class unitaryPSPACE is identical to that of Lemma 3.25. The proof for the average-case setting is analogous, too, except that we now need to ensure that the distributional states $\Psi \in \text{stateBQP}^{(\mathcal{V}, \Omega)}$ allowed by the oracle class $\text{avgUnitaryBQP}^{(\mathcal{V}, \Omega)}$ are also valid input states for a problem in avgUnitaryPSPACE ; that is we need to show that $\text{stateBQP}^{(\mathcal{V}, \Omega)} \subseteq \text{statePSPACE}$ for a distributional problem $(\mathcal{V}, \Omega) \in \text{avgUnitaryPSPACE}$. This is easily seen to hold by the same argument we used for Lemma 3.25: we can simply replace all oracle calls in the state preparation procedure for $\Psi \in \text{stateBQP}^{(\mathcal{V}, \Omega)}$ by the corresponding space-uniform circuit that implements (\mathcal{V}, Ω) ; since there are at most polynomially oracle calls, the result is a space-uniform circuit, so $\Psi \in \text{statePSPACE}$. \square

3.4 Discussion and open problems

In this section, we have 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 will 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 1. What are other unitary complexity classes that naturally relate to physically interesting problems? For example, is there a useful notion of unitaryQMA ?

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 $\text{unitaryBQP} \neq \text{unitaryPSPACE}$. For decision languages, proving such separations unconditionally is significantly out of reach of current techniques. However, 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 $\text{unitaryBQP} \neq \text{unitaryPSPACE}$, but $\text{BQP} = \text{PSPACE}$. Therefore, another interesting question is the following:

Open Problem 2. Are there barriers from traditional complexity theory to proving unitary complexity class separations?

Another important direction is to find complete problems for unitary complexity classes. We make progress on this by showing that (certain variants of) the Uhlmann transformation problem are complete for certain unitary classes, but there might be other interesting complete problems for other unitary classes. One natural option is the following:

Open Problem 3. Is Hamiltonian Fast-Forwarding [AA17] complete for unitaryPSPACE ?

One can also consider variations of the model for unitary synthesis. In this paper, we always assume that the unitary needs to be applied on a single copy of an unknown state. However, it might also make sense to consider a model where an implementation of a unitary is allowed to “consume” multiple copies of an input state, but only has to produce a single output state.

Open Problem 4. How can a multi-input version of unitary synthesis problems be formalised, including cases where the unitary is supposed to act on a part of a larger pure state? Are there meaningful notions of reductions and complexity classes of unitary synthesis problems in this multi-input model?

4 Interactive Proofs for Unitary Synthesis

In this section we introduce the model of interactive proofs for unitary synthesis problems, as well as the corresponding unitary complexity classes. In particular we introduce the unitary synthesis classes unitaryQIP and avgUnitarySZK , which are analogues of QIP and (average-case) SZK, respectively. As we will see in Sections 6 and 7, the complexity of such interactive proof classes is captured by the Uhlmann Transformation Problem.

4.1 Quantum interactive protocols

First we formally describe 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 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 register V is further divided into disjoint sub-registers $(V_{\text{work}}, V_{\text{flag}}, V_{\text{out}})$. The register V_{work} is the verifier circuit’s “workspace”, the register V_{flag} is a single qubit indicating whether the verifier accepts or rejects, and the register V_{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 V_{work} . We write $C(|\psi\rangle) \rightleftharpoons P$ to denote the interaction between the verifier circuit C and the prover P on input ρ , which is defined according to the following process. The initial state of the system is $|\phi_0\rangle = |\psi, 0 \cdots 0\rangle_{V_{\text{work}}} |0 \cdots 0\rangle_{V_{\text{flag}} V_{\text{out}} MP}$. 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 $C(|\psi\rangle) \rightleftharpoons P$ accepts (resp. rejects) if measuring the register V_{flag} in the standard basis yields the outcome 1 (resp. 0). We say that the *output of $C(|\psi\rangle) \rightleftharpoons P$ conditioned on accepting* is the density matrix

$$\frac{\text{Tr}_{V_{\text{MP}} \setminus V_{\text{out}}} \left(|1\rangle\langle 1|_{V_{\text{flag}}} \cdot \phi_{2k} \right)}{\text{Tr} \left(|1\rangle\langle 1|_{V_{\text{flag}}} \cdot \phi_{2k} \right)};$$

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

A *quantum verifier* $V = (V_x)_{x \in \{0,1\}^*}$ is a uniform sequence of polynomial-size and polynomial-round quantum verifier circuits.

4.2 Interactive proofs for unitary synthesis

We now present our notion of interactive protocols for unitary synthesis.

Definition 4.1 (unitaryQIP). *Let $c, s, \delta : \mathbb{N} \rightarrow [0, 1]$ be functions. The class $\text{unitaryQIP}_{c,s,\delta}$ is the set of unitary synthesis problems $\mathcal{U} = (U_x)_x$ where there exists a polynomial-time quantum verifier $V = (V_x)_{x \in \{0,1\}^*}$ satisfying, for all $x \in \{0, 1\}^*$ of sufficiently large length,*

- *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 ,*

$$\Pr[V_x(|\psi\rangle) \rightleftharpoons P \text{ accepts}] \geq c(|x|)$$

- *Soundness: For all input states $|\psi\rangle$ and for all quantum provers P , there exists a channel completion of Φ_x of U_x such that*

$$\text{if } \Pr[V_x(|\psi\rangle) \rightleftharpoons P \text{ accepts}] \geq s(|x|) \quad \text{then} \quad \text{td}(\sigma, \Phi_x(\psi)) \leq \delta(|x|),$$

where σ denotes the output of $V_x(|\psi\rangle) \rightleftharpoons P$ conditioned on accepting.

Here the probabilities are over the randomness of the interaction.

Finally, define

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

where the union is over all negligible functions $\epsilon(n)$, and define

$$\text{unitaryQIP} = \bigcap_{q(n) \text{ poly}} \text{unitaryQIP}_{1/q(n)}$$

where the intersection ranges over all polynomials $q(n)$.

Intuitively, a unitary synthesis problem $\mathcal{U} = (U_x)_x$ has an interactive proof if a polynomial-time verifier who receives a pair $(x, |\psi\rangle)$ can interact with an all-powerful prover, and conditioned on accepting, output a state close to $U_x |\psi\rangle$.

The class **unitaryQIP** is analogous to the state synthesis class **stateQIP** introduced by [RY22]; the only difference is that a **stateQIP** verifier for the state family $\Psi = (|\psi_x\rangle)_x$ has its input registers fixed to the all zeroes state, and in the soundness condition, if a prover makes V_x accept with probability at least $s(n)$, then its output conditioned on accepting is close to the target state $|\psi_x\rangle$.

We make a few remarks regarding the definition. First, one may notice a peculiar asymmetry between the definitions of the classes **unitaryQIP $_\delta$** and **unitaryQIP**. The class **unitaryQIP $_\delta$** is defined as a *union* over completeness parameters $c(n) = 1 - \epsilon(n)$ for some negligible function $\epsilon(n)$. This is because we want to consider unitary synthesis protocols as long as there is an honest prover that can be accepted with probability $1 - \epsilon(n)$ for *some* negligible function $\epsilon(n)$; we do not want to fix a particular negligible function. On the other hand, the class **unitaryQIP** is defined as the *intersection* of **unitaryQIP $_{1/q(n)}$** over all choices of polynomials $q(n)$. Here the quantity $1/q(n)$ denotes how well the output state (conditioned on the verifier accepting) approximates the target state, and we want to consider state sequences where for all polynomials $q(n)$ there is a protocol that can synthesize the state with error smaller than $1/q(n)$ (for sufficiently large n).

A second remark concerns the default choice of soundness $s(n) = \frac{1}{2}$ for the definition of **unitaryQIP $_\delta$** and **unitaryQIP**. In the state synthesis setting, the soundness parameter can be generically amplified via sequential repetition (see [RY22] for a proof). Thus the class **stateQIP** is the same for any soundness, completeness parameters that are separated by at least an inverse polynomial. It is not clear whether soundness amplification is possible in the unitary synthesis setting, however. 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 motivates the following open question.

Open Problem 5. Can completeness/soundness amplification be performed for **unitaryQIP**, or is there evidence that it's not possible?

In analogy to [Definition 4.1](#), we also define an average-case complexity version of **unitaryQIP**, where the verifier only has to synthesize the desired unitary well on a given distribution state.

Definition 4.2 (avgUnitaryQIP). *Let $c, s, \delta : \mathbb{N} \rightarrow [0, 1]$ be functions. The class **avgUnitaryQIP $_{c,s,\delta}$** is the set of distributional unitary synthesis problems $(\mathcal{U} = (U_x)_x, \Psi = (|\psi_x\rangle)_x)$ such that $\Psi \in \mathbf{stateQIP}$ and there exists a polynomial-time quantum verifier $V = (V_x)_{x \in \{0,1\}^*}$ satisfying, for all $x \in \{0,1\}^*$ of sufficiently large length,*

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

$$\Pr[V_x(|\psi_x\rangle) \stackrel{P}{\text{accepts}}] \geq c(|x|)$$

- *Soundness: For all quantum provers P , there exists a channel completion Φ_x of U_x such that*

$$\text{if } \Pr[V_x(|\psi_x\rangle) \stackrel{P}{\text{accepts}}] \geq s(|x|) \quad \text{then} \quad \text{td}(\sigma, (\Phi_x \otimes \text{id})(\psi_x)) \leq \delta(|x|).$$

where σ denotes the output of $V_x(|\psi_x\rangle) \stackrel{P}{\text{accepts}}$ conditioned on accepting and V_x acts the identity on the ancilla register of $|\psi_x\rangle$.

Here the probabilities are over the randomness of the interaction. Finally, define

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

where the union is over all negligible functions $\epsilon(n)$, and define

$$\text{avgUnitaryQIP} = \bigcap_{q(n) \text{ poly}} \text{avgUnitaryQIP}_{1/q(n)}$$

where the intersection ranges over all polynomials $q(n)$.

For this section, we only consider 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 6. Is there a meaningful notion of multi-prover unitary synthesis protocols, and what is their power?

A related question concerns distributed protocols for unitary synthesis, where multiple provers have to apply a unitary collectively under certain resource constraints. Such a scenario was recently studied for state synthesis problems [GMN22], and it is natural to ask what can be said in the unitary synthesis setting.

Open Problem 7. How are unitary synthesis problems related to distributed quantum computation?

4.3 Zero-knowledge protocols for state and unitary synthesis

In this section we present a notion of *zero knowledge* for unitary synthesis problems. *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; this poses an additional conceptual difficulty in trying to come up with a reasonable notion of zero knowledge simulation.

We first explore several attempts to define zero knowledge for unitary synthesis, and highlight their shortcomings. 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 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 $\mathcal{U} \in \text{unitaryBQP}$. 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 an input state that comes from half of a distribution state $|\psi_x\rangle$. 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 this is seemingly a weak notion of zero knowledge, as we will see in [Section 6](#) it captures the complexity of the Uhlmann Transformation Problem.

Definition 4.3 ($\text{avgUnitarySZK}_{\text{HV}}$). *Let $c, s, \delta : \mathbb{N} \rightarrow [0, 1]$ be functions. The class $\text{avgUnitarySZK}_{\text{HV}, c, s, \delta}$ is the set of distributional unitary synthesis problems (\mathcal{U}, Ψ) with $\mathcal{U} = (U_x)_x$ and $\Psi = (|\psi_x\rangle)_x \in \text{stateBQP}$ for which there exists a polynomial-time quantum verifier $V^* = (V_x^*)_{x \in \{0, 1\}^*}$ (called the honest verifier), an unbounded prover P^* (called the honest prover), and a polynomial-time quantum algorithm Sim (called the simulator) such that for sufficiently long $x \in \{0, 1\}^*$,*

1. *The prover P^* on input x is accepted with probability at least $c(|x|)$.*
2. *The verifier V^* satisfies the soundness condition (in [Definition 4.2](#)) of an $\text{avgUnitaryQIP}_{c, s, \delta}$ verifier for (\mathcal{U}, Ψ) .*
3. *There exists a negligible function $\epsilon : \mathbb{N} \rightarrow \mathbb{R}$ such that the simulator Sim , on input (x, r) (for $r \in \mathbb{N}$), outputs a state ρ satisfying*

$$\text{td}(\rho, \sigma_{x, r}) \leq \epsilon(|x|)$$

where $\sigma_{x, r}$ is the reduced density matrix of the verifier V_x^ 's private register (which was given the target register of the distribution state $|\psi_x\rangle$), and the purifying register of $|\psi_x\rangle$, immediately after the r 'th round of interaction with the honest prover P^* .*

Finally, define

$$\text{avgUnitarySZK}_{\text{HV}, \delta} = \bigcup_{\epsilon(n) \text{ negl}} \text{avgUnitarySZK}_{\text{HV}, 1-\epsilon, \frac{1}{2}, \delta},$$

where the union ranges over all negligible functions $\epsilon(n)$, and

$$\text{avgUnitarySZK}_{\text{HV}} = \bigcap_{q(n) \text{ poly}} \text{avgUnitarySZK}_{\text{HV}, 1/q(n)}$$

where the intersection ranges over all polynomials $q(n)$.

Note that the definition of `avgUnitaryQIP` (Definition 4.2 already includes a completeness condition. However, we need to list the completeness condition for `avgUnitarySZK` explicitly because we need to ensure that the prover P^* for whom the completeness condition holds is the same as the prover P^* in the zero-knowledge condition.

We now make several additional remarks regarding the zero knowledge definition.

Simulation of the average case. If we think of running a unitary synthesis protocol on the distribution state $|\psi_x\rangle$, then from the point of view of the verifier, it is given a pure state input $|\phi\rangle$ sampled from a distribution corresponding to the reduced density matrix of $|\psi_x\rangle$. Let \mathcal{D}_x denote this distribution of pure states. (This distribution may not be unique because the spectral decomposition is not unique, but the end result is the same.) Then in this definition the simulator’s job is to produce the view of the verifier *averaged over inputs sampled from \mathcal{D}_x* . In other words, the simulator does not have to reproduce the view of the verifier on any specific input state $|\phi\rangle$, just on average.

Complexity of the distribution state. The distribution state sequence Ψ associated with a distributional unitary synthesis problem in `avgUnitarySZKHV` is required to be in `stateBQP`, instead of some notion of `stateSZKHV`. In the definition of `avgUnitarySZKHV` we require that the simulator can output the state between an honest verifier and honest prover after each round. It is easy to see that any reasonable definition of `stateSZKHV` results in the same class as `stateBQP`.

Honest-verifier versus general zero knowledge. A natural question is whether this definition of zero knowledge can be meaningfully generalized to the *malicious verifier* setting, where 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., `SZK` = `SZKHV` and `QSZK` = `QSZKHV`) [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?

Part II

Uhlmann Transformation Problem: Definitions and Structural Results

5 Definition of 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 input states $|C\rangle, |D\rangle$ that specify an instance of the Uhlmann Transformation Problem, while exponentially complex, nonetheless have a polynomial-size description.

5.1 Uhlmann’s theorem and canonical isometries

We begin by recalling Uhlmann’s theorem.

Theorem 5.1 (Uhlmann’s theorem). *Let $|\psi\rangle_{\text{AB}}$ and $|\varphi\rangle_{\text{AB}}$ be pure states on registers AB and denote their reduced states on register A by ρ_{A} and σ_{A} , respectively. Then, there exists a unitary U_{B} acting only on register B such that*

$$F(\rho_{\text{A}}, \sigma_{\text{A}}) = |\langle \varphi |_{\text{AB}} (\text{id}_{\text{A}} \otimes U_{\text{B}}) |\psi\rangle_{\text{AB}}|^2.$$

We now 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 $|\psi\rangle, |\varphi\rangle$ (by specifying circuits for them, for example), the unitary U_x should satisfy the conclusion of Uhlmann’s theorem. However there are several subtleties that arise. First, the unitary U_{B} in Theorem 5.1 is not unique; outside of the support of $\rho_{\text{B}} = \text{Tr}_{\text{A}}(|\psi\rangle\langle\psi|_{\text{AB}})$, U_{B} can act arbitrarily. This motivates defining a *canonical* Uhlmann transformation W corresponding to a pair of bipartite states $|\psi\rangle_{\text{AB}}, |\varphi\rangle_{\text{AB}}$. A natural candidate is $W = \text{sgn}(\text{Tr}_{\text{A}}(|\varphi\rangle\langle\psi|))$ where for any linear operator K with singular value decomposition $U\Sigma V^\dagger$, we define $\text{sgn}(K) = U \text{sgn}(\Sigma) V^\dagger$ with $\text{sgn}(\Sigma)$ 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). A proof that W is a partial isometry satisfying $F(\rho, \sigma) = |\langle \varphi | \text{id} \otimes W |\psi\rangle|^2$ can be found in [MY23, Lemma 7.6]. This Uhlmann transformation is also *minimal* in the sense that any other partial isometry \tilde{W} that achieves the same guarantee satisfies $W^\dagger W \leq \tilde{W}^\dagger \tilde{W}$.

However, this definition of canonical Uhlmann transformation is not robust in the sense that arbitrarily small changes to the states $|\psi\rangle, |\varphi\rangle$ could result in arbitrarily large changes in W as measured by, say, the operator norm. Consider the following two-qutrit example:

$$\begin{aligned} |\psi\rangle &= \sqrt{1-\epsilon}|00\rangle + \sqrt{\epsilon/2}|11\rangle + \sqrt{\epsilon/2}|22\rangle, \\ |\tilde{\psi}\rangle &= \sqrt{1-\epsilon}|00\rangle + \sqrt{\epsilon/2}|12\rangle + \sqrt{\epsilon/2}|21\rangle, \\ |\varphi\rangle &= |\psi\rangle. \end{aligned}$$

The Uhlmann isometry W corresponding to $(|\psi\rangle, |\varphi\rangle)$ is simply the identity operator on \mathbb{C}^3 . On the other hand, the Uhlmann isometry \tilde{W} corresponding to $(|\tilde{\psi}\rangle, |\varphi\rangle)$ can be computed as

$$\tilde{W} = |0\rangle\langle 0| + |1\rangle\langle 2| + |2\rangle\langle 1|.$$

In other words, it swaps $|1\rangle$ with $|2\rangle$ and keeps $|0\rangle$ unchanged. The difference $W - \tilde{W}$ has operator norm at least 2, but the difference $|\psi\rangle - |\tilde{\psi}\rangle$ has norm at most ϵ , which can be arbitrarily small. We would like a definition of the canonical Uhlmann isometry that is insensitive to extremely small changes in the states $|\psi\rangle, |\varphi\rangle$.

Finally, for convenience, we only focus on bipartite states that have the same number of qubits on each side. This is not a severe assumption as we can always pad the smaller register with ancilla zero qubits, which does not affect the existence of an Uhlmann transformation.

These points motivate the following definition of canonical Uhlmann isometry. First, some notation: for $\eta \in \mathbb{R}$ and an operator K with singular value decomposition $U\Sigma V^\dagger$, we define $\text{sgn}_\eta(K)$ to be the operator

$$\text{sgn}_\eta(K) = U \text{sgn}_\eta(\Sigma) V^\dagger$$

where $\text{sgn}_\eta(\Sigma)$ denotes the projection onto the eigenvectors of Σ with eigenvalue greater than η . In other words, sgn_η is the scalar function that behaves like the usual sgn function on inputs $|x| > \eta$, and maps inputs $|x| \leq \eta$ to 0; this scalar function is applied to the diagonal matrix Σ in the usual way. We also write $\text{sgn}(K)$ to denote $\text{sgn}_0(K)$. Using sgn_η instead of sgn in the definition of the Uhlmann partial isometry removes the sensitivity to arbitrarily small changes to the input states discussed above. The parameter η can be thought of as a cutoff below which changes in the input states are ignored.

Definition 5.2 (Canonical Uhlmann partial isometry). *The canonical Uhlmann partial isometry with cutoff η corresponding to a pair of pure states $(|\psi\rangle_{\text{AB}}, |\varphi\rangle_{\text{AB}})$ is defined as*

$$W = \text{sgn}_\eta(\text{Tr}_A(|\varphi\rangle\langle\psi|)). \quad (5.1)$$

For brevity we call W the canonical η -Uhlmann isometry.

We verify several basic properties of the canonical η -Uhlmann isometry.

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 $|\psi\rangle, |\varphi\rangle$, respectively, on register A .*

1. (Approximate Uhlmann transformation) *The isometry W approximately maps $|\psi\rangle$ to $|\varphi\rangle$, i.e.,*

$$|\langle\varphi|_{\text{AB}} (\text{id}_A \otimes W_B) |\psi\rangle_{\text{AB}}|^2 \geq F(\rho_A, \sigma_A) - 2\eta \dim(\text{B}),$$

2. (Minimality) *For all partial isometries R_B satisfying*

$$F(\rho_A, \sigma_A) = |\langle\varphi|_{\text{AB}} (\text{id}_A \otimes R_B) |\psi\rangle_{\text{AB}}|^2,$$

we have $W^\dagger W \leq R^\dagger R$.

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

$$\begin{aligned} |\psi\rangle &= \sqrt{\rho} \otimes X |\Omega\rangle \\ |\varphi\rangle &= \sqrt{\sigma} \otimes Y |\Omega\rangle \end{aligned}$$

where $|\Omega\rangle = \sum_i |i\rangle_A |i\rangle_B$ 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

$$W = YU \text{sgn}_\eta(\Sigma) V^\dagger X^\dagger. \quad (5.2)$$

The fact that W is a partial isometry is clear: since the matrices X, U, V, Y are unitary and $\text{sgn}_\eta(\Sigma)$ is a projection, it can be written in the form $W = \Pi F$ where $\Pi = XU \text{sgn}_\eta(\Sigma) U^\dagger X^\dagger$ is a projection and $F = XUV^\dagger Y^\dagger$ is a unitary. To show the approximate transformation statement, we note that the proof of [MY23, Lemma 7.6] shows that

$$\langle \varphi |_{\text{AB}} (\text{id}_A \otimes W_B) | \psi \rangle_{\text{AB}} = \text{Tr}(\sqrt{\sigma} \sqrt{\rho} \text{sgn}_\eta(\sqrt{\rho} \sqrt{\sigma}))$$

where $\text{sgn}_\eta(K)$ for an arbitrary operator K with singular value decomposition $R\Sigma Q^\dagger$ is defined to be $R \text{sgn}_\eta(\Sigma) Q^\dagger$. The preceding centered equation is equal to

$$\begin{aligned} & \text{Tr}(\sqrt{\sigma} \sqrt{\rho} \text{sgn}(\sqrt{\rho} \sqrt{\sigma})) - \text{Tr}\left(\sqrt{\sigma} \sqrt{\rho} (\text{sgn}(\sqrt{\rho} \sqrt{\sigma}) - \text{sgn}_\eta(\sqrt{\rho} \sqrt{\sigma}))\right) \\ & \geq \sqrt{F(\sigma, \rho)} - \text{Tr}\left(\sqrt{\sigma} \sqrt{\rho} (\text{sgn}(\sqrt{\rho} \sqrt{\sigma}) - \text{sgn}_\eta(\sqrt{\rho} \sqrt{\sigma}))\right) \end{aligned} \quad (5.3)$$

where in the last line we used that $F(\sigma, \rho) = \text{Tr}(|\sqrt{\sigma} \sqrt{\rho}|)^2$ and that $\text{Tr}(K \text{sgn}(K^\dagger)) = \text{Tr}(|K|)$ for all operators K . Letting $U\Sigma V^\dagger$ denote the singular value decomposition of $(\sqrt{\rho} \sqrt{\sigma})^\top$, we have that $\bar{U}\Sigma V^\top$ is the singular value decomposition of $\sqrt{\sigma} \sqrt{\rho}$. Thus Equation (5.3) is equal to

$$\sqrt{F(\sigma, \rho)} - \text{Tr}(\Sigma(\text{sgn}(\Sigma) - \text{sgn}_\eta(\Sigma))) \geq \sqrt{F(\sigma, \rho)} - \eta \dim(\text{B})$$

where we used that $\text{sgn}(\Sigma) - \text{sgn}_\eta(\Sigma)$ is the projector onto the eigenvectors of Σ with eigenvalue smaller than η . Squaring both sides, we get:

$$\left(\sqrt{F(\sigma, \rho)} - \eta \dim(\text{B})\right)^2 = F(\sigma, \rho) - 2\sqrt{F(\sigma, \rho)}\eta \dim(\text{B}) + \eta^2 \dim(\text{B})^2 \geq F(\sigma, \rho) - 2\eta \dim(\text{B})$$

where we used that $0 \leq F(\sigma, \rho) \leq 1$. This shows the approximation statement.

For the minimality statement, we note that the proof of Uhlmann's theorem [Wil13, Theorem 9.2.1] shows that

$$|\langle \varphi |_{\text{AB}} (\text{id}_A \otimes R_B) | \psi \rangle_{\text{AB}}|^2 = |\text{Tr}(\sqrt{\sigma} \sqrt{\rho} (Y^\dagger R X)^\top)|^2 = |\text{Tr}((Y^\dagger R X)(\sqrt{\sigma} \sqrt{\rho})^\top)|^2$$

where in the last step we used $|\text{Tr}(K)| = |\text{Tr}(K^\top)|$ for all operators K . Let $Q = Y^\dagger R X$, and note that the singular value decomposition of $(\sqrt{\sigma} \sqrt{\rho})^\top$ is $V\Sigma U^\dagger$. By the Cauchy-Schwarz inequality for matrices, we have

$$\begin{aligned} |\text{Tr}((Y^\dagger R X)(\sqrt{\sigma} \sqrt{\rho})^\top)|^2 &= |\text{Tr}(QV\Sigma^{1/2}\Sigma^{1/2}U^\dagger)|^2 \leq \text{Tr}(QV\Sigma V^\dagger Q^\dagger) \text{Tr}(U\Sigma U^\dagger) \\ &= \text{Tr}(\Sigma V^\dagger Q^\dagger QV) \text{Tr}(\Sigma) \leq \text{Tr}(\Sigma)^2 \end{aligned}$$

where in the last line we used that the operator norm of $V^\dagger Q^\dagger QV$ is at most 1. If $|\langle \varphi |_{\text{AB}} (\text{id}_A \otimes R_B) | \psi \rangle_{\text{AB}}|^2 = F(\rho, \sigma)^2 = \text{Tr}(|\sqrt{\sigma} \sqrt{\rho}|) = \text{Tr}(\Sigma)^2$, then this implies that

$$\text{Tr}(\Sigma V^\dagger Q^\dagger QV) = \text{Tr}(\Sigma).$$

Since Σ and $V^\dagger Q^\dagger QV$ are positive semidefinite, and $V^\dagger Q^\dagger QV$ has operator norm at most 1, this implies that $V^\dagger Q^\dagger QV$ acts as the identity on the support of Σ ; in particular, $V^\dagger Q^\dagger QV \geq \text{sgn}(\Sigma)$ in the positive semidefinite ordering. This is equivalent to

$$R^\dagger R \geq XV \text{sgn}(\Sigma) V^\dagger X^\dagger \geq XV \text{sgn}_\eta(\Sigma) V^\dagger X^\dagger = W^\dagger W$$

as desired. \square

5.2 Worst-case Uhlmann transformation problem

We now 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 $(1^n, g_1, g_2, \dots)$ where 1^n represents in unary the number of qubits that C acts on, and g_1, g_2, g_3, \dots 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 circuit¹¹ 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, \dots, 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 qubits it acts on as well as the number of gates in the circuit.
- (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.

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 $F(\rho, \sigma) \geq \kappa$.

Definition 5.6 (Uhlmann Transformation Problem). *Let $\kappa, \eta : \mathbb{N} \rightarrow [0, 1]$ be functions. The (κ, η) -Uhlmann Transformation Problem is the unitary synthesis problem $\text{UHLMANN}_{\kappa, \eta} = (U_x)_{x \in \{0, 1\}^*}$ where whenever x 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 η -Uhlmann isometry for the states $|C\rangle = C|0^{2n}\rangle$ and $|D\rangle = D|0^{2n}\rangle$, with U_x acting on the last n qubits. 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, η) -Succinct Uhlmann Transformation Problem, denoted by $\text{SUCCINCTUHLMANN}_{\kappa, \eta}$, is the sequence $(U_x)_x$ where whenever x is a valid fidelity- $\kappa(n)$ succinct Uhlmann instance specifying

¹¹Here, we think of \hat{C} as being a list of AND, OR, and NOT gates.

a pair (C, D) of unitary circuits that each act on $2n$ qubits for some n , then U_x is the canonical η -Uhlmann isometry for the states $|C\rangle = C|0^{2n}\rangle$ and $|D\rangle = D|0^{2n}\rangle$, with U_x acting on the last n qubits; if x is not a valid succinct Uhlmann instance, then we define $U_x = 0$.

Although we defined the UHLMANN and SUCCINCTUHLMANN problems as parameterized by the cutoff parameter η for the sake of robustness of the definitions, we will see next that when we focus on *distributional* versions of these problems the η parameter can be without loss of generality set to 0. The cutoff parameter η only really matters for complexity results about solving UHLMANN or SUCCINCTUHLMANN in the *worst-case*.

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 . If x specifies a pair of circuits (C, D) on $2n$ qubits each, the distribution state $|\psi_x\rangle$ is also on $2n$ qubits. As we argue below, a natural choice of distribution state is $|\psi_x\rangle = C|0^{2n}\rangle$. When x represents a fidelity-1 Uhlmann instance the Uhlmann transformation U_x by definition maps $|\psi_x\rangle$ to $D|0^{2n}\rangle$.

Definition 5.7 (Distributional Uhlmann Transformation Problems). *We define a state sequence $\Psi_{\text{UHLMANN}} = (|\psi_x\rangle)_{x \in \{0,1\}^*}$ 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, η) -Uhlmann Transformation Problem is the distributional unitary synthesis problem $\text{DISTUHLMANN}_{\kappa, \eta} = (\text{UHLMANN}_{\kappa, \eta}, \Psi_{\text{UHLMANN}})$.

Analogously, we define the state family $\Psi_{\text{SUCCINCTUHLMANN}} = (|\psi_x\rangle)_x$ as follows: for all $x \in \{0,1\}^$,*

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

The distributional (κ, η) -Succinct Uhlmann Transformation Problem is the distributional unitary synthesis problem $\text{DISTSUCCINCTUHLMANN}_{\kappa, \eta} = (\text{SUCCINCTUHLMANN}_{\kappa, \eta}, \Psi_{\text{SUCCINCTUHLMANN}})$.

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 κ is close to 1.

Proposition 5.8. *Let $M = (M_x)_x$ be a quantum algorithm where for each valid fidelity- $\kappa(n)$ Uhlmann (resp. Succinct Uhlmann) instance $x = (1^n, C, D)$ (resp. $x = (1^n, \hat{C}, \hat{D})$),*

$$F\left((\text{id} \otimes M_x)(|C\rangle\langle C|), |D\rangle\langle D|\right) \geq \kappa(n) - \delta(n) \quad (5.4)$$

for some error function $\delta(n)$, where M_x acts on the second n qubits of $|C\rangle$. Then M implements $\text{DISTUHLMANN}_{\kappa, 0}$ (resp. $\text{DISTSUCCINCTUHLMANN}_{\kappa, 0}$) with average-case error $6\sqrt{1 - \kappa(n)} + \sqrt{\delta(n)}$.

Conversely, suppose that a (uniform or nonuniform) quantum algorithm $M = (M_x)_x$ implements $\text{DISTUHLMANN}_{\kappa,0}$ (resp. $\text{DISTSUCCINCTUHLMANN}_{\kappa,0}$) with average-case error δ . Then for all valid fidelity- $\kappa(n)$ Uhlmann (resp. Succinct Uhlmann) instances $x = (1^n, C, D)$ (resp. $x = (1^n, \hat{C}, \hat{D})$), the following holds:

$$F\left((\text{id} \otimes M_x)(|C\rangle\langle C|), |D\rangle\langle D|\right) \geq \left(1 - \delta(n) - 5\sqrt{1 - \kappa(n)}\right)^2.$$

Proof. We will prove this proposition for the case of Uhlmann instances; the case of succinct Uhlmann instances is entirely analogous. Throughout the proof we abuse notation slightly and write $\delta = \delta(n)$ and $\kappa = \kappa(n)$.

We begin with the first part of the proposition. Fix a valid fidelity- $\kappa(n)$ Uhlmann instance $x = (1^n, C, D)$. Let $\eta = 0$ and let W denote the canonical η -Uhlmann partial isometry corresponding to $(|C\rangle, |D\rangle)$. Let $U = W + (\text{id} - W^\dagger W)$, which is a (non-partial) isometry. Let $\Phi(K) = UKU^\dagger$ and note that it is a channel completion of the partial isometry W . (This is in fact the most straightforward channel completion: it simply applies W on the support of W , and the identity on the orthogonal complement of the support of W .) We will show that

$$\text{td}((\text{id} \otimes \Phi)|C\rangle\langle C|, |D\rangle\langle D|) \leq 5\sqrt{1 - \kappa}. \quad (5.5)$$

Before proving this, let us see how this implies the first part of the proposition. By the triangle inequality, we have

$$\begin{aligned} & \text{td}\left((\text{id} \otimes M_x)(|C\rangle\langle C|), (\text{id} \otimes \Phi)(|C\rangle\langle C|)\right) \\ & \leq \text{td}\left((\text{id} \otimes M_x)(|C\rangle\langle C|), |D\rangle\langle D|\right) + \text{td}\left(|D\rangle\langle D|, (\text{id} \otimes \Phi)(|C\rangle\langle C|)\right) \\ & \leq \sqrt{1 - \kappa} + \delta + 5\sqrt{1 - \kappa} \\ & \leq 6\sqrt{1 - \kappa} + \sqrt{\delta} \end{aligned}$$

where in the third line we applied the Fuchs-van de Graaf inequality to [Equation \(5.4\)](#) and also used [Equation \(5.5\)](#). This shows that one the state $|C\rangle$, M_x behaves (approximately) like a channel completion of the Uhlmann partial isometry. By [Definition 3.5](#), this means that M_x (approximately) implements the DISTUHLMANN problem as claimed in the first part of the proposition.

We now prove [Equation \(5.5\)](#). The main issue we have to deal with is that for $\kappa < 1$, the support of the reduced state of $|C\rangle$ on the second half of the qubits may not be contained in the support of the Uhlmann partial isometry. As a result, taking Φ to be a channel completion of the Uhlmann partial isometry as above, it is *not* the case that $\Phi(|C\rangle\langle C|) = (\text{id} \otimes W)|C\rangle\langle C|(\text{id} \otimes W^\dagger)$. (This equation does of course hold for $\kappa = 1$.)

To deal with this issue, we need to consider the state $|C\rangle$ projected onto the support of the Uhlmann partial isometry. To this end, let $\Pi = W^\dagger W$ denote the projector onto the support of W . Let $|C'\rangle$ denote the (re-normalized) projection of $|C\rangle$ onto $\text{id} \otimes \Pi$:

$$|C'\rangle = \frac{(\text{id} \otimes \Pi)|C\rangle\langle C|(\text{id} \otimes \Pi)}{\text{Tr}((\text{id} \otimes \Pi)|C\rangle\langle C|)}.$$

By the Gentle Measurement Lemma [[Wil13](#), Section 9.4], we have

$$\text{td}(|C\rangle\langle C|, |C'\rangle\langle C'|) \leq 2\sqrt{1 - \text{Tr}((\text{id} \otimes \Pi)|C\rangle\langle C|)}. \quad (5.6)$$

Note that since the projection $\text{id} \otimes \Pi$ is at least $(\text{id} \otimes W^\dagger) |D\rangle\langle D| (\text{id} \otimes W)$ in the positive semidefinite ordering, we have

$$\text{Tr}((\text{id} \otimes \Pi) |C\rangle\langle C|) \geq \text{Tr}\left((\text{id} \otimes W^\dagger) |D\rangle\langle D| (\text{id} \otimes W) |C\rangle\langle C|\right) = F(\rho, \sigma) \geq \kappa \quad (5.7)$$

where ρ, σ denote the reduced density matrices of $|C\rangle, |D\rangle$ respectively. Applying the triangle inequality, we have

$$\begin{aligned} \text{td}((\text{id} \otimes \Phi) |C\rangle\langle C|, |D\rangle\langle D|) &\leq \text{td}((\text{id} \otimes \Phi) |C\rangle\langle C|, (\text{id} \otimes \Phi) |C'\rangle\langle C'|) + \text{td}((\text{id} \otimes \Phi) |C'\rangle\langle C'|, |D\rangle\langle D|) \\ &\leq \text{td}(|C\rangle\langle C|, |C'\rangle\langle C'|) + \text{td}((\text{id} \otimes W) |C'\rangle\langle C'| (\text{id} \otimes W^\dagger), |D\rangle\langle D|) \\ &\leq 2\sqrt{1-\kappa} + \text{td}((\text{id} \otimes W) |C'\rangle\langle C'| (\text{id} \otimes W^\dagger), |D\rangle\langle D|) \end{aligned}$$

where in the second line we used the monotonicity of the trace distance under quantum channels and the fact that $|C'\rangle$ is supported on Π , and in the last line we used [Equation \(5.6\)](#) and [Equation \(5.7\)](#). To bound the last term we use the triangle inequality again:

$$\begin{aligned} &\text{td}((\text{id} \otimes W) |C'\rangle\langle C'| (\text{id} \otimes W^\dagger), |D\rangle\langle D|) \\ &\leq \text{td}(|C\rangle\langle C|, |C'\rangle\langle C'|) + \text{td}((\text{id} \otimes W) |C\rangle\langle C| (\text{id} \otimes W^\dagger), |D\rangle\langle D|) \\ &\leq 3\sqrt{1-\kappa} \end{aligned}$$

where in the last line we applied the Fuchs-van de Graaf inequality to $F((\text{id} \otimes W) |C\rangle\langle C| (\text{id} \otimes W^\dagger), |D\rangle\langle D|) \geq \kappa$. This concludes the proof of [Equation \(5.5\)](#).

We now prove the ‘‘Conversely’’ part of the proposition. Again fix a valid fidelity- $\kappa(n)$ Uhlmann instance $x = (1^n, C, D)$. By [Definition 3.5](#), there exists a channel completion Φ of the Uhlmann transformation W corresponding to the states $|C\rangle, |D\rangle$ such that

$$\text{td}\left((\text{id} \otimes M_x) |C\rangle\langle C|, (\text{id} \otimes \Phi) |C\rangle\langle C|\right) \leq \delta. \quad (5.8)$$

By the triangle inequality

$$\begin{aligned} &\text{td}\left((\text{id} \otimes M_x)(|C\rangle\langle C|), |D\rangle\langle D|\right) \\ &\leq \text{td}\left((\text{id} \otimes M_x)(|C\rangle\langle C|), (\text{id} \otimes \Phi) |C\rangle\langle C|\right) + \text{td}\left((\text{id} \otimes \Phi) |C\rangle\langle C|, (\text{id} \otimes \Phi) |C'\rangle\langle C'|\right) \\ &\quad + \text{td}\left((\text{id} \otimes \Phi) |C'\rangle\langle C'|, |D\rangle\langle D|\right). \end{aligned} \quad (5.9)$$

By [Equation \(5.8\)](#), the first term is at most δ . Using the same argument as above, by the monotonicity of trace distance under quantum channels and the Gentle Measurement Lemma, the second term of [Equation \(5.9\)](#) is at most $2\sqrt{1-\kappa}$. Similarly, the third term of [Equation \(5.9\)](#) is bounded by $3\sqrt{1-\kappa}$ as shown above.

Putting everything together, we can upper bound [Equation \(5.9\)](#) by

$$\text{td}\left((\text{id} \otimes M_x)(|C\rangle\langle C|), |D\rangle\langle D|\right) \leq \delta + 5\sqrt{1-\kappa}.$$

Applying the Fuchs-van de Graaf inequality yields the conclusion of the proposition. \square

Proposition 5.8 indicates that in the average-case setting and the setting of κ close to 1, the η cutoff parameter can be without loss of generality set to 0, as alluded to earlier. This is because Proposition 5.8 shows that solving the distributional versions of UHLMANN or SUCCINCTUHLMANN is equivalent to approximately mapping $|C\rangle$ to $|D\rangle$ while acting only on the second half of the qubits. This second statement, however, is clearly robust to small perturbations: if a quantum algorithm M can approximately map $|C\rangle$ to $|D\rangle$, then it can also approximately map $|C'\rangle$ and $|D'\rangle$ where $|C'\rangle \approx |C\rangle$ and $|D'\rangle \approx |D\rangle$. Thus the subtlety discussed at the beginning of the section about the need for a cutoff parameter η does not arise.

Since we mainly deal with solving UHLMANN or SUCCINCTUHLMANN in the average case and in the high κ regime, we will from now omit mention of the η parameter and implicitly assume it is set to 0. The only place where we explicitly need the η parameter is in Section 7.3, where we sketch how SUCCINCTUHLMANN $_{1,\eta}$ for exponentially small cutoff η is a complete problem for (worst-case) unitaryPSPACE.

Finally, we pose a question about the tightness of Proposition 5.8.

Open Problem 9. Can Proposition 5.8 be improved to give meaningful guarantees when the fidelity parameter κ is bounded away from 1?

Improving it would be helpful when reasoning about Uhlmann transformations for UHLMANN $_{\kappa}$ instances with small κ (for an example of this, see Section 8.2).

6 Structural Results about the Uhlmann Transformation Problem

Having defined the Uhlmann Transformation Problem and its succinct version as unitary synthesis problems, we now prove some structural results about their complexity. Specifically we show that the distributional Uhlmann Transformation Problem is complete for the zero knowledge unitary complexity class avgUnitarySZK $_{\text{HV}}$ defined in Section 4. We also prove a hardness amplification result for the Uhlmann Transformation Problem, which has cryptographic applications as we discuss in Section 8. We then introduce a simple “padding trick” that shows that the complexity of the distributional Uhlmann Transformation Problem is the same for all κ that is polynomially-bounded away from 0 or 1. As discussed in the previous section, since we are only dealing with the distributional Uhlmann Transformation Problem, we set the cutoff parameter η to 0 and omit reference to it.

6.1 Completeness for unitary zero knowledge

In this section we show that DISTUHLMANN $_{1-\text{negl}}$ is complete for the unitary complexity class avgUnitarySZK $_{\text{HV}}$ (see Section 4.3 for the definition of this class). What we mean by this is that for every negligible function $\text{negl}(n)$, the distributional unitary synthesis problem DISTUHLMANN $_{1-\text{negl}}$ is contained in avgUnitarySZK $_{\text{HV}}$, and every problem in avgUnitarySZK $_{\text{HV}}$ is polynomial-time reducible to DISTUHLMANN $_{1-\text{negl}}$ for *some* negligible function $\text{negl}(n)$ (related to the simulation error of the problem).

We first introduce the notation employed throughout this section. A register block $R_{[i:j]}$ is an ordered collection of registers, denoted as $R_{[i:j]} := R_i R_{i+1} \dots R_j$, with the size of the collection defined as, $|R_{[i:j]}| := j - i + 1$. When the first index is omitted, the collection is taken to start at $i = 1$, so $R_{[m]} = R_1 \dots R_m$. For a permutation π on $|R_{[0:m]}|$ elements, we use P_π to denote the

unitary for a “block permutation” that permutes the registers inside a block in the obvious way, and $\mathcal{P}_\pi(\cdot) = P_\pi(\cdot)P_\pi^\dagger$ the associated channel.

We first show that for all negligible functions $\mu(n)$, $\text{DISTUHLMANN}_{1-\mu}$ is contained in $\text{avgUnitarySZK}_{\text{HV}}$ in [Proposition 6.1](#). Then, in [Proposition 6.5](#) we show that $\text{DISTUHLMANN}_{1-\text{negl}}$ is $\text{avgUnitarySZK}_{\text{HV}}$ -hard, i.e. that any problem in $\text{avgUnitarySZK}_{\text{HV}}$ polynomial-time reduces to $\text{DISTUHLMANN}_{1-\epsilon}$ for some negligible function $\epsilon(n)$. In [Theorem 6.7](#), we combine these two statements to conclude that $\text{DISTUHLMANN}_{1-\text{negl}}$ is complete for $\text{avgUnitarySZK}_{\text{HV}}$.

6.1.1 $\text{DISTUHLMANN}_{1-\text{negl}} \in \text{avgUnitarySZK}_{\text{HV}}$

Proposition 6.1. *$\text{DISTUHLMANN}_{1-\mu} \in \text{avgUnitarySZK}_{\text{HV}}$ for all negligible functions $\mu(n)$.*

Proof. Let $\mu(n)$ be a negligible function. We show that for all polynomials q , $\text{DISTUHLMANN}_{1-\mu} \in \text{avgUnitarySZK}_{\text{HV}, 1-\nu, 1/2, 1/q}$ for $\nu(n) = 32q(n)^2\mu(n)$; since $\nu(n)$ is still negligible, this suffices to show the proposition. For this, we need to design a protocol that satisfies the conditions from [Definition 4.3](#). Consider the following protocol ([Protocol 1](#)).

Protocol 1. $\text{avgUnitarySZK}_{\text{HV}, 1-\nu, \frac{1}{2}, 1/q}$ verifier for $\text{DISTUHLMANN}_{1-\mu}$

Input: A valid $\text{UHLMANN}_{1-\mu}$ instance $x = (1^n, C, D)$, and an n qubit quantum register \mathbf{B}_0 .

1. Let $m = 32q(n)^2$. Prepare the state $\bigotimes_{i=1}^m |C\rangle_{\mathbf{A}_i \mathbf{B}_i}$. Select a permutation $\pi \in S_{m+1}$ uniformly at random, and apply \mathcal{P}_π to the register block $\mathbf{B}_{[0:m]} = \mathbf{B}_0 \mathbf{B}_1 \dots \mathbf{B}_m$. Send the block $\mathbf{B}_{[0:m]}$ to the prover.
2. The verifier receives register block \mathbf{B} from the prover. Then:
 - (a) Apply $\mathcal{P}_{\pi^{-1}}$ to $\mathbf{B}_{[0:m]}$.
 - (b) Apply $(D^\dagger)^{\otimes m}$ to registers $\mathbf{A}\mathbf{B}_{[m]}$, and measure in the computational basis. If the outcome is the all-0 string for all i , accept and output the \mathbf{B}_0 register. Otherwise, reject.

Note that all registers, \mathbf{B}_i and \mathbf{A}_i , used in the protocol have a dependence on the instance x , but as the instance x is fixed at the beginning of the protocol, we omit explicitly writing this dependence. [Protocol 1](#) describes the actions of the verifier. To satisfy [Definition 4.3](#), we also need to define an honest prover P^* , who behaves as follows: let $\Phi(\cdot)$ be an arbitrary channel completion of the canonical Uhlmann partial isometry for (C, D) . Upon receipt of the registers $\mathbf{B}_{[0:m]} = \mathbf{B}_0 \dots \mathbf{B}_m$, the honest prover P^* applies $\Phi(\cdot)$ to each register \mathbf{B}_i individually and sends back the resulting state.

We will show that [Protocol 1](#) with the honest prover P^* satisfies the three properties from [Definition 4.3](#). Since the proofs are slightly involved, we separate them out into individual lemmas, which we prove below using the same notation and parameter settings introduced here:

1. The honest prover P^* needs to succeed with probability at least $1 - \nu(n)$ ([Lemma 6.2](#)).
2. The verifier needs to satisfy the soundness condition of an $\text{avgUnitaryQIP}_{1-\nu, 1/2, 1/q}$ protocol ([Lemma 6.3](#)).

3. The protocol needs to satisfy the zero-knowledge condition (Lemma 6.4).

Combined, Lemmas 6.2 to 6.4 imply Proposition 6.1. \square

We now prove the individual lemmas referenced in the proof of Proposition 6.1.

Lemma 6.2 (avgUnitaryQIP completeness). *For all valid UHLMANN $_{1-\mu}$ instances $x = (1^n, C, D)$, for sufficiently large n the honest prover P^* satisfies*

$$\Pr[V_x(|C\rangle_{A_0 B_0}) \Leftarrow P^*] \geq 1 - \nu(n).$$

Proof. We want to show that the honest prover, who applies the optimal Uhlmann isometry, is accepted by the verifier with probability at least $1 - \nu$. Let W_B be the optimal Uhlmann partial isometry for the circuit pair (C, D) . Because we are considering an UHLMANN $_{1-\mu}$ instance we have that

$$1 - \mu(n) \leq |\langle D | (\text{id}_A \otimes W_B) |C\rangle|^2.$$

The honest prover action on the product state $|C\rangle^{\otimes m+1}$ is exactly given by $W_B^{\otimes m+1}$. Because the fidelity is multiplicative under tensor products, the probability of the verifier accepting is given by

$$\left(|\langle D | (\text{id}_A \otimes (W)_B) |C\rangle|^2 \right)^m \geq (1 - \mu(n))^m \geq 1 - m \cdot \mu(n) = 1 - \nu(n).$$

Additionally, after interacting with the honest prover and conditioned on accepting, the verifier has successfully applied W to the input state. \square

Lemma 6.3 (avgUnitaryQIP soundness). *For all valid UHLMANN $_{1-\mu}$ instances $x = (1^n, C, D)$, for sufficiently large n , for all quantum provers P , there exists a channel completion Φ_x of U_x such that*

$$\text{if } \Pr[V_x(|C\rangle) \Leftarrow P \text{ accepts}] \geq \frac{1}{2} \quad \text{then} \quad \text{td}(\sigma, (\Phi_x \otimes \text{id}) |C\rangle\langle C|) \leq 1/q(n),$$

where σ denotes the output of $V_x(|C\rangle) \Leftarrow P$, conditioned on V_x accepting.

Proof. We argue that soundness holds in three steps. We first show that by applying the block permutation P_π and inverting it after the interaction with the prover, the verifier has forced the state after interacting with the prover to be a symmetric state across the registers $\mathbf{AB}_{[0:m]}$. Second, we show that measuring $|D\rangle\langle D|$ on the m decoy registers and accepting yields a state close to measuring $|D\rangle\langle D|$ on all $m+1$ registers. Finally we apply the Gentle Measurement Lemma to show that, conditioned on accepting, the verifier has a state close to the optimal Uhlmann unitary applied to the input state.

We begin by expressing the state of the verifier's registers after interacting with the prover and undoing the permutation in step 2(a). Assume that the verifier's quantum input is the B_0 register of $|C\rangle_{A_0 B_0}$ (the distributional input). In the protocol, the verifier will first apply a random permutation on $\mathbf{B}_{[0:m]}$; then the prover will perform some arbitrary action on $\mathbf{B}_{[0:m]}$, represented by a quantum channel $\Lambda_{\mathbf{B}_{[0:m]}}$; and finally the verifier will undo the random permutation from the first step. Treating A_0 as the purification register of the verifier's quantum input, the state of the registers $\mathbf{B}_{[0:m]} A_{[0:m]}$ after these three steps is given by

$$\rho^* := \mathbb{E}_{\pi \in S_{m+1}} \left((\mathcal{P}_{\pi^{-1}})_{\mathbf{B}_{[0:m]}} \circ \Lambda_{\mathbf{B}_{[0:m]}} \circ (\mathcal{P}_\pi)_{\mathbf{B}_{[0:m]}} \otimes \text{id}_{A_{[0:m]}} \right) (|C\rangle\langle C|^{\otimes m+1}).$$

Note that in addition to permuting the $\mathbf{B}_{[0:m]}$ registers and then permuting them back, we can extend the permutation to include the $\mathbf{A}_{[0:m]}$ registers, too. This is because $(\mathcal{P}_\pi)_{\mathbf{AB}_{[0:m]}} = (\mathcal{P}_\pi)_{\mathbf{A}_{[0:m]}} \otimes (\mathcal{P}_\pi)_{\mathbf{B}_{[0:m]}}$, and since Λ does not act on $\mathbf{A}_{[0:m]}$, the permutations on $\mathbf{A}_{[0:m]}$ simply cancel. Therefore,

$$\rho^* = \mathbb{E}_{\pi \in S_{m+1}} \left((\mathcal{P}_{\pi^{-1}})_{\mathbf{AB}_{[0:m]}} \circ (\Lambda_{\mathbf{B}_{[0:m]}} \otimes \text{id}_{\mathbf{A}_{[0:m]}}) \circ (\mathcal{P}_\pi)_{\mathbf{AB}_{[0:m]}} \right) (|C\rangle\langle C|^{\otimes m+1}).$$

This state is clearly permutation-invariant, i.e. $(\mathcal{P}_\sigma)_{\mathbf{AB}_{[0:m]}}(\rho^*) = \rho^*$ for any permutation $\sigma \in S_{m+1}$.

In the last step of the protocol, the verifier performs the projective measurement $\{\Pi^{(0)} = |D\rangle\langle D|, \Pi^{(1)} = \text{id} - \Pi^{(0)}\}$ on each of the systems in $\mathbf{AB}_{[m]}$ and accepts if all of them yield outcome 0. We define random variables X_0, \dots, X_m with the joint distribution

$$\Pr[X_0 = b_0 \wedge \dots \wedge X_m = b_m] = \text{Tr} \left(\left(\bigotimes_{i=0}^m \Pi_{\mathbf{A}_i \mathbf{B}_i}^{(b_i)} \right) \rho^* \right),$$

i.e. X_i corresponds to the verifier's measurement on the i -th system. Since we are assuming $\Pr[V_x(|C\rangle) \stackrel{P}{\text{accepts}}] \geq \frac{1}{2}$, we have that $\Pr[(X_1, \dots, X_m) = (0, \dots, 0)] \geq 1/2$. Intuitively, the “bad outcome” is that the verifier receives outcome 0 for X_1, \dots, X_m , but if the verifier had measured the 0-th system, he would have received outcome 1. We can bound the probability of this happening as

$$\begin{aligned} \Pr[X_0 = 1 | (X_1, \dots, X_m) = (0, \dots, 0)] &\leq 2 \Pr[X_0 = 1 \wedge (X_1, \dots, X_m) = (0, \dots, 0)] \\ &\leq \frac{2}{m+1} \sum_{i=0}^{m+1} \Pr[X_i = 1 \wedge (X_j)_{j \neq i} = (0, \dots, 0)] \\ &\leq \frac{2}{m+1}. \end{aligned} \tag{6.1}$$

For the first inequality, we used the definition of conditional probability and $\Pr[(X_1, \dots, X_m) = (0, \dots, 0)] \geq 1/2$. For the second inequality, we used the fact that due to the permutation-invariance of ρ^* , the random variables (X_0, \dots, X_m) are exchangeable (i.e. their joint distribution is invariant under permutations), and for the last inequality we used that $(X_i = 1 \wedge (X_j)_{j \neq i} = (0, \dots, 0))$ are disjoint events, so the sum of their probabilities is at most 1.

Denoting the verifier's output state conditioned on acceptance by σ , [Equation \(6.1\)](#) tells us that

$$F(\sigma, |D\rangle\langle D|) = \text{Tr}(|D\rangle\langle D| \sigma)^2 \geq \left(1 - \frac{2}{m+1}\right)^2 \geq 1 - \frac{4}{m+1}.$$

By Fuchs-van de Graaf we have

$$\text{td}(\sigma, |D\rangle\langle D|) \leq \sqrt{\frac{4}{m+1}}.$$

Then [Equation \(5.5\)](#) in the proof of [Proposition 5.8](#) shows that for all channel completions Φ_x of U_x , we have that

$$\text{td}((\Phi_x \otimes \text{id}) |C\rangle\langle C|, |D\rangle\langle D|) \leq 5\sqrt{\mu(n)}$$

so therefore

$$\text{td}\left(\sigma, (\Phi_x \otimes \text{id}) |C\rangle\langle C|\right) \leq \sqrt{\frac{4}{m+1}} + 5\sqrt{\mu(n)}.$$

By the choice of $m = 32q(n)^2$, since $\mu(n)$ is negligible, for sufficiently large n this is at most $1/q(n)$ as desired. This completes the proof of [Lemma 6.3](#). \square

Lemma 6.4 (avgUnitarySZK_{HV} zero-knowledge). *There exists a negligible function negl and a polynomial-time simulator that, on input $(x, 1)$,¹² outputs a state ρ satisfying*

$$\text{td}(\rho, \sigma_{x,1}) \leq \text{negl}(n),$$

where $\sigma_{x,1}$ is the reduced density matrix of V_x^* 's private register and the purifying register of the input, immediately after interacting with the honest prover P^* .

Proof. The simulator simply outputs the state $|D\rangle^{\otimes m+1}$. Because the fidelity is being measured between product states, the fidelity between the simulator output and the state of the verifier after interacting with the honest prover is

$$\left(|\langle D | (\text{id}_A \otimes W_B) |C\rangle|^2\right)^{m+1} \geq 1 - (m+1)\mu(n).$$

By the standard relationship between trace distance and fidelity, the trace distance between the simulators output and the state of the verifier after interacting with the prover is at most $\sqrt{(m+1)\mu(n)}$. Since m is a polynomial in n , $\sqrt{(m+1)\mu(n)}$ is also a negligible function in n , so the simulator satisfies the definition of avgUnitarySZK_{HV}. \square

6.1.2 DISTUHLMANN_{1-negl} is avgUnitarySZK_{HV}-hard

Now we show that all problems in avgUnitarySZK_{HV} reduce to DISTUHLMANN_{1- ν} for *some* negligible $\nu(n)$ (which depends on the avgUnitarySZK_{HV}-problem). We highlight the annoying fact that it is not known if there is a single negligible function $\nu^*(n)$ such that DISTUHLMANN_{1- ν^*} is hard for avgUnitarySZK_{HV}. In particular, the value of ν will depend on the error to which the simulator can prepare the verifier's state.

Open Problem 10. Does there exist a negligible function μ such that every distributional unitary synthesis problem in avgUnitarySZK_{HV} has a protocol, (V, P^*, Sim) , such that Sim prepares the verifiers state to within trace distance error μ ?

If the above problem was answered in the affirmative, then it would directly imply that there is a single distributional unitary synthesis problem that is complete for avgUnitarySZK_{HV}. Note that the number of rounds in the algorithm does not matter because the Padding Trick (Section 6.3) can be used to transform a protocol with simulator error δ to one with simulator error δ/p for any polynomial p . This question is tightly related to another broader difference between SZK_{HV} and avgUnitarySZK_{HV}, which will be discussed in more detail in Section 6.4.

Proposition 6.5. *Let $(\mathcal{U} = (U_x)_x, \Psi = (|\psi_x\rangle)_x)$ be a distributional unitary synthesis problem in avgUnitarySZK_{HV}. Then there exists a negligible function ν such that (\mathcal{U}, Ψ) polynomial-time reduces to DISTUHLMANN_{1- ν} .*

Proof. By Definition 4.3, for all polynomials q there exists a negligible function μ such that $(\mathcal{U}, \Psi) \in \text{avgUnitarySZK}_{\text{HV}, 1-\mu, 1/2, 1/q}$. Let $V^* = (V_x^*)_x$ be the honest, r -round avgUnitarySZK_{HV, 1- μ , 1/2, 1/q} verifier for (\mathcal{U}, Ψ) , and let $(V_{x,i})_{i=1}^{r+1}$ be the unitaries that this verifier applies throughout the protocol, where $V_{x,i}$ is the unitary applied in the i -th round. $V_{x,i}$ acts on a workspace register F_{i-1} and a prover message Q_{i-1} , and outputs a pair of registers $F_i Q_i$. Additionally, $V_{x,0}$ takes in a quantum

¹²Note that there is only 1 interaction with the prover in the protocol.

input in register A, and an ancilla register R. See Figure 6.1.2 for an image describing how the verifier and prover interact.

Let Sim be the zero-knowledge simulator for V^* , and let ϵ be the negligible function such that Sim , when run on input (x, i) , outputs a state within $\epsilon(|x|)$ of the reduced density matrix of V^* immediately after the i -th round of interaction with the honest prover. Since Sim is a polynomial time quantum algorithm, for all x, i there exists a polynomial time unitary circuit $\text{Sim}_{x,i}$ that implements $\text{Sim}(x, i)$ (i.e. in $\text{Sim}_{x,i}$, the input x, i is hard-coded). Since the circuit $\text{Sim}_{x,i}$ implements a unitary while $\text{Sim}(x, i)$ might perform measurements and trace out registers, we need to assume that $\text{Sim}_{x,i}$ might require an additional (private) register P that is traced out by $\text{Sim}(x, i)$. In this section, we abuse notation and interchange the unitary implemented by $\text{Sim}_{x,i}$ with the explicit circuit description of $\text{Sim}_{x,i}$ wherever it is clear from context which one is intended. We emphasize that $\text{Sim}_{x,i}$ is a fixed quantum circuit that acts only on $|0\rangle$, and produces a purification of the state that Sim would produce when run on input (x, i) . Every $\text{Sim}_{x,i}$ acts on registers $F_i Q_i P B$, where F_i and Q_i are the verifiers registers, B is the purification register for the initial input (initially in AB), and P is a purification register for the simulator, as explained before. Since Sim produces the state *after* the interaction, we need to define an additional circuit that prepares the initial state of the system, which we will call $\text{Sim}_{x,0}$. Since the initial state is in stateBQP , there is a polynomial-time circuit such that $(\text{Sim}_{x,0})_{AB} \otimes \text{id}_R |0\rangle_{ABR} = |\psi_x\rangle \otimes |0\rangle_R$, which prepares the initial state of the verifier when run on $|0\rangle_{ABR}$ (recall that the initial state of the system includes an ancilla register R for the verifier). We relabel the registers AR to be $F_0 Q_0$ so that $\text{Sim}_{x,0}$ follows the pattern of the other $\text{Sim}_{x,i}$. Assume that every $\text{Sim}_{x,i}$ uses a private register of the same size, and that the private register has polynomial in $|x|$ many qubits, which we can achieve by padding every $\text{Sim}_{x,i}$ with extra ancilla qubits.

We now define a quantum query circuit making exactly r calls to a $\text{DISTUHLMANN}_{1-2\epsilon^2}$ oracle. The classical label for the i -th Uhlmann oracle will be (an explicit classical description of) the following pair (A_i, B_i) of polynomial-time quantum circuits.

$$\begin{aligned} A_i &= (V_{x,i})_{F_{i-1} Q_{i-1}} \circ (\text{Sim}_{x,i-1})_{F_{i-1} Q_{i-1} P B} \\ B_i &= (\text{Sim}_{x,i})_{F_i Q_i P B} \end{aligned}$$

Both of these are polynomial time quantum circuits. A_i is a unitary that, when applied to $|0\rangle_{F_{i-1} Q_{i-1} P B}$, prepares a purification of the verifier's state immediately before the i -th round of interaction. B_i is a unitary that, when applied to $|0\rangle_{F_i Q_i P B}$, prepares the verifier's state after the i -th round of interaction with the prover. We first show that (A_i, B_i) are a valid $\text{UHLMANN}_{1-2\epsilon^2}$ instance. Let Φ_i be the channel representing the honest prover in the i -th interaction acting on Q_i . Let $\sigma_{x,i}$ be reduced the state of the verifier registers (and hidden input register B) immediately after the i -th interaction with the honest prover. By the definition of Sim , we have that

$$\text{td}(\text{Tr}_P(|A_i\rangle\langle A_i|), V_{x,i} \sigma_{x,i-1} V_{x,i}^\dagger) \leq \epsilon(|x|) \text{ and} \quad (6.2)$$

$$\text{td}(\text{Tr}_P(|B_i\rangle\langle B_i|), \sigma_{x,i}) \leq \epsilon(|x|). \quad (6.3)$$

We also have that the state of the verifier after the i -th round of interaction can be attained by applying the verifiers unitary $V_{x,i}$ and the provers channel Φ_i to the state after the $(i-1)$ -th round, formally

$$((\Phi_i)_{Q_i} \otimes \text{id})(V_{x,i} \sigma_{x,i-1} V_{x,i}^\dagger) = \sigma_{x,i}.$$

Fix an i , and let ρ_A and ρ_B be the reduced states of $|A_i\rangle\langle A_i|$ and $|B_i\rangle\langle B_i|$ on $F_i\mathbf{B}$. We have that

$$\begin{aligned}
F(\rho_A, \rho_B) &\geq F(((\Phi_i)_{\mathbf{Q}_i} \otimes I_{F_i\mathbf{B}}) (\text{Tr}_{\mathbf{P}}(|A_i\rangle\langle A_i|)), \text{Tr}_{\mathbf{P}}(|B_i\rangle\langle B_i|)) \\
&\geq 1 - \text{td}(((\Phi_i)_{\mathbf{Q}_i} \otimes I_{F_i\mathbf{B}}) (\text{Tr}_{\mathbf{P}}(|A_i\rangle\langle A_i|)), \text{Tr}_{\mathbf{P}}(|B_i\rangle\langle B_i|))^2 \\
&\geq 1 - \text{td}(((\Phi_i)_{\mathbf{Q}_i} \otimes I_{F_i\mathbf{B}}) (V_{x,i}\sigma_{x,i-1}V_{x,i}^\dagger), \text{Tr}_{\mathbf{P}}(|B_i\rangle\langle B_i|))^2 - \epsilon^2(|x|) \\
&\geq 1 - \text{td}(((\Phi_i)_{\mathbf{Q}_i} \otimes I_{F_i\mathbf{B}}) (V_{x,i}\sigma_{x,i-1}V_{x,i}^\dagger), \sigma_{x,i})^2 - 2\epsilon(|x|)^2 \\
&= 1 - 2\epsilon^2(|x|).
\end{aligned}$$

Here the first line holds because the states on the right are extensions of the states ρ_A and ρ_B . Because Φ_i acts only on \mathbf{Q}_i , the reduced state of the left hand state on $F_i\mathbf{B}$ is the same as $|A_i\rangle\langle A_i|$. The subsequent lines follow because the trace distance obeys the triangle inequality and contracts under trace preserving channels, using the inequalities from [Equations \(6.2\) and \(6.3\)](#). Note that this means the Uhlmann unitary that acts on \mathbf{Q}_i and \mathbf{P} , since we only showed that the reduced states on $F_i\mathbf{B}$ have high fidelity with each other. Now consider the following $\text{avgUnitaryBQP}^{\text{DISTUHLMANN}_{1-2\epsilon^2}}$ query algorithm protocol for (\mathcal{U}, Ψ) .

Algorithm 1. $\text{avgUnitaryBQP}_{3/q(n)}^{\text{DISTUHLMANN}_{1-2\epsilon^2}}$ query algorithm for (\mathcal{U}, Ψ)

Input: Classical string x specifying U_x and quantum register \mathbf{A} .

1. Initialize $i \leftarrow 1$, register $\mathbf{R} \leftarrow |0\rangle\langle 0|$ and relabel $F_0\mathbf{Q}_0 \leftarrow \mathbf{AR}$. While $i \leq r$:
 - (a) Run $V_{x,i}$ on $F_{i-1}\mathbf{Q}_{i-1}$ to get a state on $F_i\mathbf{Q}_i$, if $V_{x,i}$ rejects, abort and output $|0\rangle_{\mathbf{A}}$.
 - (b) Call $\text{DISTUHLMANN}_{1-2\epsilon^2}$ oracle on the instance corresponding to an explicit circuit representation of (A_i, B_i) , and quantum register $\mathbf{Q}_i\mathbf{P}$.
 - (c) $i \leftarrow i + 1$.
2. Run $V_{x,r+1}$ on $F_r\mathbf{Q}_r$ to get a state on \mathbf{AR} .
3. Output register \mathbf{A} .

In order to show that (\mathcal{U}, Ψ) polynomial-time reduces to $\text{DISTUHLMANN}_{1-2\epsilon^2}$, we need to show that for all polynomials q , there exists another polynomial p such that all $1/p$ -error average case instantiations of [Algorithm 1](#) with $\text{DISTUHLMANN}_{1-2\epsilon^2}$ implement (\mathcal{U}, Φ) .

Claim 6.6. Fix a polynomial q , and let $p(n) = rq(n)$ (where r is the number of rounds as before). Then all $1/p$ -error average case instantiations of [Algorithm 1](#) with $\text{DISTUHLMANN}_{1-2\epsilon^2}$ implement (\mathcal{U}, Φ) to average case error $3/q(n)$.

Proof. We first show by induction that for every $i \leq r$, the input to the i -th $\text{DISTUHLMANN}_{1-2\epsilon^2}$ oracle call is at most $(i-1) \cdot (1/p(n) + \epsilon\sqrt{2})$ in trace distance from the ‘‘correct’’ distributional state $|A_i\rangle := A_i|0\rangle$ for which the guarantee of the DISTUHLMANN holds.

The input to the first call to $\text{DISTUHLMANN}_{1-2\epsilon^2}$ is exactly $|A_0\rangle = (V_{x,1})_{\mathbf{A}}|\psi_x\rangle_{\mathbf{AB}}$, so the trace distance error before the 1-st call is 0.

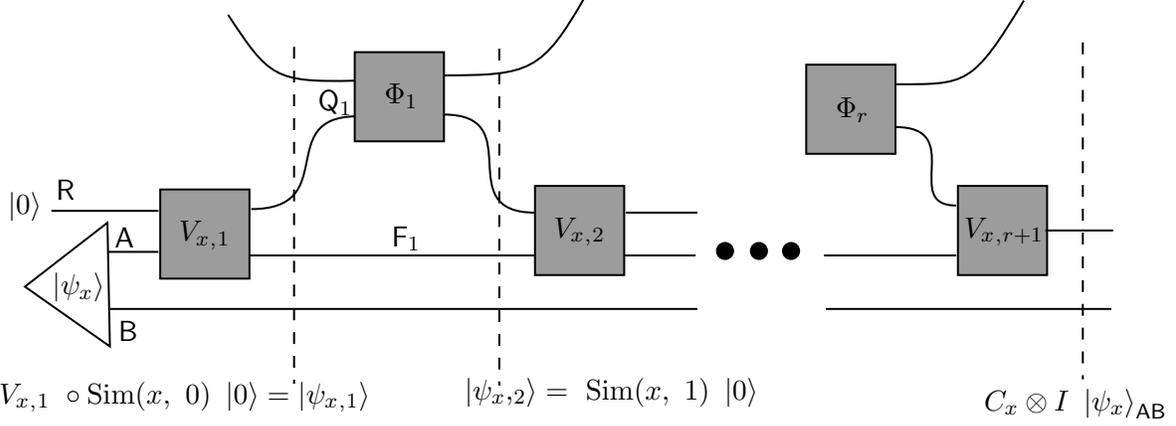


Figure 2: A avgUnitarySZK protocol with r rounds. The prover receives the A register of $|\psi\rangle_{AB}$. Every round of interaction consists of the verifier applying $V_{x,i}$ to $F_{i-1}Q_{i-1}$ to get F_iQ_i and then exchanging Q_i with the prover. The first and final rounds are special. In the first round, the verifier takes in A and a workspace R, and in the final round the verifier either accepts or rejects, and outputs a register. Sim can be used to generate the state after every interacting with the prover.

Now assume that the claim is true up to the i -th call to $\text{DISTUHLMANN}_{1-2\epsilon^2}$. Let ρ_i be the input to the i -th call to $\text{DISTUHLMANN}_{1-2\epsilon^2}$. Let $\Phi_{(A_i, B_i)}$ be the channel that the i -th call to the $\text{DISTUHLMANN}_{1-2\epsilon^2}$ oracle implements, and let W_i be the optimal Uhlmann unitary for instance (A_i, B_i) . By assumption we have that

$$\begin{aligned}
\text{td}(\Phi_{(A_i, B_i)}(\rho_i), |B_i\rangle\langle B_i|) &\leq \text{td}(\Phi_{(A_i, B_i)}(\rho_i), \Phi_{(A_i, B_i)}(|A_i\rangle\langle A_i|) + \text{td}(\Phi_{(A_i, B_i)}(|A_i\rangle\langle A_i|), |B_i\rangle\langle B_i|) \\
&\leq (i-1)(1/p(n) + \epsilon\sqrt{2}) + \text{td}(\Phi_{(A_i, B_i)}(A_i |0\rangle\langle 0| A_i^\dagger), B_i |0\rangle\langle 0| B_i^\dagger) \\
&\leq (i-1)(1/p(n) + \epsilon\sqrt{2}) + 1/p(n) + \text{td}(W_i |A_i\rangle\langle A_i| W_i^\dagger, |B_i\rangle\langle B_i|) \\
&\leq i(1/p(n) + \epsilon\sqrt{2})
\end{aligned}$$

Here we first apply the induction hypothesis and the fact that quantum channels decrease trace distance. Then we use the fact that $\Phi_{(A_i, B_i)}$ is a $1/p(n)$ -error average case solver. Finally we use the fact that (A_i, B_i) is a valid $\text{DISTUHLMANN}_{1-2\epsilon^2}$ instance, so the states $W_i |A_i\rangle$ and $|B_i\rangle$ are within $\epsilon\sqrt{2}$ in trace distance. The state that the query algorithm gives as input to the oracle is

$$V_{x,i+1}(\Phi_{(A_i, B_i)}(\rho_i)),$$

which is within $i(1/p(n) + \epsilon\sqrt{2})$ trace distance of $|A_{i+1}\rangle = V_{x,i+1} |B_i\rangle$ because unitaries preserve trace distance. By induction, for all i , the input to the i -th oracle call in the protocol is within $(i-1) \cdot (1/p(n) + \epsilon\sqrt{2})$. Following the same inequalities, the *output* of the final oracle call satisfies

$$\text{td}(\Phi_{(A_r, B_r)}(\rho_r), |B_r\rangle\langle B_r|) \leq r(1/p(n) + \epsilon\sqrt{2}).$$

Let $\sigma_{x,r}$ be the state of the verifier after the final interaction with the honest prover. Then by the definition of the simulator, we have that

$$\text{td}(\Phi_{(A_r, B_r)}(\rho_r), \sigma_{x,r}) \leq r/p(n) + (r+1)\epsilon\sqrt{2}.$$

By the definition of the honest prover, there exists a negligible function μ such that the honest prover is accepted with probability $1 - \mu$, and conditioned on accepting the verifier outputs a state within $1/q(n)$ of $U_x |\psi_x\rangle\langle\psi_x| U_x^\dagger$ in trace distance. Thus we have that

$$\text{td}(V_{x,r+1}\sigma_{x,r}V_{x,r+1}^\dagger, U_x |\psi_x\rangle\langle\psi_x| U_x^\dagger) \leq \mu + 1/q.$$

Combining everything we have that

$$\begin{aligned} & \text{td}(V_{x,r+1}\Phi_{(A_r,B_r)}(\rho_r)V_{x,r+1}^\dagger, U_x |\psi_x\rangle\langle\psi_x| U_x^\dagger) \\ & \leq \text{td}(V_{x,r+1}\sigma_{x,r}V_{x,r+1}^\dagger, U_x |\psi_x\rangle\langle\psi_x| U_x^\dagger) + r(1/p(n) + \epsilon\sqrt{2}) \\ & \leq 1/q + \mu + r(1/p + \epsilon\sqrt{2}) \\ & \leq 2/q + r\epsilon\sqrt{2} + \mu \\ & \leq 3/q. \end{aligned}$$

Here we use the fact that $p = rq$, and since ϵ and μ are negligible, for sufficiently large n , $r\epsilon\sqrt{2} + \mu \leq 1/q$. \square

Because $(\mathcal{U}, \Psi) \in \text{avgUnitarySZK}_{\text{HV}}$, there exists a negligible function ϵ such that for all polynomials q' , there exists a verifier that implements (\mathcal{U}, Ψ) with average case error $1/3q'$, and a simulator that makes simulation error ϵ . Thus for all polynomials q' , there exists a polynomial time quantum query algorithm, specified by [Algorithm 1](#) when V is taken to have average case error $1/3q'$, and another polynomial $p = rq'$, that achieves average case error $1/q'$ when instantiated with $1/p$ -error average case instantiations of $\text{DISTUHLMANN}_{1-2\epsilon^2}$. In other words, (\mathcal{U}, Ψ) polynomial-time reduces to $\text{DISTUHLMANN}_{1-2\epsilon^2}$. \square

We summarise the results of [Proposition 6.1](#) and [Proposition 6.5](#) in the following theorem, which shows that $\text{DISTUHLMANN}_{1-\text{negl}}$ is “almost complete” for avgUnitarySZK up to the aforementioned issue that we cannot find a single negligible function ν such that avgUnitarySZK reduces to $\text{DISTUHLMANN}_{1-\nu}$.

Theorem 6.7. *For all negligible functions μ , $\text{DISTUHLMANN}_{1-\mu} \in \text{avgUnitarySZK}_{\text{HV}}$, and for all distributional unitary synthesis problems (\mathcal{U}, Ψ) , there exists a negligible function ν such that (\mathcal{U}, Ψ) reduces to $\text{DISTUHLMANN}_{1-\nu}$.*

6.2 Hardness amplification

In this section, we prove a hardness amplification result for the Uhlmann Transformation Problem, which roughly states that if it is hard to implement DISTUHLMANN in polynomial time (i.e., $\text{DISTUHLMANN} \notin \text{avgUnitaryBQP}$), then in fact it is hard to implement DISTUHLMANN even with large average case error approaching 1. This hardness amplification statement has applications to amplifying the security of quantum commitment schemes as we show in [Section 8](#).

Theorem 6.8. *The following two statements are equivalent:*

1. For all negligible functions $\epsilon(n)$, $\text{DISTUHLMANN}_{1-\epsilon} \in \text{avgUnitaryBQP}$ (resp. $\text{avgUnitaryBQP}/\text{poly}$).

2. For all negligible functions $\epsilon(n)$, $\text{DISTUHLMANN}_{1-\epsilon} \in \text{avgUnitaryBQP}_{1-\xi}$ (resp. $\text{avgUnitaryBQP}/\text{poly}_{1-\xi}$), where $\xi(n) = n^{-1/16}$.

While [Theorem 6.8](#) will be useful, it is not the strongest possible amplification statement one would hope to prove: one could hope to show that instead of just suppressing the error to an inverse polynomial, it can actually be suppressed to an inverse exponential. We call this “strong amplification” and leave it as an open problem:

Open Problem 11. Can strong amplification be proved? In other words, does solving the Uhlmann transformation problem with inverse polynomial error imply being able to solve it with inverse exponential error?

Strong amplification for Uhlmann would also have ramifications for the question of whether quantum commitments with weak security can be boosted to commitments with strong security (see [Conjecture 8.9](#)). This would be of independent interest for quantum cryptography.

We first give an overview of the proof of [Theorem 6.8](#). Recall from [Definition 3.10](#) that $\text{avgUnitaryBQP}_\delta$ denotes the class of distributional unitary synthesis problems that can be implemented with average case error δ , and that $\text{DISTUHLMANN}_{1-\epsilon} \in \text{avgUnitaryBQP}$ means that for all inverse polynomials δ , $\text{DISTUHLMANN}_{1-\epsilon} \in \text{avgUnitaryBQP}_\delta$.

The “only if” direction of the theorem is immediate: by definition, for $0 \leq \delta \leq \delta' \leq 1$ we have $\text{avgUnitaryBQP}_\delta \subseteq \text{avgUnitaryBQP}_{\delta'}$.

For the “if” direction, the idea is to reduce implementing the Uhlmann transformation U_x corresponding to a valid Uhlmann instance $x = (1^n, C, D)$ to the task of implementing the Uhlmann transformation for the *parallel repetition* of the instance, which we denote by $x^{\otimes k} = (1^{nk}, C^{\otimes k}, D^{\otimes k})$ for some integer k . If the circuits C, D acted on registers AB , then the circuits $C^{\otimes k}, D^{\otimes k}$ act on k copies denoted by $\text{A}_1\text{B}_1, \dots, \text{A}_k\text{B}_k$, and output the states $|C\rangle^{\otimes k}, |D\rangle^{\otimes k}$. What we show is that being able to implement the repeated Uhlmann transformation with error very close to 1 can be turned into a way of implementing the original Uhlmann transformation U_x with very small error. Put another way, if it was hard to implement the original Uhlmann transformation U_x almost exactly, then it is still hard to implement the repeated Uhlmann transformation even approximately. We abstract this reduction out in the following Lemma:

Lemma 6.9. *Let C, D be unitary circuits such that the states $|C\rangle := C|0\dots 0\rangle, |D\rangle := D|0\dots 0\rangle$ are bipartite states on registers AB . Let $k \in \mathbb{N}$ and let $|C\rangle^{\otimes k}, |D\rangle^{\otimes k}$ be states on registers $\text{A}_{[k]}$ and $\text{B}_{[k]}$ respectively. Suppose there is a quantum circuit R acting on register $\text{B}_{[k]}$ such that*

$$F\left((\text{id} \otimes R)(|C\rangle\langle C|^{\otimes k}), |D\rangle\langle D|^{\otimes k}\right) \geq \nu.$$

Then for all $T \in \mathbb{N}$ there exists a quantum circuit M which acts on register B such that

$$F\left((\text{id} \otimes M)(|C\rangle\langle C|), |D\rangle\langle D|\right) \geq 1 - \left(2(1 - \nu)^T + \frac{32T}{\sqrt{k}}\right).$$

and the size of M is at most $\text{poly}(T, |R|, |C|, |D|)$ where $|R|, |C|, |D|$ denote the sizes of circuits R, C, D . Furthermore, if R is an instance of a uniformly generated quantum algorithm, so is M .

Before proving [Lemma 6.9](#), we first show how it implies [Theorem 6.8](#).

Proof of Theorem 6.8. We present the proof for the uniform class avgUnitaryBQP ; the proof for the non-uniform class $\text{avgUnitaryBQP}/\text{poly}$ is entirely analogous.

As mentioned the “only if” direction is trivial, and we focus on the “if” direction. That is, we assume that $\text{DISTUHLMANN}_{1-\mu} \in \text{avgUnitaryBQP}_{1-\xi}$ for all negligible functions $\mu(n)$, where $\xi(n) = n^{-1/16}$, and we aim to show that $\text{DISTUHLMANN}_{1-\mu} \in \text{avgUnitaryBQP}$ for all negligible functions $\mu(n)$.

Fix a negligible function $\epsilon(n)$ and a polynomial $q(n)$. Define the functions

$$k(n) := (nq(n))^8 \quad \delta(n) := k(n)\epsilon(n) \quad T(n) = 2q(n)/\xi(nk(n))^2.$$

Note that $\delta(n)$ is also a negligible function. Therefore by assumption $\text{DISTUHLMANN}_{1-\delta} \subseteq \text{DISTUHLMANN}_{(1-\epsilon)^k} \in \text{avgUnitaryBQP}_{1-\xi}$ there exists a uniform polynomial-time algorithm $R = (R_x)_x$ that implements $\text{DISTUHLMANN}_{1-\delta}$ with average-case error $1 - \xi$.

Fix a $\text{UHLMANN}_{1-\epsilon}$ instance $x = (1^n, C, D)$, and let $k = k(n), \delta = \delta(n), T = T(n)$. We write x^k to denote the parallel repeated instance $(1^{nk}, C^{\otimes k}, D^{\otimes k})$. Note x^k is a valid $\text{UHLMANN}_{(1-\epsilon)^k}$ instance. By the second part of [Proposition 5.8](#), it holds that

$$\mathbb{F}\left((\text{id} \otimes R_{x^k})(|C\rangle\langle C|^{\otimes k}, |D\rangle\langle D|^{\otimes k})\right) \geq \left(\xi(nk) - 5\sqrt{\delta(nk)}\right)^2 \geq \xi(nk)^2 - 10\sqrt{\delta(nk)}. \quad (6.4)$$

Define $\nu = \xi(nk)^2 - 10\sqrt{\delta(nk)}$. Since δ is a negligible function, for sufficiently large n the quantity ν is lower bounded by $\xi(nk)^2/2$. We now invoke [Lemma 6.9](#): there exists a polynomial-time quantum algorithm $M = (M_x)_x$ such that for all valid $\text{UHLMANN}_{1-\epsilon}$ instances $x = (1^n, C, D)$,

$$\mathbb{F}\left((\text{id} \otimes M_x)(|C\rangle\langle C|, |D\rangle\langle D|)\right) \geq 1 - \left(2(1 - \nu(n))^{T(n)} + \frac{32T(n)}{\sqrt{k(n)}}\right).$$

By our choice of k, ν, T , we get

$$\begin{aligned} 2(1 - \nu)^T + \frac{32T}{\sqrt{k}} &\leq 2(1 - \xi(nk)^2/2)^{2q(n)/\xi(nk)^2} + \frac{64q(n)}{n^4 \xi(nk)^2 q(n)^4} \\ &\leq 2e^{-q(n)} + \frac{64(nk)^{1/8}}{n^4 q(n)^3} \leq O\left(\frac{1}{q(n)^2}\right), \end{aligned}$$

where in the second line we used the assumption that $1/\xi(nk) \leq (nk)^{1/16}$. Thus we have argued that

$$\mathbb{F}((\text{id} \otimes M_x) |C\rangle\langle C|, |D\rangle\langle D|) \geq 1 - O(1/q(n)^2) \geq 1 - \epsilon(n) - O(1/q(n)^2).$$

Using the first part of [Proposition 5.8](#), we get that the algorithm M_x implements $\text{DISTUHLMANN}_{1-\epsilon}$ with average-case error $O(\sqrt{\epsilon(n)}) + O(1/q(n)) \leq O(1/q(n))$ for sufficiently large n . Since this is true for all polynomials $q(n)$ and all $\text{UHLMANN}_{1-\epsilon}$ instances $x = (1^n, C, D)$, this establishes that $\text{DISTUHLMANN}_{1-\epsilon} \in \text{avgUnitaryBQP}$, as desired. \square

Proof of Lemma 6.9. First, some notation: we write $\mathbf{A}_{-i}, \mathbf{B}_{-i}$ to denote $\mathbf{A}_{[k]}$ without \mathbf{A}_i and $\mathbf{B}_{[k]}$ without \mathbf{B}_i , respectively.

The circuit R is not necessarily unitary as it may trace out or measure qubits, so let \tilde{R} denote the unitary extension of R , i.e., \tilde{R} is the circuit given by R except all the measurements are performed coherently using ancilla qubits. Note that the size of \tilde{R} is at most polynomial in the size of R . The

unitary \tilde{R} acts on registers $B_{[k]}G$ where $B_{[k]}$ is the second register of the state $|C\rangle^{\otimes k}$ and G is an ancilla register.

The algorithm M is presented in [Algorithm 2](#). The algorithm depends on the parameters k, T , and makes calls to the circuits C, D, R . Thus the claim about the circuit size and uniformity of M follow from inspection.

Algorithm 2. *Algorithm M that maps $|C\rangle$ to $|D\rangle$ with small error, given that R maps $|C\rangle^{\otimes k}$ to $|D\rangle^{\otimes k}$ with large error.*

Input: Quantum register B .

1. Sample i uniformly from $[k]$.
2. Initialize registers $A_{-i}B_{-i}$ in the state $|C\rangle^{\otimes k-1}$ and register G in the all-zero state.
3. Relabel the B register as B_i .
4. For $t \in [T]$:
 - (a) Perform the following measurement, which we will call P_{-i} :
 - i. Apply $(C^{\otimes k-1})^\dagger$ to registers $A_{-i}B_{-i}$.
 - ii. Measure whether the $A_{-i}B_{-i}$ registers are in the all-zeroes state.
 - iii. Apply $C^{\otimes k-1}$.
 - (b) Perform the following measurement, which we will call Q_{-i} :
 - i. Apply \tilde{R} to registers $B_{[k]}G$.
 - ii. Apply $(D^{\otimes k-1})^\dagger$ to registers $A_{-i}B_{-i}$.
 - iii. Measure whether the $A_{-i}B_{-i}$ registers are in the all-zeroes state.
 - iv. Apply $D^{\otimes k-1}$.
 - v. Apply \tilde{R}^\dagger to registers $B_{[k]}G$.
 - (c) If the Q_{-i} outcome succeeds (i.e., all-zeroes are measured in step (iii)), then exit loop.
5. Apply \tilde{R} to registers $B_{[k]}G$, and output register B_i .

Define the projectors

$$P := |C\rangle\langle C|_{A_{[k]}B_{[k]}}^{\otimes k} \otimes |0\rangle\langle 0|_G \quad \text{and} \quad Q := \tilde{R}^\dagger \left(|D\rangle\langle D|_{A_{[k]}B_{[k]}}^{\otimes k} \otimes \text{id}_G \right) \tilde{R}.$$

The assumption that R maps $|C\rangle^{\otimes k}$ to have fidelity at least ν with $|D\rangle^{\otimes k}$ can be rewritten as $\text{Tr}(PQ) \geq \nu$. For simplicity assume that $\nu = \text{Tr}(PQ)$ exactly. Let

$$|v\rangle := |C\rangle^{\otimes k} \otimes |0\rangle, \quad |w\rangle := Q|v\rangle / \sqrt{\nu}.$$

The two-dimensional subspace spanned by $|v\rangle$ and $|w\rangle$ defines two additional vectors $|v^\perp\rangle, |w^\perp\rangle$

where

$$\begin{aligned} |v\rangle &= \sqrt{\nu} |w\rangle + \sqrt{1-\nu} |w^\perp\rangle, & |v^\perp\rangle &= \sqrt{1-\nu} |w\rangle - \sqrt{\nu} |w^\perp\rangle \\ |w\rangle &= \sqrt{\nu} |v\rangle + \sqrt{1-\nu} |v^\perp\rangle, & |w^\perp\rangle &= \sqrt{1-\nu} |v\rangle - \sqrt{\nu} |v^\perp\rangle. \end{aligned}$$

Furthermore, this two-dimensional subspace is invariant under the action of P, Q , as $|v\rangle = P|w\rangle/\sqrt{\nu}$ and $|w\rangle = Q|v\rangle/\sqrt{\nu}$. We remark that this is a special case of Jordan's Lemma [Bha13, Chapter VII].

Now for every $i \in [k]$ define the projectors

$$P_{-i} = |C\rangle\langle C|^{\otimes k-1} \otimes \text{id}_{\mathbf{A}_i \mathbf{B}_i} \otimes |0\rangle\langle 0|_{\mathbf{G}} \quad \text{and} \quad Q_{-i} = \tilde{R}^\dagger \left(|D\rangle\langle D|^{\otimes k-1} \otimes \text{id}_{\mathbf{A}_i \mathbf{B}_i \mathbf{G}} \right) \tilde{R}.$$

Note that P_{-i}, Q_{-i} do not act on registers $\mathbf{A}_i \mathbf{B}_i$, and that $P_{-i}P = PP_{-i} = P$ and $Q_{-i}Q = QQ_{-i} = Q$.

We now argue that the operators P_{-i}, Q_{-i} are not far from P, Q for a randomly chosen i .

Claim 6.10. *For all unit length $|\psi\rangle$,*

$$\mathbb{E}_i \left\| (P - P_{-i}) |\psi\rangle \right\|^2 \leq \frac{1}{k} \quad \text{and} \quad \mathbb{E}_i \left\| (Q - Q_{-i}) |\psi\rangle \right\|^2 \leq \frac{1}{k}$$

where the expectation is over a uniformly random $i \in [k]$.

Proof. Note that $\mathbb{E}_i P_{-i} = (1 - \frac{1}{k})P$. We now calculate:

$$\begin{aligned} \mathbb{E}_i \left\| (P - P_{-i}) |\psi\rangle \right\|^2 &= \mathbb{E}_i \langle \psi | (P - P_{-i})(P - P_{-i}) |\psi\rangle = \mathbb{E}_i \langle \psi | P_{-i} |\psi\rangle - \langle \psi | P |\psi\rangle \\ &= \langle \psi | (\mathbb{E}_i P_{-i} - P) |\psi\rangle \leq \left\| \mathbb{E}_i P_{-i} - P \right\|_\infty \\ &= \left\| \frac{1}{k} P \right\|_\infty = \frac{1}{k}. \end{aligned}$$

The proof for Q 's proceeds analogously. □

Claim 6.11. *For all $|\psi\rangle \in \text{span}\{|v\rangle, |w\rangle\}$, we have*

$$\mathbb{E}_i \max \left\{ \left\| (P - P_{-i}) |\psi\rangle \right\|^2, \left\| (Q - Q_{-i}) |\psi\rangle \right\|^2 \right\} \leq \frac{4}{k}.$$

Proof. Claim 6.10 implies

$$\mathbb{E}_i \left\| (P - P_{-i}) |v\rangle \right\|^2 \leq \frac{1}{k} \quad \text{and} \quad \mathbb{E}_i \left\| (P - P_{-i}) |v^\perp\rangle \right\|^2 \leq \frac{1}{k}.$$

Now a unit vector $|\psi\rangle$ in the span of $|v\rangle, |w\rangle$ can be written as $|\psi\rangle = \alpha |v\rangle + \beta |v^\perp\rangle$, so

$$\mathbb{E}_i \left\| (P - P_{-i}) |\psi\rangle \right\|^2 \leq 2 \mathbb{E}_i \left(|\alpha|^2 \left\| (P - P_{-i}) |v\rangle \right\|^2 + |\beta|^2 \left\| (P - P_{-i}) |v^\perp\rangle \right\|^2 \right) \leq \frac{2}{k}$$

where we used that $|\alpha|^2 + |\beta|^2 = 1$. The proof for the Q 's is analogous. □

We now analyze the performance of [Algorithm 2](#). Let V_i denote the unitary corresponding to the “for loop” in [Algorithm 2](#), i.e., step 4, conditioned on sampling i in step 1. The algorithm is described in terms of measurements, but we can imagine coherently performing the measurements and storing the outcome in an ancilla qubit. In particular, we describe V_i as a sequence of alternating unitary operations. We introduce the following labels for registers.

1. Let \mathbf{S} denote $\mathbf{A}_{[k]}\mathbf{B}_{[k]}\mathbf{G}$.
2. Let $\mathbf{H}_{[T]}$ denote ancilla qubits that store the outcomes of the P measurements.
3. Let \mathbf{F} denote an ancilla qubit that indicates whether a Q measurement succeeded.

The ancilla qubits all start in the zero state. Define the following unitary transformations:

1. For all $j \in [T]$, define

$$A_{ij} = |0\rangle\langle 0|_{\mathbf{F}} \otimes \left[P_{-i} \otimes X_{\mathbf{H}_j} + (I - P_{-i}) \otimes \text{id}_{\mathbf{H}_j} \right] + |1\rangle\langle 1|_{\mathbf{F}} \otimes \text{id}$$

In other words, A_{ij} performs the j 'th P_{-i} measurement: it checks if the \mathbf{F} qubit is set to $|1\rangle$. If so, it does nothing. Otherwise, it performs the P_{-i} measurement and flips the qubit in register \mathbf{H}_j .

2. We define

$$B_i = |0\rangle\langle 0|_{\mathbf{F}} \otimes (\text{id} - Q_{-i}) + |1\rangle\langle 0|_{\mathbf{F}} \otimes Q_{-i} + |1\rangle\langle 1|_{\mathbf{F}} \otimes \text{id} .$$

In other words, B_i checks if the \mathbf{F} qubit is set to $|1\rangle$. If so, it does nothing. Otherwise, it performs the Q_{-i} measurement and if the Q_{-i} outcome occurs, and flips \mathbf{F} qubit.

Thus the state of the algorithm V_i after the j 'th step is

$$|\varphi_{ij}\rangle := B_i A_{ij} B_i A_{i,j-1} \cdots B_i A_{i1} |v\rangle |0 \cdots 0\rangle_{\mathbf{S}\mathbf{F}\mathbf{H}_1 \cdots \mathbf{H}_T} .$$

Clearly V_i is computable by a polynomial-size circuit.

We now consider another algorithm \hat{V} which is the same as V_i except instead of performing the P_{-i}, Q_{-i} measurements, performs P, Q instead. Define the unitary matrices $\hat{A}_1, \dots, \hat{A}_T$ and \hat{B} in the same way except they perform the P and Q measurements instead of P_{-i} and Q_{-i} . Thus the state of the algorithm \hat{V} after the j 'th step is

$$|\hat{\varphi}_j\rangle := \hat{B} \hat{A}_j \hat{B} \hat{A}_{j-1} \cdots \hat{B} \hat{A}_1 |v\rangle |0 \cdots 0\rangle_{\mathbf{S}\mathbf{F}\mathbf{H}_1 \cdots \mathbf{H}_T} .$$

Define $|\hat{\varphi}_0\rangle := |v\rangle |0 \cdots 0\rangle$. We will argue that $|\varphi_{ij}\rangle$ is not far from $|\hat{\varphi}_j\rangle$ on average over a randomly chosen index i .

Claim 6.12. *For all $j = 0, \dots, T$, the \mathbf{S} register of $|\hat{\varphi}_j\rangle$ is supported on the subspace $\text{span}\{|v\rangle, |w\rangle\}$.*

Proof. We prove this by induction. This holds for $j = 0$ because the initial state is $|v\rangle |0 \cdots 0\rangle$. Assume for induction that the statement is true up to $j - 1$. Note that

$$|\hat{\varphi}_j\rangle = \hat{B} \hat{A}_j |\hat{\varphi}_{j-1}\rangle .$$

The operator \hat{A}_j either performs the P measurement on register \mathbf{S} or does nothing; the post-measurement states remain inside the two-dimensional subspace $\text{span}\{|v\rangle, |w\rangle\}$ because this subspace is invariant under the action of P . Same with the \hat{B} operator, which either performs the Q measurement or does nothing. \square

Claim 6.13. For all $i \in [k]$ and $j \in [T]$ we have

$$\mathbb{E}_i \left\| (B_i A_{ij} - \hat{B} \hat{A}_j) |\hat{\varphi}_{j-1}\rangle \right\| \leq \frac{8}{\sqrt{k}}.$$

Proof. By triangle inequality,

$$\begin{aligned} \left\| (B_i A_{ij} - \hat{B} \hat{A}_j) |\hat{\varphi}_{j-1}\rangle \right\| &\leq \left\| B_i (A_{ij} - \hat{A}_j) |\hat{\varphi}_{j-1}\rangle \right\| + \left\| (B_i - \hat{B}) \hat{A}_j |\hat{\varphi}_{j-1}\rangle \right\| \\ &= \left\| (A_{ij} - \hat{A}_j) |\hat{\varphi}_{j-1}\rangle \right\| + \left\| (B_i - \hat{B}) \hat{A}_j |\hat{\varphi}_{j-1}\rangle \right\|, \end{aligned}$$

where in the second line we used that B_i is unitary. We analyze each term separately. By triangle inequality again,

$$\begin{aligned} \left\| (A_{ij} - \hat{A}_j) |\hat{\varphi}_{j-1}\rangle \right\| &\leq \left\| |0\rangle\langle 0|_{\mathbb{F}} \otimes (P_{-i} - P) \otimes X_{\mathbb{H}_j} |\hat{\varphi}_{j-1}\rangle \right\| + \left\| |0\rangle\langle 0|_{\mathbb{F}} \otimes (P_{-i} - P) \otimes \text{id}_{\mathbb{H}_j} |\hat{\varphi}_{j-1}\rangle \right\| \\ &= 2 \left\| (P_{-i} - P) |\hat{\varphi}_{j-1}\rangle \right\|. \end{aligned}$$

Similarly we have

$$\left\| (B_i - \hat{B}) \hat{A}_j |\hat{\varphi}_{j-1}\rangle \right\| \leq 2 \left\| (Q_{-i} - Q) \hat{A}_j |\hat{\varphi}_{j-1}\rangle \right\|.$$

Averaging over $i \in [k]$ we get

$$\begin{aligned} \mathbb{E}_i \left\| (B_i A_{ij} - \hat{B} \hat{A}_j) |\hat{\varphi}_{j-1}\rangle \right\| &\leq 2 \left(\mathbb{E}_i \left\| (P_{-i} - P) |\hat{\varphi}_{j-1}\rangle \right\| + \left\| (Q_{-i} - Q) \hat{A}_j |\hat{\varphi}_{j-1}\rangle \right\| \right) \\ &\leq 2 \left(\sqrt{\mathbb{E}_i \left\| (P_{-i} - P) |\hat{\varphi}_{j-1}\rangle \right\|^2} + \sqrt{\mathbb{E}_i \left\| (Q_{-i} - Q) \hat{A}_j |\hat{\varphi}_{j-1}\rangle \right\|^2} \right) \\ &\leq 4 \sqrt{\frac{4}{k}} = \frac{8}{\sqrt{k}} \end{aligned}$$

where in the second line we used Jensen's inequality, and in the third line we used [Claim 6.11](#) with the fact that the \mathbb{S} registers of $|\hat{\varphi}_{j-1}\rangle$ and $\hat{A}_j |\hat{\varphi}_{j-1}\rangle$ are supported on the subspace $\text{span}\{|v\rangle, |w\rangle\}$. \square

Putting everything together, we have by the triangle inequality

$$\mathbb{E}_i \left\| |\varphi_{iT}\rangle - |\hat{\varphi}_T\rangle \right\| \leq \mathbb{E}_i \sum_{j=1}^T \left\| (B_i A_{ij} - \hat{B} \hat{A}_j) |\hat{\varphi}_{j-1}\rangle \right\| \leq 8T/\sqrt{k}. \quad (6.5)$$

Now we analyze the behavior of the \hat{V} algorithm; by what we just argued, the behavior of the V_i algorithm is similar on average over i (assuming that T is sufficiently smaller than \sqrt{k}).

Claim 6.14. $\left\| (\text{id} - Q) |\hat{\varphi}_T\rangle \right\|^2 \leq (1 - \nu)^T$.

Proof. Since the projector $\text{id} - Q$ does not act on the ancilla $\mathbb{H}_{[T]}$ registers, the quantity $\left\| (\text{id} - Q) |\hat{\varphi}_T\rangle \right\|^2$ is the probability that running the algorithm \hat{V} with *incoherent* P, Q measurements never yields a Q outcome at any of the T iterations.

Since the initial state of the algorithm is $|v\rangle|0\dots 0\rangle$, and the algorithm simply alternates between performing the $\{P, \text{id} - P\}$ and $\{Q, \text{id} - Q\}$ projective measurements, no matter what the measurement outcomes are, the register \mathbf{S} of the post-measurement state is always either $|v\rangle, |w\rangle, |v^\perp\rangle, |w^\perp\rangle$. If register \mathbf{S} is ever in the state $|w\rangle$, then that means the Q outcome must have occurred, and the algorithm stops. Thus the quantity $\left\|(\text{id} - Q)|\hat{\varphi}_T\rangle\right\|^2$ is the probability that the first iteration resulted in register \mathbf{S} being in the state $|w^\perp\rangle$, and for every iteration thereafter started in $|w^\perp\rangle$ and ended in $|w^\perp\rangle$.

The probability that the first iteration ends in the state $|w^\perp\rangle$ is exactly $1 - \nu$. In all the iterations thereafter, conditioned on the starting state being $|w^\perp\rangle$, performing the $\{P, \text{id} - P\}$ measurement followed by the $\{Q, \text{id} - Q\}$ measurement yields the outcome $|w^\perp\rangle$ state again with probability $\nu^2 + (1 - \nu)^2$. Thus we get

$$\left\|(\text{id} - Q)|\hat{\varphi}_T\rangle\right\|^2 = (1 - \nu)(\nu^2 + (1 - \nu)^2)^{T-1} \leq (1 - \nu)^T$$

as desired. \square

We now bound the performance of M . We have that

$$F((\text{id}_A \otimes M)|C\rangle\langle C|, |D\rangle\langle D|) = \langle D | (\text{id}_A \otimes M)(|C\rangle\langle C|) | D \rangle = 1 - \text{Tr}\left((\text{id} - |D\rangle\langle D|)(\text{id}_A \otimes M)(|C\rangle\langle C|)\right).$$

Note that we can write the output of M when given as input register \mathbf{B} of $|C\rangle$ as

$$(\text{id}_A \otimes M)(|C\rangle\langle C|) = \mathbb{E}_i \text{Tr}_{\overline{\mathbf{B}_i}} \left(\tilde{R} V_i (|C\rangle\langle C|^{\otimes k} \otimes |0\dots 0\rangle\langle 0\dots 0|) V_i^\dagger \tilde{R}^\dagger \right)$$

where $\text{Tr}_{\overline{\mathbf{B}_i}}(\cdot)$ denotes the partial trace of all registers except for \mathbf{B}_i , and $|0\dots 0\rangle$ denotes the ancilla qubits in registers $\mathbf{G}, \mathbf{F}, \mathbf{H}_{[T]}$. Now observe that $V_i |C\rangle^{\otimes k} |0\dots 0\rangle$ is nothing but $|\varphi_{iT}\rangle$. Therefore

$$\begin{aligned} \text{Tr}\left((\text{id} - |D\rangle\langle D|)(\text{id}_A \otimes M)(|C\rangle\langle C|)\right) &= \mathbb{E}_i \left\| (\text{id} - |D\rangle\langle D|)_{\mathbf{A}_i \mathbf{B}_i} \tilde{R}_{x^k} |\varphi_{iT}\rangle \right\|^2 \\ &\leq 2 \left\| (\text{id} - Q) |\hat{\varphi}_T\rangle \right\|^2 + 2 \mathbb{E}_i \left\| |\varphi_{iT}\rangle - |\hat{\varphi}_T\rangle \right\|^2 \\ &\leq 2(1 - \nu)^T + 4 \mathbb{E}_i \left\| |\varphi_{iT}\rangle - |\hat{\varphi}_T\rangle \right\|^2 \\ &\leq 2(1 - \nu)^T + \frac{32T}{\sqrt{k}}. \end{aligned} \tag{6.6}$$

In the second line we used the triangle inequality and the fact that

$$\left\| (\text{id} - |D\rangle\langle D|)_{\mathbf{A}_i \mathbf{B}_i} \tilde{R} |\varphi_{iT}\rangle \right\|^2 = \left\| \tilde{R}^\dagger (\text{id} - |D\rangle\langle D|)_{\mathbf{A}_i \mathbf{B}_i} \tilde{R} |\varphi_{iT}\rangle \right\|^2$$

because \tilde{R} is unitary, and that $Q \leq \tilde{R}^\dagger |D\rangle\langle D|_{\mathbf{A}_i \mathbf{B}_i} \tilde{R}$ in the positive semidefinite ordering. The third line uses [Claim 6.14](#) and the fact that $\left\| |\varphi_{iT}\rangle - |\hat{\varphi}_T\rangle \right\|^2 \leq 2 \left\| |\varphi_{iT}\rangle - |\hat{\varphi}_T\rangle \right\|$. The fourth line uses [Equation \(6.5\)](#).

This concludes the proof of [Lemma 6.9](#). \square

6.3 The padding trick

We now turn to the complexity of $\text{DISTUHLMANN}_\kappa$ when κ is bounded away from 0 and 1 by some inverse-polynomial quantity. Note that for all $0 \leq \kappa_1 \leq \kappa_2 \leq 1$, we have that all valid instances of $\text{UHLMANN}_{\kappa_2}$ are valid instances of $\text{UHLMANN}_{\kappa_1}$ but not vice versa (a similar statement holds for SUCCINCTUHLMANN). Thus, implementing general $\text{UHLMANN}_{\kappa_1}$ transformations may potentially be more difficult than implementing $\text{UHLMANN}_{\kappa_2}$ transformations. Furthermore, it is no longer apparent that there is a zero-knowledge protocol for, say, $\text{DISTUHLMANN}_{1/2}$. Thus it is not clear how the complexities of $\text{UHLMANN}_{\kappa_1}$ and $\text{UHLMANN}_{\kappa_2}$ 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 $\text{DISTUHLMANN}_{\kappa_1}$ and $\text{DISTUHLMANN}_{\kappa_2}$ are equivalent under polynomial-time reductions.

Lemma 6.15 (Padding trick). *Let $0 \leq \kappa_1 \leq \kappa_2 \leq 1$ and let C, D be circuits on $2n$ qubits such that $F(\rho, \sigma) \geq \kappa_1$ 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. $F(\tau, \mu) \geq \kappa_2$ 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

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

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 $F(\tau, \mu) = \alpha F(\rho, \sigma) + 1 - \alpha \geq \alpha \kappa_1 + 1 - \alpha \geq \kappa_2$.

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

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

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

$$\text{sgn}\left(\alpha \text{Tr}_A(|C\rangle\langle D|) \otimes |0\rangle\langle 0| + (1 - \alpha) |1^n\rangle\langle 1^n| \otimes |1\rangle\langle 1|\right) = \text{sgn}(\text{Tr}_A(|C\rangle\langle D|)) \otimes |0\rangle\langle 0| + |1^n\rangle\langle 1^n| \otimes |1\rangle\langle 1|$$

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

Lemma 6.16 (Average-case reductions for $\text{DISTUHLMANN}_\kappa$ for different fidelities κ). *Let $\kappa : \mathbb{N} \rightarrow [0, 1]$ be such that $1/p(n) \leq \kappa(n) \leq 1 - 1/p(n)$ for all n for some polynomial $p(n)$. Then $\text{DISTUHLMANN}_\kappa$ polynomial-time reduces to $\text{DISTUHLMANN}_{1-1/p}$.*

Proof. For every valid UHLMANN_κ instance $x = (1^n, C, D)$, let $y = (1^{2(n+1)}, E, F)$ denote the valid $\text{UHLMANN}_{1-1/p}$ instance given by the padding trick (Lemma 6.15), 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 6.15 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 .

To prove the lemma, let $q(n)$ be an arbitrary polynomial. By Definition 3.21 we need to find another polynomial $r(n)$ (which can depend on $q(n)$) and a polynomial-time quantum query algorithm A^* such that any $1/r(n)$ -error average case instantiation (see Definition 3.20) of $A_{1-1/p}^{\text{DISTUHLMANN}}$ implements $\text{DISTUHLMANN}_{1/p}$ with average-case error $1/q(n)$.

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

To show that this implements $\text{DISTUHLMANN}_{1/p}$, let $r(n) = p(n)q(n)$, and let $A^{\text{DISTUHLMANN}_{1-1/p}}$ denote a $1/r(n)$ -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 $\text{DISTUHLMANN}_{1-1/p}$ with average-case error $1/r(n)$ and is used to instantiate the $\text{DISTUHLMANN}_{1-1/p}$ -oracle. This means there is a channel completion Φ_y of V_y such that

$$\text{td}\left(\left(\text{id} \otimes H_y\right)\left(|E\rangle\langle E|\right), \left(\text{id} \otimes \Phi_y\right)\left(|E\rangle\langle E|\right)\right) \leq \frac{1}{r(|y|)}.$$

By the third item of Lemma 6.15, any channel completion Φ_y of V_y can be turned into a channel completion of Ξ_x of U_x , the UHLMANN_κ transformation corresponding to $(|C\rangle, |D\rangle)$. Define $\Xi_x(\rho) := \text{Tr}_G(\Phi_x(\rho \otimes |0\rangle\langle 0|_G))$ where G denotes the last qubit. Let Π denote the support onto U_x . Then $\Xi_x(\Pi\rho\Pi) = \text{Tr}_G(\Phi_x(\Pi\rho\Pi \otimes |0\rangle\langle 0|_G))$. But notice that the state $\Pi\rho\Pi \otimes |0\rangle\langle 0|$ is contained in the support of V_y ; therefore

$$\text{Tr}_G(\Phi_x(\Pi\rho\Pi \otimes |0\rangle\langle 0|)) = \text{Tr}_G\left(V_y(\Pi\rho\Pi \otimes |0\rangle\langle 0|)V_y^\dagger\right) = U_x\Pi\rho\Pi U_x^\dagger$$

where we used the expression for V_y given by Lemma 6.15. Thus we can evaluate the performance of the instantiation $A^{\text{DISTUHLMANN}_{1-1/p}}$ on the input $|C\rangle$:

$$\begin{aligned}
& \text{td}\left((\text{id} \otimes A_x^{\text{DISTUHLMANN}_{1-1/p}})(|C\rangle\langle C|), (\text{id} \otimes \Xi_x)(|C\rangle\langle C|)\right) \\
&= \text{td}\left((\text{id} \otimes H_y)(|0\rangle\langle 0| \otimes |C\rangle\langle C| \otimes |0\rangle\langle 0|), (\text{id} \otimes \Phi_y)(|0\rangle\langle 0| \otimes |C\rangle\langle C| \otimes |0\rangle\langle 0|)\right) \\
&= \frac{1}{\alpha(n)} \text{td}\left((\text{id} \otimes H_y)(P|E\rangle\langle E|P^\dagger), (\text{id} \otimes \Phi_y)(P|E\rangle\langle E|P^\dagger)\right) \\
&\leq \frac{1}{\alpha(n)} \text{td}\left((\text{id} \otimes H_y)(|E\rangle\langle E|), (\text{id} \otimes \Phi_y)(|E\rangle\langle E|)\right) \\
&\leq \frac{1}{\alpha(n)r(n)} = \frac{1}{q(n)}.
\end{aligned}$$

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 $\alpha(n), r(n)$. \square

The padding trick allows us to make statements about UHLMANN_κ and $\text{DISTUHLMANN}_\kappa$ for the case where κ is at least an inverse polynomial. However, it may be that UHLMANN with negligible κ is more powerful than this. We leave this as an open question.

Open Problem 12. What is the power of UHLMANN_κ or $\text{DISTUHLMANN}_\kappa$ for negligible κ ?

6.4 A polarization lemma for unitary zero knowledge?

Sahai and Vadhan [SV03] introduced the `STATISTICALDISTANCE` problem and showed that it is complete for `SZK`. Here, an instance $(1^n, C_0, C_1)$ of `STATISTICALDISTANCE` consists of a pair of probability distributions (specified by circuits C_0, C_1 which produce samples from them) and the problem is to decide whether the distributions are *close* (below the threshold $1/3$) or *far apart* (above the threshold $2/3$) in terms of statistical distance. A key technical ingredient in their proof system is the so-called “polarization lemma”. This is an efficient transformation that takes as input a pair of probability distributions (specified by circuits) and produces a new pair of distributions (in the form of new pair of circuits) with the following two guarantees:

- if the initial pair of distributions is statistically *close* (below the threshold $1/3$), then the new pair of distributions is statistically *much closer* (below the threshold 2^{-n}), whereas
- if the initial pair of distributions is statistically *far apart* (above the threshold $2/3$), then new pair is statistically *much further apart* (above the threshold $1 - 2^{-n}$).

This raises the following natural question: is it possible to obtain a “polarization lemma” in the context of `avgUnitarySZK` – the unitary analogue of (average-case) `SZK`? Specifically, we ask:

Open Problem 13. Is it possible to prove a “polarization lemma” which transforms an instance of UHLMANN_κ for a small κ , say $\kappa = 1/2$, into an instance of $\text{UHLMANN}_{1-\text{negl}(n)}$ for some negligible function, say 2^{-n} ?

Note that the latter problem is complete for `avgUnitarySZK`, as we established in [Theorem 6.7](#). Watrous [[Wat06](#)] previously extended the polarization technique to *density operators* (specified by quantum circuits which prepare them), and showed that `QUANTUMSTATEDISTINGUISHABILITY` is complete for `QSZK`. This suggests that one could potentially apply a similar transformation as in [[Wat06](#), Theorem 1] in order to map an `UHLMANN1/2` instance $(1^n, C, D)$ with $F(\rho, \sigma) \geq 1/2$ (where ρ and σ represent the mixed states induced by C, D) into an `UHLMANN1-2^{-n}` instance $(1^n, \tilde{C}, \tilde{D})$ with $F(\tilde{\rho}, \tilde{\sigma}) \geq 1-2^{-n}$. While such a circuit transformation is indeed possible via auxiliary qubits (which encode random coins required for polarization), any auxiliary qubits must necessarily be part of the *purifying register* on which the Uhlmann unitary is allowed to act upon. This significantly complicates the matter when quantum input states are taken into account; for example, it is unclear how to relate instances of `DISTUHLMANN1/2` to valid instances of `DISTUHLMANN1-2^{-n}`. We leave the task of finding a polarization lemma for `avgUnitarySZK` – or to find evidence against one – as an interesting open problem.

7 Structural Results about the Succinct Uhlmann Transformation Problem

In this section, we show that the `DISTSUCCINCTUHLMANN1` problem captures the complexity of both `avgUnitaryPSPACE` and `avgUnitaryQIP`, which allows us to show that the two unitary complexity classes are equal. Concretely, we show that `DISTSUCCINCTUHLMANN1` is a complete problem both for `avgUnitaryQIP` ([Section 7.1](#)) and for `avgUnitaryPSPACE` ([Section 7.2](#)), which implies equality of the classes ([Corollary 7.13](#)). We then show additional structural results about the succinct Uhlmann transformation problem, namely that `SUCCINCTUHLMANN` is complete for worst-case `unitaryPSPACE` for a suitable choice of cutoff parameter ([Section 7.3](#)), and how `DISTSUCCINCTUHLMANN` relates to classical (worst-case) `PSPACE` ([Section 7.4](#)).

7.1 Completeness for `avgUnitaryQIP`

7.1.1 `DISTSUCCINCTUHLMANN1` \in `avgUnitaryQIP`

We begin with an `avgUnitaryQIP` protocol for `DISTSUCCINCTUHLMANN1`, which we will use to show that `DISTSUCCINCTUHLMANN1` \in `avgUnitaryQIP`. The protocol closely mirrors that of [Protocol 1](#) (the `avgUnitarySZK` protocol for `DISTUHLMANN`), 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 easily get copies of the `statePSPACE`-state $|C\rangle$ and can no longer directly implement the unitary D^\dagger to check that the Uhlmann transformation was applied correctly, which were important steps in [Protocol 1](#). For the first problem, we recall that `statePSPACE` = `stateQIP` [[MY23](#)], so by interacting with the prover, the verifier generate additional copies of the input state $|C\rangle$ (up to arbitrary inverse polynomial error). To solve the second problem, we show that the verifier can perform the measurement $\{|D\rangle\langle D|, \text{id} - |D\rangle\langle D|\}$ on an arbitrary state with help from the prover. We describe these in more detail next.

Interactive state synthesis. First we recall the main result of of [[RY22](#)], which shows that there is an efficient interactive protocol to synthesize any state sequence $(|\psi_x\rangle)_x \in \text{statePSPACE}$. We describe this result at a high level (for formal details see [[RY22](#)]): for every `statePSPACE` state sequence $(|\psi_x\rangle)_x$ there exists a polynomial-time quantum verifier $V = (V_x)_x$ such (a) there exists

an honest prover P^* that is accepted by the verifier with probability 1 (*completeness*), and after interacting with the honest prover the output register of the verifier is close to $|\psi_x\rangle$ to within 2^{-n} in trace distance (*honest closeness*), and (b) for all provers P that are accepted with probability at least $\frac{1}{2}$ (*soundness*), the output register of the verifier is close to $|\psi_x\rangle$ within some polynomial $1/p(|x|)$ in trace distance (*closeness*).

In what follows we will utilize as a subroutine the interactive state synthesis protocol for the sequence $\Gamma = (|C\rangle)_{\hat{C}}$ 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 $\Gamma \in \text{statePSPACE}$, and therefore there is a **stateQIP** protocol to synthesize Γ .

Interactive measurement synthesis. Next we describe another primitive which is a protocol for *interactive measurement synthesis*. At a high level, this is a protocol where a verifier gets a description of a measurement M and an input register A in an unknown state τ . The verifier interacts with a prover and at the end outputs a measurement outcome bit b as well as register A . If the prover is accepted with sufficiently high probability, then (a) the measurement outcome bit b is 1 with probability close to $\text{Tr}(M\tau)$, and (b) conditioned on acceptance and $b = 1$, the output register A is close to being in the state $\tau|_M$, the post-measurement state¹³ of τ conditioned on measuring M .

We show there is an efficient interactive measurement synthesis protocol for the case when the measurement M is a rank-one projector $|\psi\rangle\langle\psi|$ for some succinctly described state $|\psi\rangle$.

Lemma 7.1 (Approximate measurement protocol). *Let $\Psi = (|\psi_x\rangle)_x$ be a **stateQIP** family of states. Then for all polynomials $p(n)$, there exists a polynomial-time quantum verifier V that takes as input register A , and outputs an accept/reject flag, a measurement outcome bit b , and a register A such that the following properties hold:*

1. (*Completeness*) *There exists an honest prover P^* such that for all input states τ_A*

$$\Pr[V(\tau_A) \stackrel{P^*}{\text{accepts}}] = 1.$$

Furthermore, given input state $|\psi_x\rangle\langle\psi_x|$ in register A , the verifier outputs $b = 1$ with overwhelming probability:

$$\Pr[V(|\psi_x\rangle\langle\psi_x|_A) \stackrel{P^*}{\text{outputs 1}}] \geq 1 - 2^{-|x|}.$$

2. (*Soundness*) *For all input states τ_{AR} (where R is an arbitrary external register not touched by the verifier or prover) and for all provers P such that $V(\tau_{AR}) \stackrel{P}{\text{accepts}}$ with probability at least $1/2$,*

$$\left| \Pr[V \text{ outputs } b = 1 \mid V \text{ accepts}] - \text{Tr}\left(|\psi_x\rangle\langle\psi_x|_A \tau_A\right) \right| \leq \frac{1}{p(|x|)},$$

where the events “outputs $b = 1$ ” and “accepts” are with respect to the interaction $V(\tau_{AR}) \stackrel{P}{\text{accepts}}$. If additionally $\text{Tr}\left(|\psi_x\rangle\langle\psi_x|_A \tau_A\right) \geq \frac{1}{2}$, then the final state $(\tau_{acc})_{AR}$ at the end of the protocol conditioned on acceptance and conditioned on measurement outcome bit $b = 1$ satisfies

$$\text{td}(\tau_{acc}, \tau|_{\psi_x \otimes \text{id}}) \leq \frac{1}{p(|x|)}, \tag{7.1}$$

¹³Recall the notation used for post-measurement states defined in [Section 2](#).

where $\tau|_{\psi_x \otimes \text{id}}$ denotes the post-measurement state of τ_{AR} conditioned on projecting the A register onto the state $|\psi_x\rangle$. Let $1/p(n)$ be the closeness of the verifier.

In the second part of the soundness condition, we only require that the verifier's quantum output is close in trace distance to $\tau|_{\psi_x \otimes \text{id}}$ if the verifier accepts with probability $\frac{1}{2}$ and the probability of obtaining measurement outcome 1 (with the ideal measurement) is at least $1/2$. Intuitively, the reason for this is that Equation (7.1) makes a statement involving the conditioned state $\tau|_{\psi_x \otimes \text{id}}$, which can become very sensitive to errors if the measurement probability $\text{Tr}\left(|\psi_x\rangle\langle\psi_x|_{\text{A}} \tau_{\text{A}}\right)$ is very small. The $1/2$ threshold can be relaxed to being any inverse polynomial if the trace distance error is suitably adjusted.

We defer the proof of Lemma 7.1 to Section 7.1.3.

We now use these two primitives (interactive state and measurement synthesis) to prove the following.

Lemma 7.2. $\text{DISTSUCCINCTUHLMANN}_1 \in \text{avgUnitaryQIP}$.

Proof. Fix a polynomial $q(n)$. We present in Protocol 2 an avgUnitaryQIP protocol for $\text{DISTSUCCINCTUHLMANN}_1$ with completeness $1 - 2^{-\Omega(n)}$, soundness $\frac{1}{2}$, and closeness $1/q(n)$. We use as subroutines

1. The stateQIP protocol for synthesizing the state sequence Γ (which is all succinctly described states) with completeness 1, soundness $1/2$, and closeness $1/32q(n)^2$.
2. The approximate measurement protocol from Lemma 7.1 for the state sequence Γ with closeness $1/32q(n)^2$.

For a circuit C we write $C^{\otimes m}$ to denote m parallel copies of the circuit which generates the product state $|C\rangle^{\otimes m}$.

Protocol 2. avgUnitaryQIP $_{1-2^{-n+1}, \frac{1}{2}, \frac{1}{q}}$ verifier for $\text{DISTSUCCINCTUHLMANN}_1$

Input: Classical string $x = (1^n, \hat{C}, \hat{D})$ specifying a succinct description of a pair of circuits (C, D) , and quantum register B_0 .

1. Let $m = 16q(n)^2$, and perform the stateQIP protocol to synthesize $|C\rangle^{\otimes m}$ in registers $A_1 B_1 \cdots A_m B_m$. If the stateQIP protocol rejects, reject.
2. Select a permutation $\pi \in S_{m+1}$ uniformly at random and apply \mathcal{P}_π to $B_{[0:m]}$. Send $B_{[0:m]}$ to the prover.
3. Verifier receives registers $B_{[0:m]}$ from the prover. Then
 - (a) Apply $\mathcal{P}_{\pi^{-1}}$ to $B_{[0:m]}$.
 - (b) Perform the approximate measurement protocol with measurement $|D\rangle\langle D|^{\otimes m}$ on quantum register $AB_{[m]}$. If the protocol rejects or outputs $b = 0$, reject.
 - (c) Accept and output the register B_0 .

We show that the verifier described in [Protocol 2](#) satisfies the required properties of `avgUnitaryQIP` protocols. First, it is clear that the verifier runs in polynomial time. This uses the fact that the `stateQIP` and approximate measurement verifiers run in polynomial time, and the succinct descriptions of $|C\rangle^{\otimes m}$ and $|D\rangle^{\otimes m}$ are polynomial-sized in the lengths of the succinct descriptions \hat{C} and \hat{D} . We prove the completeness and soundness conditions in separate lemmas:

1. There is an honest quantum prover that success with probability at least $1 - 2^{-n+1}$ ([Lemma 7.3](#)).
2. The verifier satisfies the soundness condition of an `avgUnitaryQIP` _{$1-2^{-n+1}, 1/2, 1/q$} protocol ([Lemma 7.4](#)).

Combined, [Lemmas 7.3](#) and [7.4](#) imply [Lemma 7.2](#). □

Lemma 7.3 (Completeness). *For all valid `SUCCINCTUHLMANN`₁ instances $x = (1^n, \hat{C}, \hat{D})$, for sufficiently large n , there exists an honest prover for [Protocol 2](#) satisfying*

$$\Pr[V_x(|C\rangle) \Leftarrow P] \geq 1 - 2^{-n+1}.$$

Proof. We define an honest prover that acts as follows: the honest prover first implements the honest prover `stateQIP` protocol with honest closeness 2^{-n} . Then the prover implements the Uhlmann unitary between C and D . Finally the prover implements the honest prover for the approximate measurement protocol. After the first step of the protocol, the verifier holds a state within trace distance 2^{-n} of $|C\rangle^{\otimes m+1}$ on registers $\text{AB}_{[0:m]}$, and after the second step the optimal Uhlmann unitary has been performed. Therefore after the second step the verifier holds a state within trace distance 2^{-n} of $|D\rangle^{\otimes m+1}$. By the completeness property of the approximate measurement protocol, the verifier accepts with probability 1, and when run on $|D\rangle^{\otimes m}$, the protocol outputs the bit $b = 1$ with probability at least $1 - 2^{-n}$. Since the input state is within 2^{-n} of $|D\rangle^{\otimes m}$ in trace distance, the approximate measurement protocol on the verifier's real state outputs 1 with probability at least $1 - 2^{-n+1}$. When interacting with this honest prover, this is the only step where the verifier has a non-zero chance of rejecting, so the verifier accepts with probability at least $1 - 2^{-n+1}$. □

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

$$\text{if } \Pr[V_x(|C\rangle) \Leftarrow P \text{ accepts}] \geq \frac{1}{2} \quad \text{then} \quad \text{td}(\sigma, (\Phi_x \otimes \text{id})|C\rangle\langle C|) \leq 1/q(n),$$

where σ denotes the output of $V_x(|C\rangle) \Leftarrow P$ conditioned on the verifier V_x accepting where $q(n)$ is the polynomial used to define [Protocol 2](#).

Proof. By the definition of `SUCCINCTUHLMANN`₁, for all channel completions Φ_x of U_x we have that $(\Phi_x \otimes \text{id})|C\rangle\langle C| = |D\rangle\langle D|$, so it suffices to show that conditioned on accepting, the verifier outputs a state within $1/q(n)$ of $|D\rangle\langle D|$ in trace distance. The proof follows the template set by the proof that `DISTUHLMANN` _{$1-\text{negl}$} \in `avgUnitarySZK`_{HV}, with some subtle differences. We first appeal to [Lemma 6.3](#) to claim that if the verifier could prepare exactly $|C\rangle\langle C|^{\otimes m}$ in registers $\text{AB}_{[m]}$ after the `stateQIP` protocol, measuring $|D\rangle\langle D|$ on A_0B_0 accepts with high probability. We then show that the verifier's true state, with errors coming from both state preparation and approximate measurement, is close to this ideal post-measurement state. Finally we apply the Gentle Measurement Lemma.

We begin, as before, by expressing the state of the verifier's registers. By the soundness property of **stateQIP**, if the verifier accepts with probability at least $1/2$, after step 1 the verifier has a state in registers $\mathbf{AB}_{[0:m]}$ that is within $1/32q(n)^2$ of $|C\rangle^{\otimes m}$ in trace distance. Let ρ_0 be the state of registers $\mathbf{AB}_{[m]}$ after accepting in step 1 of the protocol. After performing the **stateQIP** protocol, the verifier applies a random permutation on $\mathbf{B}_{[0:m]}$; then the prover will perform some arbitrary action on $\mathbf{B}_{[0:m]}$ represented by a quantum channel Λ ; and finally the verifier will undo the permutation from the first step. Treating \mathbf{A}_0 as a purification of the verifier's quantum input, the state of $\mathbf{AB}_{[0:m]}$ is given by

$$\rho^* := \mathbb{E}_{\pi \in S_{m+1}} \left((\mathcal{P}_{\pi^{-1}})_{\mathbf{B}_{[0:m]}} \circ \Lambda_{\mathbf{B}_{[0:m]}} \circ (\mathcal{P}_{\pi})_{\mathbf{B}_{[0:m]}} \right) (|C\rangle\langle C|_{\mathbf{A}_0\mathbf{B}_0} \otimes (\rho_0)_{\mathbf{AB}_{[m]}}) \quad (7.2)$$

Let the state σ^* be defined as follows

$$\sigma^* = \mathbb{E}_{\pi \in S_{m+1}} \left((\mathcal{P}_{\pi^{-1}})_{\mathbf{B}_{[0:m]}} \circ \Lambda_{\mathbf{B}_{[0:m]}} \circ (\mathcal{P}_{\pi})_{\mathbf{B}_{[0:m]}} \right) (|C\rangle\langle C|^{\otimes m+1}).$$

One can think of σ^* as the state the verifier hopes to have in their registers after step 3(a). Because trace distance can only decrease when applying a channel, we have that

$$\text{td}(\rho^*, \sigma^*) \leq \text{td}((\rho_0)_{\mathbf{AB}_{[m]}}, |C\rangle\langle C|^{\otimes m}) \leq \frac{1}{32q^2},$$

where the final inequality comes from the **stateQIP** soundness promise, as explained above. Let ρ_{acc} be the state of the verifier after step 3(b) conditioned on the verifier accepting. In step 3(b), the verifier hopes to measure some ideal measurement and see outcome \mathcal{M} , described below as

$$\mathcal{M} = \text{id}_{\mathbf{A}_0\mathbf{B}_0} \otimes |D\rangle\langle D|^{\otimes m}.$$

Then let $\rho_{acc}^* = \rho^*|_{\mathcal{M}}$ and $\sigma_{acc}^* = \sigma^*|_{\mathcal{M}}$. Our goal is to get a lower bound for the quantity

$$\text{Tr}(|D\rangle\langle D|_{\mathbf{A}_0\mathbf{B}_0} \rho_{acc}^*), \quad (7.3)$$

because applying the Gentle Measurement Lemma will then give us a bound on the trace distance between ρ_{acc} and $|D\rangle\langle D|_{\mathbf{A}_0\mathbf{B}_0}$. Following the calculations in [Lemma 6.3](#), we have that

$$\text{Tr}(|D\rangle\langle D|_{\mathbf{A}_0\mathbf{B}_0} \sigma_{acc}^*) \geq 1 - \frac{2}{m+1}.$$

From the approximate measurement soundness ([Lemma 7.1](#)), together with the assumption that the verifier accepts with probability at least $1/2$ (and thus the outcome bit b of the approximate measurement protocol is 1 with at least the same probability), we have that

$$\text{td}(\rho_{acc}, \rho_{acc}^*) \leq \frac{1}{32q^2}.$$

We can compute the trace distance between ρ_{acc}^* and σ_{acc}^* directly as follows:

$$\begin{aligned}
2\text{td}(\sigma_{acc}^*, \rho_{acc}^*) &= \left\| \frac{\mathcal{M}\sigma^*\mathcal{M}}{\text{Tr}(\mathcal{M}\sigma^*)} - \frac{\mathcal{M}\rho^*\mathcal{M}}{\text{Tr}(\mathcal{M}\rho^*)} \right\|_1 \\
&\leq \left\| \frac{\mathcal{M}\sigma^*\mathcal{M}}{\text{Tr}(\mathcal{M}\sigma^*)} - \frac{\mathcal{M}\sigma^*\mathcal{M}}{\text{Tr}(\mathcal{M}\rho^*)} \right\|_1 + \left\| \frac{\mathcal{M}(\sigma^* - \rho^*)\mathcal{M}}{\text{Tr}(\mathcal{M}\rho^*)} \right\|_1 \\
&\leq \|\mathcal{M}\sigma^*\mathcal{M}\|_1 \left| \frac{1}{\text{Tr}(\mathcal{M}\sigma^*)} - \frac{1}{\text{Tr}(\mathcal{M}\rho^*)} \right| + \frac{\|\mathcal{M}(\sigma^* - \rho^*)\mathcal{M}\|_1}{\text{Tr}(\mathcal{M}\rho^*)} \\
&\leq \text{Tr}(\mathcal{M}\sigma^*) \left| \frac{\text{Tr}(\mathcal{M}\rho^*) - \text{Tr}(\mathcal{M}\sigma^*)}{\text{Tr}(\mathcal{M}\rho^*)\text{Tr}(\mathcal{M}\sigma^*)} \right| + \frac{1}{8q^2} \\
&\leq \frac{3}{16q^2}.
\end{aligned}$$

For both terms, we get bounds from the fact that $\text{td}(\rho^*, \sigma^*) \leq 1/32q^2$ (and trace distance is contractive under channels, including measurements) and $\text{Tr}(\mathcal{M}\rho^*) \geq 1/2$. For the second term, we multiply by 2 because the trace distance is half the 1-norm. Thus we have that

$$\text{td}(\sigma_{acc}^*, \rho_{acc}^*) \leq \frac{3}{32q^2}.$$

Applying the triangle inequality we have that

$$\text{td}(\rho_{acc}, \sigma_{acc}^*) \leq \frac{1}{8q^2}.$$

From this trace distance bound we can bound Equation (7.3) by

$$\text{Tr}(|D\rangle\langle D|_{A_0B_0} \rho_{acc}) \geq 1 - \frac{2}{m+1} - \frac{1}{8q^2}.$$

Applying the gentle measurement lemma (Proposition 2.2), we see that the trace distance error from the state $|D\rangle\langle D|$ is at most

$$2\sqrt{\frac{2}{m+1} + \frac{1}{8q^2}} \leq 2\sqrt{\frac{1}{4q^2}} \leq 1/q,$$

where we use the fact that $m = 16q^2$, so $2/(m+1) \leq 1/(8q^2)$. This completes the proof of Lemma 7.4. \square

7.1.2 DISTSUCCINCTUHLMANN₁ is avgUnitaryQIP-hard

Having shown that $\text{DISTSUCCINCTUHLMANN}_1 \in \text{avgUnitaryQIP}$, we now need to show that it is in fact a complete problem, i.e. any unitary synthesis problem in avgUnitaryQIP can be reduced to $\text{DISTSUCCINCTUHLMANN}_1$. This is the statement of Lemma 7.5. Before giving the full proof of Lemma 7.5, we provide some intuition. We need to show that any distributional unitary synthesis problem $(\mathcal{U}, \Psi) \in \text{avgUnitaryQIP}$ can be solved by a polynomial-sized circuit with access to a $\text{DISTSUCCINCTUHLMANN}_1$ -oracle.

As a first step, let us consider a **stateQIP**-protocol (i.e. an interactive protocol where the verifier receives no input state and is asked to prepare a certain quantum state from scratch) and implement

this in $\text{stateBQP}^{\text{DISTSUCCINCTUHLMANN}_1}$. For any stateQIP -protocol, by [MY23, Lemma 7.5] there exist purifications of the intermediate states of the protocol (on the verifier and message registers) that are in statePSPACE . Furthermore, from the proof of [MY23, Lemma 7.5] it is easy to see that the circuits preparing these purifications have succinct descriptions that are efficiently computable from the descriptions of the verifier actions. Then, a possible successful prover strategy in the stateQIP -protocol is simply to implement the Uhlmann transformation between these purifications; see [MY23, Proof of Thm. 7.1] for a more detailed explanation of this idea. These Uhlmann transformations can be accomplished by a $\text{DISTSUCCINCTUHLMANN}_1$ -oracle: we can efficiently compute the succinct descriptions of the circuits between which we need to apply the Uhlmann transformation and feed these descriptions to the Uhlmann oracle in order to perform the required transformation, effectively simulating the prover with the Uhlmann oracle.

Now we consider the more difficult case of an avgUnitaryQIP -protocol. The key difficulty compared to the stateQIP -setting is that we are only given one copy of one register to which we want to apply our desired unitary. However, we can observe that the above argument for the stateQIP -protocol only relied on being able to compute the succinct classical descriptions of the circuits preparing purifications of the intermediate states of the protocol. Once we have these classical descriptions, we can implement the required Uhlmann transformation on any given state, i.e. the step of applying the Uhlmann oracle does not require having access to arbitrarily many copies of the input state.

Therefore, to apply the avgUnitaryQIP -protocol on a given input register, we proceed in two steps. The first step is purely classical: since in a distributional unitary synthesis problem $(\mathcal{U}, \Psi) \in \text{avgUnitaryQIP}$ the state family Ψ is in stateQIP , we can construct a stateQIP -protocol for the state $U_x |\psi_x\rangle$ with $U_x \in \mathcal{U}$ and $|\psi_x\rangle \in \Psi$.¹⁴ As described above, this stateQIP -protocol allows us to efficiently (classically) compute succinct descriptions of the circuits preparing purifications of the intermediate states of the protocol. In the second (quantum) step, we can now use these pre-computed succinct classical descriptions to efficiently simulate the avgUnitaryQIP -protocol with the Uhlmann oracle. For this, when it is the verifier's turn, we simply apply the (efficient) verifier actions, and when it is the prover's turn we use our pre-computed succinct classical descriptions and the Uhlmann oracle to apply the prover actions. This way, we can simulate the actions of the avgUnitaryQIP -protocol given only a single copy of the input register.

We formalise this idea in the following lemma.

Lemma 7.5. *avgUnitaryQIP polynomial-time reduces to $\text{DISTSUCCINCTUHLMANN}_1$.*

Proof. Let $(\mathcal{U}, \Psi) \in \text{avgUnitaryQIP}$. This means that there exists some polynomial-time quantum verifier $V = (V_x)$ who receives as input the \mathbf{A} -register of the state $|\psi_x\rangle_{\mathbf{AR}}$ and satisfies the completeness and soundness condition in Definition 4.2. Throughout the proof, whenever we say “successful prover”, we mean a prover that is accepted in the protocol with probability at least the soundness threshold $s(n) = 1/2$. Since $\Psi \in \text{stateQIP}$, there exists another polynomial-time verifier $V' = (V'_x)$ for synthesising the states $\Psi = (|\psi_x\rangle)$; note that V' receives no quantum input. We can combine these two verifier's into one verifier $\tilde{V} = (\tilde{V}_x)$ who receives no input and first executed the actions of V' ; at the end of this, \tilde{V} will be in possession of a state on registers \mathbf{A} and \mathbf{R} . \tilde{V} then runs V with \mathbf{A} as the input register and outputs the resulting state. If either V or V' rejects, so does \tilde{V} .

¹⁴Note that of course this is not the same as solving the average unitary synthesis problem: here, we simply prepare the desired state from scratch, whereas in the unitary synthesis setting we are given a single register of an entangled quantum state and have to apply the desired unitary to that register while keeping the entanglement with the remaining (inaccessible) register intact.

Applying [MY23, Lemma 7.5] to the verifier \tilde{V} shows that the intermediate states on the message and verifier register in the interaction of \tilde{V} with any prover with sufficiently high success probability have purifications in `statePSPACE`. Furthermore, from the proof of [MY23, Lemma 7.5] it is easy to see that 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 $|\psi_{n,j}\rangle$ and $|\varphi_{n,j}\rangle$. 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 i of the protocol, there exist polynomial-space quantum circuits C_x^i and D_x^i with efficiently computable succinct classical descriptions \hat{C}_x^i and \hat{D}_x^i such that $|\alpha_x^i\rangle_{V^i M^i P^i} = C_x^i |0 \dots 0\rangle$ and $|\beta_x^i\rangle_{V^i M^i P^i} = D_x^i |0 \dots 0\rangle$ are purifications of the reduced state on the message register M^i and verifier register V^i of the interactive protocol right before and after the prover's action in round i . Observe that because the verifier register in the interactive protocol is not acted upon by the prover, the reduced states on the verifier register are unchanged, i.e.

$$\mathrm{Tr}_{M^i P^i}(|\alpha_x^i\rangle\langle\alpha_x^i|_{V^i M^i P^i}) = \mathrm{Tr}_{M^i P^i}(|\beta_x^i\rangle\langle\beta_x^i|_{V^i M^i P^i}).$$

We can therefore interpret the circuit pair (C_x^i, D_x^i) as an instance of the `SUCCINCTUHLMANN` problem, with V^i taking the role of the register that cannot be acted upon by the Uhlmann unitary.¹⁵ With access to a `DISTSUCCINCTUHLMANN`-oracle, we can therefore apply an Uhlmann transformation mapping $|\alpha_x^i\rangle_{V^i M^i P^i} = C_x^i |0 \dots 0\rangle$ to $|\beta_x^i\rangle_{V^i M^i P^i} = D_x^i |0 \dots 0\rangle$ by acting only on registers $M^i P^i$. This means that with the `DISTSUCCINCTUHLMANN`-oracle, we can efficiently implement the actions of a successful prover in the interactive protocol.¹⁶

We now use this observation to construct a polynomial-size quantum query circuit that, when instantiated with `DISTSUCCINCTUHLMANN`₁ and run on register A of $|\psi_x\rangle$, produces the same output state as the quantum interactive protocol with verifier $V = (V_x)$ for this problem. The query circuit is constructed as follows: the circuit receives as input register A of $|\psi_x\rangle$. The circuit applies the first action of the verifier V , which we can assume to be unitary by purifying the actions of V and which can be done in polynomial-time since V is efficient. To the resulting state, the query circuit then applies an oracle gate with the succinct Uhlmann instance $(1^n, \hat{C}_x^{i^*}, \hat{D}_x^{i^*})$, where i^* is the round of the verifier \tilde{V} that corresponds to the first round of the verifier V (i.e. the first round that is part of the `avgUnitaryQIP`, not the `stateQIP`, protocol). As we showed above, $\hat{C}_x^{i^*}$ and $\hat{D}_x^{i^*}$ as well as the number of qubits n are efficiently computable given a description of the verifier \tilde{V} . This step will correctly implement the actions of a successful prover on this state. The query circuit then proceeds in this manner, applying the next action of the verifier V , simulating the next action of the prover using the oracle gates, etc.

Since V is polynomial-time, it is clear that the query circuit we constructed above is polynomial-time, too. Finally, to show that it outputs the same state as the interactive protocol, we simply notice that since the quantum query circuits simulates a run of the protocol with an honest prover

¹⁵Technically we also need to include the space requirement of C_x^i and D_x^i , which can be explicitly computed from the proof of [MY23, Lemma 7.5], as part of the Uhlmann instance, and pad the verifier register V^i with additional qubits so that V^i and $M^i P^i$ have the same number n of qubits. To help with readability, we do not do this explicitly in the proof.

¹⁶Note that of course not every successful prover has to implement the Uhlmann transformation. The important point is that we can implement *some* successful prover in this way, and the guarantee of the interactive protocol applies to any successful prover.

and we are applying it on the state $|\psi_x\rangle$ for which the guarantee of the `avgUnitaryQIP`-problem (\mathcal{U}, Ψ) holds, it follows that the query circuit produces the correct state. \square

Combining [Lemma 7.2](#) and [Lemma 7.5](#), we immediately obtain the following theorem.

Theorem 7.6. *The distributional unitary synthesis problem $\text{DISTSUCCINCTUHLMANN}_1$ is complete for `avgUnitaryQIP`.*

7.1.3 Proof of approximate measurement protocol ([Lemma 7.1](#))

To conclude this subsection, we need to prove [Lemma 7.1](#), which we used in [Lemma 7.2](#). The key insight, first observed in [\[RY22\]](#), will be that given copies of a pure state, the verifier can approximately perform the projection onto the pure state via density matrix exponentiation, described below.

Lemma 7.7 (Density Matrix Exponentiation [\[LMR14, KLL⁺17\]](#)). *Let $t \in \mathbb{R}$. There exists a quantum polynomial-time algorithm DME that takes as input registers $\text{AC}_{[m]}$ and outputs register A with the following guarantee: if the input registers are in state $\tau_{\text{AB}} \otimes \rho_{\text{C}_{[m]}}^{\otimes k}$, where B is an arbitrary purifying register on which the algorithm does not act and ρ is an n -qubit mixed state, then the output state σ_{AB} of the algorithm satisfies*

$$\text{td}(\sigma_{\text{AB}}, (W_{\text{A}} \otimes \text{id}_{\text{B}})\tau_{\text{AB}}(W_{\text{A}}^\dagger \otimes \text{id}_{\text{B}})) \leq O(t^2/k), \text{ where } W = e^{2\pi i t \cdot \rho}.$$

Let U_{DME} be a unitary dilation of DME, so that applying U_{DME} and tracing out all registers except for A yields σ_{AB} in the lemma statement above. Although not proven here, following from the implementation in [\[LMR14\]](#), DME does not act on an ancilla register. Then there is a quantum polynomial time algorithm that implements a controlled DME operation, on a control register R , which implements the following unitary

$$C_{\text{R}} \text{DME} = |0\rangle\langle 0|_{\text{R}} \otimes \text{id} + |1\rangle\langle 1|_{\text{R}} \otimes (U_{\text{DME}})_{\text{AC}_{[m]}}.$$

We now describe the *approximate measurement* protocol, mentioned in [Lemma 7.1](#), which uses the controlled $C_{(\cdot)}$ DME operation as a subroutine. Let k_q be the number of copies of the “program state” ρ needed to implement DME to trace distance error $1/(10q(n))$.

Protocol 3. Approximate measurement

Input: A classical string x that is a succinct representation of a polynomial-space circuit C , acting on n qubits, that prepares some state $|\psi_x\rangle = |C\rangle$, and a quantum register A .

1. Perform the `stateQIP` protocol for preparing $|\psi_x\rangle^{\otimes k_q}$ in register $\text{C}_{[m]}$ with soundness error $1/(10q(n))$. If the protocol rejects, reject.
2. If the `stateQIP` protocol accepts:
 - (a) Prepare ancilla qubit $|+\rangle_{\text{N}}$.
 - (b) Perform C_{N} DME on registers $\text{AC}_{[m]}$ with $t = \frac{1}{2}$.
 - (c) Measure N with the POVM $\{|+\rangle\langle +|, |-\rangle\langle -|\}$. Accept and output register A and the result of the measurement (0 for the first outcome, 1 for the second).

Lemma 7.8 (Approximate measurement completeness). *There exists an honest prover P^* such that when V implements Protocol 3,*

$$\Pr[V(\tau_{\text{AB}}) \stackrel{P^*}{\Leftarrow} \text{ accepts}] = 1.$$

Proof. The honest prover implements the honest stateQIP protocol for $|\psi_x\rangle^{\otimes k_q}$ with completeness error 2^{-n} . By the completeness of stateQIP, the verifier accepts with probability 1 during the stateQIP protocol. Hence, the verifier accepts with probability 1. \square

Corollary 7.9 (Approximate measurement honest prover output probability). *For the honest prover P^* , when the input state is $|\psi_x\rangle\langle\psi_x|_{\text{A}} \otimes \rho_{\text{B}}$ for some state ρ_{B} ,*

$$\Pr[V(|\psi_x\rangle\langle\psi_x|_{\text{A}} \otimes \rho_{\text{B}}) \stackrel{P^*}{\Leftarrow} \text{ outputs } 1] \geq 1 - 2^{-n}.$$

Proof. We first describe the DME protocol in more detail (see [LMR14] for a full description). The protocol involves performing partial SWAP gates ($e^{-i\Delta t \text{SWAP}}$) with a well-chosen value of Δt . From [LMR14, Equation (1)], the action of the partial SWAP gate on one of the input registers is given by

$$\text{Tr}_{\text{P}}(e^{-i\Delta t S} ((\rho)_{\text{P}} \otimes (\sigma)_{\text{Q}}) e^{i\Delta t S}) = \cos^2(\Delta t)\sigma + \sin^2(\Delta t)\rho - i \sin(\Delta t)[\rho, \sigma], \quad (7.4)$$

whence it follows that when $\rho = \sigma = |\psi_x\rangle\langle\psi_x|$, the DME algorithm implements the identity operation. Hence, if the verifier's state after step 1 was exactly $|\psi_x\rangle^{\otimes k_q+1}$, it would accept with probability 1.

By the completeness property of the honest prover (for stateQIP), the state of the verifier's system after step 1 is within 2^{-n} of $|\psi_x\rangle^{\otimes k_q+1}$ in trace distance. Since step 2 of the protocol can be thought of as a single measurement, the probability that the verifier accepts after interacting with the honest prover is at least $1 - 2^{-n}$. \square

Lemma 7.10 (Approximate measurement soundness). *For all provers P that are accepted by the verifier with probability at least $1/2$,*

$$|\Pr[V(\tau_{\text{AB}}) \stackrel{P}{\Leftarrow} \text{ outputs } 1] - \text{Tr}(|\psi_x\rangle\langle\psi_x| \otimes \text{id})\tau| \leq \delta(|x|). \quad (7.5)$$

Furthermore if the verifier outputs 1 with probability at least $1/2$, conditioned on accepting and outputting 1, the verifier outputs a state τ_{acc} satisfying

$$\text{td}(\tau_{\text{acc}}, \tau|_{\psi_x \otimes \text{id}}) \leq 1/q(n). \quad (7.6)$$

Proof. By the stateQIP soundness property, conditioned on accepting with probability at least $1/2$, the verifier holds a state within $1/(10q(n))$ of $|\psi_x\rangle\langle\psi_x|^{\otimes k_q}$ in \mathbb{C} . Let ρ_1 be the state of \mathbb{C} after interacting with the prover on step 1 and accepting. Define the following unitary W

$$W = e^{i\pi|\psi_x\rangle\langle\psi_x|} = \text{id} - 2|\psi_x\rangle\langle\psi_x|.$$

W is the unitary that DME will approximate when $\rho = |\psi_x\rangle\langle\psi_x|$ and $t = 1/2$ in Lemma 7.7. Now define the following states.

$$\begin{aligned} \sigma &= C_{\text{N}} \text{DME}(|+\rangle\langle+|_{\text{N}} \otimes \tau_{\text{AB}} \otimes (\rho_1)_{\text{C}}), \\ \sigma' &= C_{\text{N}} \text{DME}(|+\rangle\langle+|_{\text{N}} \otimes \tau_{\text{AB}} \otimes (|\psi_x\rangle\langle\psi_x|)_{\text{C}}), \\ \sigma^* &= \frac{1}{2} \left(|0\rangle\langle 0|_{\text{N}} \otimes \tau_{\text{AB}} + |1\rangle\langle 1|_{\text{N}} \otimes (W\tau W^\dagger)_{\text{AB}} + |0\rangle\langle 1|_{\text{N}} \otimes (\tau W^\dagger)_{\text{AB}} + |1\rangle\langle 0|_{\text{N}} \otimes (W\tau)_{\text{AB}} \right). \end{aligned}$$

Note that σ is the state the algorithm will hold after step 2(b), σ' is the state the verifier would hold if it could do perfect state preparation of $|\psi_x\rangle\langle\psi_x|$ in step 1, and σ^* is the state the verifier would hold if it could perform W on A instead of performing C_N DME with perfect program states. From the `stateQIP` soundness property,

$$\text{td}(\sigma, \sigma') \leq \frac{1}{10q(n)}$$

and from [Lemma 7.7](#),

$$\text{td}(\sigma', \sigma^*) \leq \frac{1}{10q(n)}.$$

Combining these with the triangle inequality yields

$$\text{td}(\sigma, \sigma^*) \leq \frac{1}{5q(n)}. \quad (7.7)$$

It suffices to show the following claim about the ideal state σ^* .

Claim 7.11. *Measuring the POVM $\{|+\rangle\langle+|, |-\rangle\langle-|\}$ on σ^* yields outcome 1 with probability*

$$\text{Tr}(|\psi_x\rangle\langle\psi_x| \otimes \text{id})\tau.$$

and the state of register A after measuring the POVM on σ^ and seeing outcome $|-\rangle\langle-|$ is $\tau|_{\psi_x \otimes \text{id}}$.*

We can assume that τ is a pure state since we can take B to be a purifying register, so let $\tau = |\phi\rangle\langle\phi|_{AB}$ be a pure state. Since W has 2 eigenvalues, with corresponding eigenspaces $|\psi_x\rangle\langle\psi_x| \otimes \text{id}$ and $\text{id} - |\psi_x\rangle\langle\psi_x| \otimes \text{id}$, consider the following decomposition of $|\phi\rangle$ in the $\{|\psi_x\rangle\langle\psi_x|_A \otimes \text{id}_B, \text{id} - |\psi_x\rangle\langle\psi_x|_A \otimes \text{id}_B\}$ subspaces

$$|\phi\rangle = \alpha|\phi_\psi\rangle + \beta|\phi_\perp\rangle.$$

It is clear from the definition of σ^* that σ^* is a pure state when τ is a pure state. Then we can express $\sigma^* = |\phi^*\rangle\langle\phi^*|$ as a pure state (in ket notation) as

$$|\phi^*\rangle = \frac{1}{\sqrt{2}}|0\rangle_N \otimes (\alpha|\phi_\psi\rangle + \beta|\phi_\perp\rangle)_{AB} + \frac{1}{\sqrt{2}}|1\rangle_N \otimes (-\alpha|\phi_\psi\rangle + \beta|\phi_\perp\rangle)_{AB}.$$

Re-arranging terms, we get

$$|\phi^*\rangle = \beta|+\rangle_N \otimes |\phi_\perp\rangle_{AB} + \alpha|-\rangle_N \otimes |\phi_\psi\rangle_{AB}.$$

Then it is clear that the probability of seeing outcome $|-\rangle\langle-|$ when measuring the POVM $\{|+\rangle\langle+|_N, |-\rangle\langle-|_N\}$ is

$$|\alpha^2| = \text{Tr}(|\psi_x\rangle\langle\psi_x|_A \tau_{AB}).$$

Thus, the measurement yields outcome 1 with the desired probability. With the trace distance bound from [Equation \(7.7\)](#), we have [Equation \(7.5\)](#). Furthermore the state of registers AB after measuring the POVM on σ^* and seeing outcome $|-\rangle\langle-|$ is

$$|\phi_\psi\rangle\langle\phi_\psi| = \tau|_{\psi_x \otimes \text{id}}.$$

Our goal now is to bound the post-measurement state when measuring $|-\rangle\langle-|$ on σ instead of σ^* . Before doing this, we prove a useful inequality relating the post-measurement state of states that

start out close. Let ρ and ρ' be any two states satisfying $\text{td}(\rho, \rho') \leq \delta \leq 1/4$, and $\text{Tr}(\Pi\rho) \geq 1/2$ for some projector Π . Then we have that

$$\begin{aligned} \text{td}(\rho|_{\Pi}, \rho'|_{\Pi}) &\leq \frac{1}{\text{Tr}(\Pi\rho)} \text{td}\left(\Pi\rho\Pi, \Pi\rho'\Pi \frac{\Pi\rho}{\Pi\rho'}\right) \\ &\leq 2\text{td}(\rho, \rho'(1+4\delta)) \\ &\leq \|\rho - \rho'(1+4\delta)\|_1 \\ &\leq \|\rho - \rho'\|_1 + 4\delta\|\rho'\|_1 \\ &\leq 5\delta. \end{aligned}$$

Here the second line results from the fact that $\text{Tr}(\Pi\rho') \geq \text{Tr}(\Pi\rho) - \delta$, so

$$\begin{aligned} \frac{\text{Tr}(\Pi\rho)}{\text{Tr}(\Pi\rho')} &\leq \frac{\text{Tr}(\Pi\rho)}{\text{Tr}(\Pi\rho) - \delta} = \frac{1}{1 - \delta/\text{Tr}(\Pi\rho)} \\ &\leq 1 + 2\delta/\text{Tr}(\Pi\rho) \\ &\leq 1 + 4\delta. \end{aligned}$$

Here the last line uses the fact that for $x \leq 1/2$, we have $\frac{1}{1-x} \leq 1 + 2x$, and the assumption that $\text{Tr}(\Pi\rho) \geq 1/2$. The rest of the lines apply the definition of trace distance and the triangle inequality for the 1-norm. In the calculations above, let $\rho = \sigma$, $\rho' = \sigma^*$, and $\Pi = |-\rangle\langle -|$. We have shown that

$$\sigma^*|_{|-\rangle\langle -|} = \tau|_{\psi_x \otimes \text{id}} \quad \text{and} \quad \text{td}(\sigma, \sigma^*) \leq 1/(5q(n)),$$

and by the assumption that $\text{Tr}(|\psi_x\rangle\langle\psi_x|_{\mathbb{A}} \tau_{\text{AB}}) \geq 1/2$, we have that

$$\text{Tr}(|-\rangle\langle -|_{\mathbb{N}} \sigma^*) \geq \frac{1}{2}.$$

Putting these together with the definition of $\tau_{\text{acc}} = \sigma|_{|-\rangle\langle -|}$, we have that

$$\text{td}(\tau_{\text{acc}}, \tau|_{\psi_x \otimes \text{id}}) \leq \frac{1}{q(n)}.$$

This completes the proof of the lemma. □

Finally we combine the previous lemmas to prove [Lemma 7.1](#).

Proof of Lemma 7.1. [Lemma 7.8](#) and [Corollary 7.9](#) prove completeness. [Lemma 7.10](#) proves soundness. □

7.2 Completeness for avgUnitaryPSPACE

Having shown that $\text{DISTSUCCINCTUHLMANN}_1$ is complete for avgUnitaryQIP, we will now show that it is also complete for avgUnitaryPSPACE. Together, this implies that avgUnitaryQIP = avgUnitaryPSPACE ([Corollary 7.13](#)).

Theorem 7.12. *DISTSUCCINCTUHLMANN₁ is complete for avgUnitaryPSPACE.*

Proof. We first show that $\text{DISTSUCCINCTUHLMANN}_1 \in \text{avgUnitaryPSPACE}$. This is essentially a restatement of [MY23, Theorem 7.4], but re-written using notation defined in this paper. An instance U_x of SUCCINCTUHLMANN_1 is specified by a succinct description of a pair of unitary circuits (C_x, D_x) on $n = \text{poly}(|x|)$ qubits. This means that the space complexity of C_x and D_x is $\text{poly}(|x|)$, so the state families $|\psi_x\rangle_{\text{AB}} = C_x |0^{2n}\rangle_{\text{AB}}$ and $|\phi_x\rangle = D_x |0^{2n}\rangle_{\text{AB}}$ are in statePSPACE (where A, B have n qubits each, and C_x, D_x act only on B). Then, [MY23, Theorem 7.4] states that there exist a family of unitaries $(K_x)_x \in \text{unitaryPSPACE}$ that performs the Uhlmann transformation between the state families $|\psi_x\rangle$ and $|\phi_x\rangle$. More formally, for any polynomial p , $(|\psi_x\rangle)_x, (|\phi_x\rangle)_x \in \text{statePSPACE}_{1/p}$, and $F(\rho_x, \sigma_x) = 1$, where ρ_x and σ_x are the reduced density matrices of $|\psi_x\rangle_{\text{AB}}$ and $|\phi_x\rangle_{\text{AB}}$ on register A , it holds that $\text{td}\left((\text{id} \otimes K_x) |\psi_x\rangle\langle\psi_x| (\text{id} \otimes K_x^\dagger), |\phi_x\rangle\langle\phi_x|\right) \leq O(1/p(|x|))$. This implies that $\text{DISTSUCCINCTUHLMANN}_1 \in \text{avgUnitaryPSPACE}$.¹⁷

We now need to show that any distributional unitary synthesis problem $(\mathcal{U} = (U_x)_x, \Psi = (|\psi_x\rangle)_x) \in \text{avgUnitaryPSPACE}$ can be reduced to a succinct Uhlmann problem in the sense of Definition 3.21. The idea for this is simple, though the formalisation is slightly tedious: to implement $(\mathcal{U} = (U_x)_x, \Psi = (|\psi_x\rangle)_x)$, we can simply run the Uhlmann transformation between $|\psi_x\rangle$ and $U_x |\psi_x\rangle$. Since $\Psi \in \text{statePSPACE}$, $U_x |\psi_x\rangle$ is too, so we can efficiently construct a string y that describes this Uhlmann instance. Further note that their reduced states on the first half of the qubits are identical, since U_x only acts on the second half of qubits. With access to a $\text{DISTSUCCINCTUHLMANN}_1$ -oracle, we can therefore implement this Uhlmann transformation, and as a result implement any unitary synthesis problem $(\mathcal{U}, \Psi) \in \text{avgUnitaryPSPACE}$.

To show this formally, we fix any polynomial $q(n)$ and need to construct a quantum query algorithm $C^* = (C_x^*)_x$ and a polynomial $r(n)$ such that all $1/r(n)$ -error average case instantiations of $C^{\text{DISTSUCCINCTUHLMANN}_1}$ implement (\mathcal{U}, Ψ) with average-case error $1/q(n)$.

Since $(\mathcal{U}, \Psi) \in \text{avgUnitaryPSPACE}$, by definition $\Psi = (|\psi_x\rangle)_x \in \text{statePSPACE}$, i.e. there exists a family of space-uniform circuits $S = (S_x)$ on $2n = \text{poly}(|x|)$ qubits such that $|\psi'_x\rangle := S_x |0^{2n}\rangle$ is $1/q'(|x|)$ -close in trace distance to $|\psi_x\rangle$ for $q'(n)$ a polynomial (dependent on q) that we will choose later. Let $A = (A_x)_x$ denote the space-uniform quantum algorithm that implements (\mathcal{U}, Ψ) with average-case error $1/q'(n)$. Define the circuit T_x to be the concatenation of $\text{id} \otimes A_x$ and S_x (i.e. it implements $(\text{id} \otimes A_x)S_x$), which is space-uniform since A and S are space-uniform. Since both S_x and T_x are space-uniform circuits on at most $2n$ qubits, this means that, given x , we can efficiently construct a string y such that $y = (1^n, \hat{S}, \hat{T})$ is a valid succinct Uhlmann instance (Definition 5.5) for the family of circuit pairs (S, T) . We therefore define the following family of quantum query circuits: C_x^* contains a single oracle gate acting on n qubits with label y , where $y = (1^n, \hat{S}, \hat{T})$ is a valid succinct Uhlmann instance constructed from x as described before. Since y can be efficiently computed from x , $(C_x^*)_x$ is a time-uniform family of quantum query circuits.

By assumption, there exists a channel completion Φ_x of U_x such that

$$\text{td}\left((A_x \otimes \text{id})(\psi_x), (\Phi_x \otimes \text{id})(\psi_x)\right) \leq 1/q'(n).$$

Furthermore, by construction the Uhlmann unitary for circuits S_x and T_x applied to the state $|\psi'_x\rangle = S_x |0^{2n}\rangle$ produces the state $T_x |0^{2n}\rangle = (A_x \otimes \text{id}) |\psi'_x\rangle$. Therefore, considering a $1/r(n)$ -error average case instantiation $C^{\text{DISTSUCCINCTUHLMANN}_1}$ and using $\text{td}(\psi_x, \psi'_x) \leq 1/q'(n)$, we can apply the

¹⁷Note that [MY23] does not employ the language of average case unitary complexity classes, but their phrasing of “there exists a unitary in unitaryPSPACE that performs the Uhlmann transformation on these specific states” is equivalent to our definition of average case unitary classes.

triangle inequality to get

$$(\text{id} \otimes C_x^{\text{DISTSUCCINCTUHLMANN}_1})(\psi_x) = (\text{id} \otimes A_x)(\psi_x) \leq 1/r(n) + 2/q'(n).$$

Choosing $r(n) = q'(n) = 4q(n)$ and combining these two statements with the triangle inequality, this means that $C_x^{\text{DISTSUCCINCTUHLMANN}_1}$ implements U_x (for channel completion Φ_x) with average-case error $1/q(n)$ as desired. \square

We are now in a position to prove that `avgUnitaryQIP` and `avgUnitaryPSPACE` are in fact equal. This answers an average-case version of an open problem raised in [RY22, MY23], namely whether `unitaryQIP = unitaryPSPACE`, and is one of the first non-trivial results on relations between unitary complexity classes. It also highlights the utility of having complete problems for unitary complexity classes, just like complete problems for traditional complexity classes are an invaluable tool for relating classes to one another.

Corollary 7.13. `avgUnitaryPSPACE = avgUnitaryQIP`.

Proof. This follows immediately from the fact that `DISTSUCCINCTUHLMANN` is complete both for `avgUnitaryQIP` and `avgUnitaryPSPACE`. \square

While this resolves the question in the average case, the worst-case version of this question remains open:

Open Problem 14. Does it hold that `unitaryQIP = unitaryPSPACE`?

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

Open Problem 15. `SUCCINCTUHLMANN` \in `unitaryBQPPSPACE`? This is a “dual” statement to [Theorem 7.12](#). 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 $f : \{0, 1\}^{\text{poly}(n)} \rightarrow \{0, 1\}$ such that the unitary U can be implemented by A^{fU} .

7.3 Completeness for worst-case unitaryPSPACE

Most of the results in this paper that we have seen so far – and the ones that follow – focus on the complexity of the distributional Uhlmann Transformation Problem and average-case unitary complexity classes such as `avgUnitaryBQP` and `avgUnitaryPSPACE`. As mentioned previously, average-case unitary complexity classes are natural for studying problems where the goal is to locally transform one entangled state to another.

However the “worst-case” unitary synthesis problems like `UHLMANN` and “worst-case” unitary complexity classes such as `unitaryBQP` and `unitaryPSPACE` are natural in their own right, and there are many interesting questions about them. For example, is `UHLMANN` complete for a natural worst-case unitary complexity classes? Is `unitaryQIP = unitaryPSPACE`, just like `avgUnitaryQIP = avgUnitaryPSPACE`?

Here we describe a result about worst-case unitary complexity: `SUCCINCTUHLMANN` is complete for `unitaryPSPACE`, complementing the completeness of `DISTSUCCINCTUHLMANN` for `avgUnitaryPSPACE`. We sketch the argument for this, and leave a deeper exploration of worst-case unitary complexity classes, and the questions mentioned above, to future work.

Theorem 7.14. $\text{SUCCINCTUHLMANN}_{1,\eta}$ is complete for unitaryPSPACE for cutoff parameter $\eta = 2^{-2n}$.

Recall that the unitary synthesis problems UHLMANN and SUCCINCTUHLMANN are parameterized by a cutoff parameter η , which is used to make the definition of the canonical Uhlmann isometry (see [Definition 5.2](#)) more robust. As discussed at the end of [Section 5](#), the cutoff parameter is set to 0 for the distributional problems DISTUHLMANN and $\text{DISTSUCCINCTUHLMANN}$. However the cutoff parameter is important for discussing the worst-case complexity of the Uhlmann Transformation Problem.

Proof sketch. First we sketch the hardness result; i.e., that $\text{SUCCINCTUHLMANN}_{1,\eta}$ is hard for unitaryPSPACE . Let A denote a polynomial space quantum algorithm that implements a unitary synthesis problem $\mathcal{U} \in \text{unitaryPSPACE}$. Suppose for simplicity that A is a unitary algorithm (i.e., it consists only of unitary gates). Fix an instance size n , and consider the following two states: let $|C\rangle$ denote the maximally entangled state on n qubits, and let $|D\rangle$ denote the state obtained by applying A on half of the maximally entangled state. Clearly $(|C\rangle, |D\rangle)$ are computable in polynomial space and thus $(1^n, \hat{C}, \hat{D})$ are valid SUCCINCTUHLMANN_1 instances. The canonical Uhlmann isometry W with cutoff η corresponding to $(|C\rangle, |D\rangle)$ is exactly the unitary A , which can be seen as follows:

$$W = \text{sgn}_\eta(\text{Tr}_A(|D\rangle\langle C|)) = \text{sgn}_\eta(\text{Tr}_A((\text{id} \otimes A)|C\rangle\langle C|)) = \text{sgn}_\eta(2^{-n}A) = A$$

where we used that $2^{-n} \geq \eta$. Thus implementing this Uhlmann transformation with inverse polynomial error can be used to implement \mathcal{U} to inverse polynomial error. In the case that A is not a unitary circuit, we can leverage the fact that a *purification* of the mixed state $(\text{id} \otimes A)(|C\rangle\langle C|)$ can be synthesized in polynomial space; this uses the fact that statePSPACE is closed under purification [[MY23](#), Theorem 6.1].

Next we sketch the containment of $\text{SUCCINCTUHLMANN}_{1,\eta}$ in unitaryPSPACE . This follows from an average-case-to-worst-case reduction. Let $(1^n, \hat{C}, \hat{D})$ be a valid SUCCINCTUHLMANN_1 instance. Then [[MY23](#), Theorem 7.4], which was also used to prove that $\text{DISTSUCCINCTUHLMANN}_1 \in \text{avgUnitaryPSPACE}$, implies that there is a polynomial space algorithm A such that

$$\text{td}\left((\text{id} \otimes A)(|C\rangle\langle C|), |D\rangle\langle D|\right) \leq 2^{-4n}.$$

We claim that the algorithm A actually implements with small *worst-case error* the canonical Uhlmann isometry with cutoff η corresponding to $(|C\rangle, |D\rangle)$. Since the reduced density matrices of $|C\rangle$ and $|D\rangle$ on the first n qubits are identical we can write the Schmidt decompositions of $|C\rangle, |D\rangle$ as

$$|C\rangle = \sum_i \sqrt{p_i} |v_i\rangle \otimes |s_i\rangle, \quad |D\rangle = \sum_i \sqrt{p_i} |v_i\rangle \otimes |t_i\rangle$$

for some orthonormal bases $\{|v_i\rangle\}, \{|s_i\rangle\}, \{|t_i\rangle\}$. Imagine measuring the first n qubits of $(\text{id} \otimes A)(|C\rangle\langle C|)$ and $|D\rangle\langle D|$ in the $\{|v_i\rangle\}$ basis; then by the convexity of the trace distance we get

$$\sum_i p_i \text{td}\left(A(|s_i\rangle\langle s_i|), |t_i\rangle\langle t_i|\right) \leq 2^{-4n}.$$

It must be that for every i such that $p_i \geq 2^{-2n}$ we have $\text{td}\left(A(|s_i\rangle\langle s_i|), |t_i\rangle\langle t_i|\right) \leq 2^{-2n}$; otherwise the total error would exceed 2^{-4n} . The canonical Uhlmann isometry with cutoff η corresponding to $(|C\rangle, |D\rangle)$ can be calculated to be

$$W = \sum_{i:p_i \geq \eta} |t_i\rangle\langle s_i| .$$

Since A maps $|s_i\rangle$ to $|t_i\rangle$ with error 2^{-2n} for every i with $p_i \geq \eta$, this implies that A approximates W with exponentially small error. (Additional care has to be taken to show that A coherently maps $|s_i\rangle$ to $|t_i\rangle$, but this follows from the fact that A maps $|C\rangle$ to $|D\rangle$.) \square

7.4 Relationship between avgUnitaryPSPACE and PSPACE

We now turn our attention to the relationship between avgUnitaryPSPACE and “traditional” worst-case PSPACE, which will again involve the $\text{DISTSUCCINCTUHLMANN}_1$ problem. We will show that even though avgUnitaryPSPACE is a class of distributional (average-case) unitary synthesis problems, it is “harder” than PSPACE. At first blush, this seems like it should not be true because the average case solver is allowed an inverse polynomial error on the distributional input; meaning, if the input is sampled randomly from instances of a PSPACE-complete problem, the average case solver can be incorrect on a large fraction of them. However, we show that languages in PSPACE are computable in polynomial time, given oracle access to $\text{DISTSUCCINCTUHLMANN}_1$. A general definition for a reduction between a decision problem and average case unitary synthesis problem can easily be extracted from the proposition.

The key idea is to take advantage of the *nonadaptive random-self-reducibility* of PSPACE. Informally, a language satisfies nonadaptive random-self reducibility if there exists a series of *fixed* distributions over inputs such any algorithm that decides the language with high probability over that distribution can be used to decide the language for all instances. More formally, Fortnow and Feigenbaum showed [FF93, Corollary 4.4] that there exists a PSPACE-complete language L satisfying the following: there exists a polynomial $m(n)$ such that for all $n \in \mathbb{N}$,

- (i) there exist $m = m(n)$ polynomial-time computable functions $\{\sigma_i\}$ that each take as input randomness $r \in \{0, 1\}^m$ and an instance $x \in \{0, 1\}^n$, and
- (ii) there exists a polynomial-time computable function ϕ that takes as input randomness $r \in \{0, 1\}^m$, an instance $x \in \{0, 1\}^n$, and answers $y \in \{0, 1\}^m$,

such that for all instances $x \in \{0, 1\}^n$

$$\Pr_r[\phi(r, x, f_L(z_1), \dots, f_L(z_m)) = f_L(x)] \geq \frac{3}{4}$$

where f_L is the characteristic function of L and $z_i = \sigma_i(r, x)$. Additionally, for all $x_1, x_2 \in \{0, 1\}^n$, when r is chosen uniformly at random, $\sigma_i(x_1, r)$ is identically distributed to $\sigma_i(x_2, r)$.

Theorem 7.15. *Let $L \in \text{PSPACE}$. There exists a polynomial time query algorithm $C^* = (C_x^*)_x$ and a polynomial p such that for all $x \in \{0, 1\}^n$, all $1/p(n)$ -error average-case instantiations $C_x^{\text{DISTSUCCINCTUHLMANN}}$ accept with probability at least $2/3$ (completeness), and for all $x \notin L$, all $1/p(n)$ -error average case instantiations accept with probability at most $1/3$ (soundness).*

Proof. At a high level, recall that a language satisfies random-self-reducibility if there exists efficiently sample distributions such that given the answer to f_L on those instances, the answer to $f_L(x)$ can be determined efficiently. We transform this property into a `DISTSUCCINCTUHLMANN` instance by having the first circuit (denoted A) sample the fixed distributions (where the A purifies the system by holding a uniform superposition over the randomness). The second circuit (denoted B) simply samples the fixed distribution, and also appends the answers for each instance in another register. Recall that in `DISTSUCCINCTUHLMANN`, we give succinct representations of circuits, so generating the succinct representation of B can be done efficiently (even though implementing B would likely take exponential time). It is clear that solving `DISTSUCCINCTUHLMANN` on the distributional input with 0-error and measuring the system would yield an input sampled from the fixed distribution, together with the corresponding values of f_L , which would be used to get the answer for the original instance with high probability. We now make this intuition formal.

Let L be a `PSPACE`-complete language that is non-adaptively random-self reducible. Then there exist polynomial-time computable functions ϕ_L and $\{\sigma_{L,i}\}$ satisfying the conditions from the definition of nonadaptive random-self-reducibility above.

Because all $\sigma_{L,i}$ run in polynomial time in the length of x , there is a polynomial time quantum circuit A that prepares the following state

$$A|0\rangle = \sum_{r \in \{0,1\}^m} |r\rangle_{\mathbf{A}} \otimes |\sigma_{L,1}(r, x), \sigma_{L,2}(r, x), \dots, \sigma_{L,m}(r, x)\rangle_{\mathbf{B}} \otimes |0^m\rangle_{\mathbf{C}}.$$

As described in the high level description, the \mathbf{B} register stores the samples from the fixed distributions $\sigma_{L,i}$, and the \mathbf{A} register purifies the system by storing the randomness used to generate the samples. It is important to note that A is polynomial sized, so a polynomial time quantum algorithm can generate a copy of $A|0\rangle$.

Since $L \in \text{PSPACE}$, there exists a polynomial space Turing machine M_L that decides the language. For every input of length n , this Turing machine can be turned into a succinct representation of a circuit $C_{L,n}$ that implements the characteristic function f_L for inputs of length n via standard Turing machine to circuit reductions. Therefore there exists an efficient algorithm preparing a succinct representation of a quantum circuit B that prepares the following state

$$B|0\rangle = \sum_{r \in \{0,1\}^m} |r\rangle_{\mathbf{A}} \otimes |\sigma_{L,1}(r, x), \sigma_{L,2}(r, x), \dots, \sigma_{L,m}(r, x)\rangle_{\mathbf{B}} \otimes |C_{L,n}(\sigma_{L,1}(r, x)), \dots, C_{L,n}(\sigma_{L,m}(r, x))\rangle_{\mathbf{C}}.$$

In order to fully align with the definitions, the circuits can be padded with an additional ancillary register initialized to $|0\rangle$ so that the size of \mathbf{BC} is the same as \mathbf{A} (because `SUCCINCTUHLMANN`, as defined, implements a n -qubit channel, where the inputs specify $2n$ -qubit states). Let \hat{x} be the classical string $(1^n, \hat{A}, \hat{B})$. Finally, let $\phi_{L,x}$ be a polynomial time quantum circuit implements the function ϕ_L when the input x is hard coded, i.e.

$$\phi_{L,x} |r, b_1, b_2, \dots, b_m, l\rangle = |r, b_1, b_2, \dots, b_m, l \oplus \phi_L(x, r, b_1, b_2, \dots, b_m)\rangle$$

Then, the following family of polynomial-time query circuits $(C_x^*)_x$ decides L .

Protocol 4. $\text{BQP}^{\text{DISTSUCCINCTUHLMANN}_1}$ protocol for $L \in \text{PSPACE}$

Input: Classical string x .

1. Prepare a copy of $A|0\rangle$ on registers ABC .
2. Call the $\text{DISTSUCCINCTUHLMANN}_1$ oracle on quantum registers BC with classical input \hat{x} .
3. Let O be a single qubit register in the $|0\rangle$ state. Run $\phi_{L,x}$ on registers ACO .
4. Measure O in the computational basis and accept if the measurement outcome is 1.

In order to prove the proposition, we will show that, when instantiated with a 0-error average case $\text{DISTSUCCINCTUHLMANN}_1$ oracle, Protocol 4 decides L with completeness $3/4$ and soundness $1/4$. Then by the operational definition of the trace distance, even when instantiated with a $1/12$ -error average case solver, the protocol still accepts with probability at least $3/4 - 1/12 = 2/3$ if $x \in L$ and at most probability $1/3$ if $x \notin L$.

Assume that the call to $\text{DISTSUCCINCTUHLMANN}$ in Protocol 4 is instantiated with a 0-error average case solver. Then we can write the state of registers $ABCO$ after step 3 in the protocol as

$$\sum_r |r\rangle_A \otimes |\sigma_{L,1}(r,x), \dots, \sigma_{L,1}(r,x)\rangle_B \otimes |C_{L,n}(\sigma_{L,1}(r,x)), \dots, C_{L,n}(\sigma_{L,m}(r,x))\rangle_C \otimes |\phi_L(x,r, C_{L,n}\sigma_{L,1}(r,x), \dots, C_{L,n}\sigma_{L,m}(r,x))\rangle_O \quad (7.8)$$

The probability that the protocol accepts in step 4 is exactly the probability that, when r is chosen uniformly at random, ϕ_L outputs the outputs 1 when run on x, r and f_L applied to each $\sigma_{L,i}(r,x)$. By the definition of nonadaptive random-self-reducibility, ϕ_L is correct with probability $3/4$. Thus, when $x \in L$, $f_L(x) = 1$, so with probability at least $3/4$, the protocol accepts. Similarly if $x \notin L$, $f_L(x) = 0$, so with probability at most $1/4$ the protocol accepts.

Now, assume that Protocol 4 is instantiated with a $1/12$ -error average case solver instead. By the definition of $1/12$ -error solver and the fact that unitaries preserve trace distance, the state of the protocol after step 3 is within $1/12$ of the state in Equation 7.8, in trace distance. Then, for any measurement M , the probability that M accepts on the protocol state is within $1/12$ of the probability that M accepts on the state in Equation 7.8. So if $x \in L$, the protocol accepts with probability at least $2/3$, and if $x \notin L$, the protocol accepts with probability at most $1/3$. \square

In this section, we have used the random self-reducibility of PSPACE to relate avgUnitaryPSPACE and PSPACE . It is natural to wonder whether a similar self-reducibility property also holds for unitaryPSPACE itself, and in particular whether SUCCINCTUHLMANN might be randomly self-reducible as a unitary synthesis problem:

Open Problem 16. Is SUCCINCTUHLMANN randomly self reducible (in some suitably defined sense), in analogy to randomly self-reducible PSPACE -complete problems?

Part III

Uhlmann Transformation Problem: Applications

8 Applications to Quantum Cryptography

In this section, we connect the Uhlmann Transformation Problem to concepts in quantum cryptography. We first discuss an equivalence between the existence of quantum commitment schemes and the hardness of the Uhlmann Transformation Problem. Then, we relate the problem of breaking (a class of) one-way state generators, a primitive recently introduced by Morimae and Yamakawa [MY22b], to solving UHLMANN_κ for *small* $\kappa \ll 1$ (whereas most of the other results we discuss in this paper concern UHLMANN_κ for κ negligibly close to 1). Finally, we show that any *falsifiable quantum cryptographic assumption* must imply that $\text{DISTSUCCINCTUHLMANN}$ cannot be solved in polynomial time. Put in other words, this essentially means that any security definition that can be phrased in terms of a security game is either information-theoretically realizable or can be broken in avgUnitaryPSPACE .

8.1 Quantum commitment schemes

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 scheme [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 $\text{poly}(\lambda)$ 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 $C_{\lambda,b}^\dagger$ 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 non-uniform polynomial-time algorithms (resp. for non-uniform 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 :*

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

Here, $\rho_{\lambda,b}$ denotes the reduced density matrix of $|\psi_{\lambda,b}\rangle$ on register \mathbf{C} . If ϵ is a negligible function of λ then we simply say that the scheme satisfies strong computational (resp. statistical) hiding. If $\epsilon(\lambda) \leq 1 - \frac{1}{p(\lambda)}$ for some polynomial $p(\lambda)$ we say it satisfies weak computational (resp. statistical) hiding.

We call the left hand side of Equation (8.1) the advantage of the family of adversaries $A = (A_\lambda)_\lambda$.

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 non-uniform polynomial-time algorithms (resp. for all non-uniform algorithms) $A = (A_\lambda)_\lambda$ that take as input the reveal register \mathbf{R} the following holds for sufficiently large λ :*

$$F\left(\left(A_\lambda \otimes \text{id}_{\mathbf{C}}\right)(\psi_{\lambda,0}), \psi_{\lambda,1}\right) \leq \epsilon(\lambda), \quad (8.2)$$

where $\psi_{\lambda,b} = |\psi_{\lambda,b}\rangle_{\mathbf{A}} \langle \psi_{\lambda,b}|_{\mathbf{RC}}$.

If ϵ is a negligible function of λ then we simply say that the scheme satisfies strong computational (resp. statistical) honest binding. Otherwise if $\epsilon(\lambda) \leq 1 - \frac{1}{p(\lambda)}$ for some polynomial $p(\cdot)$ we say that it satisfies weak 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 to include adversaries that have quantum side information, but for simplicity we focus on adversaries take classical side information (by way of the non-uniformity of the adversary’s circuits). This would require us to consider unitary complexity classes with *quantum advice*, e.g., `avgUnitaryBQP/qpoly`. 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 is 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].

Commitment flavor switching. The reduction works as follows. Let $\{C_{\lambda,b}\}_{\lambda,b}$ denote a commitment scheme. For every $\lambda \in \mathbb{N}$ and $b \in \{0, 1\}$, define the circuit $C'_{\lambda,b}$ that acts on one more qubit than $C_{\lambda,b}$ does, and produces the following state:

$$|\psi'_{\lambda,b}\rangle_{\mathbf{C}'\mathbf{R}'} := C'_{\lambda,b}|0 \cdots 0\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle_{\mathbf{A}} |\psi_{\lambda,0}\rangle_{\mathbf{RC}} + (-1)^b |1\rangle_{\mathbf{A}} |\psi_{\lambda,1}\rangle_{\mathbf{RC}} \right),$$

where $|\psi_{\lambda,b}\rangle = C_{\lambda,b}|0\cdots 0\rangle$ and the registers are $C' = RA$ and $R' = C$ (i.e., the reveal and commitment registers are swapped, and the commitment register has an extra qubit). Clearly, the circuit $C'_{\lambda,b}$ is polynomial-size if $C_{\lambda,b}$ is.

Proposition 8.7 ([HMY23, Theorem 7]). *Let $\epsilon(n), \delta(n)$ be functions. If $\{C_{\lambda,b}\}_{\lambda,b}$ is an ϵ -computationally (resp. statistical) hiding and δ -statistical (resp. computational) binding commitment scheme, then $\{C'_{\lambda,b}\}_{\lambda,b}$ is a $\sqrt{\delta}$ -statistical (resp. computational) hiding and ϵ -computationally (resp. statistical) binding commitment scheme.*

Hardness amplification for commitments. In Section 6 we proved a hardness amplification result for the Uhlmann transformation problem (Theorem 6.8). The key lemma in the proof of this result, Lemma 6.9, also implies that the computational binding property of a commitment scheme can also be amplified: roughly speaking, if there is a commitment scheme where it is hard for a malicious sender to map the 0-commitment to have fidelity more than $1 - 1/p(\lambda)$ with the 1-commitment for some polynomial $p(\lambda)$, then there exists another commitment scheme where it is hard for an adversary to map the 0-commitment to have more than $\frac{1}{q(\lambda)}$ overlap with the 1-commitment for all polynomials $q(\lambda)$. Flavor switching (Proposition 8.7) then implies hardness amplification for the hiding property (i.e., if it is somewhat hard to distinguish between commitments to 0 and 1, there is another commitment scheme for which it is much harder). This answers an open question of [Yan22], who asked whether hardness amplification for commitments is possible.

Theorem 8.8 (Amplification of quantum commitment schemes). *The following are equivalent:*

1. *Strong statistical hiding and weak computational binding commitment schemes exist.*
2. *Strong statistical binding and weak computational hiding commitment schemes exist.*
3. *For every polynomial $p(\lambda)$, strong statistical hiding and $\frac{1}{p(\lambda)}$ -computational binding commitment schemes exist.*
4. *For every polynomial $p(\lambda)$, strong statistical binding and $\frac{1}{p(\lambda)}$ -computational hiding commitment schemes exist.*

Proof. Proposition 8.7 shows that (2) \implies (1) and (3) \implies (4). Furthermore, (4) \implies (2) is trivial by definition of binding. Thus it only remains to prove (1) \implies (3).

Let $C := \{C_{\lambda,b}\}_{\lambda,b}$ be a strong statistical hiding, weak computational binding commitment scheme with corresponding commitment states $\{|\psi_{\lambda,b}\rangle\}$, and let $p(\lambda)$ be some polynomial. There exists a polynomial $q(\lambda)$ such that for all non-uniform polynomial size quantum families of circuits $\{R_\lambda\}_\lambda$ and for all sufficiently large λ it holds that

$$F\left(\left(R_\lambda \otimes \text{id}_C\right)(\psi_{\lambda,0}), \psi_{\lambda,1}\right) \leq 1 - \frac{1}{q(\lambda)}.$$

Let $\nu(\lambda) = 1/p(\lambda)$. There exist polynomials $k(\lambda), T(\lambda)$ such that

$$1 - \left(2(1 - \nu(\lambda))^{T(\lambda)} + \frac{32T(\lambda)}{\sqrt{k(\lambda)}}\right) \geq 1 - \frac{1}{q(\lambda)}$$

for all sufficiently large λ . For notational brevity we write $k = k(\lambda), T = T(\lambda), \nu = \nu(\lambda)$.

Consider the *amplified commitment scheme* $C^{\otimes k} := \{C_{\lambda,b}^{\otimes k(\lambda)}\}_{\lambda,b}$. This commitment scheme is clearly polynomial-time and uniform. Applying the contrapositive of [Lemma 6.9](#) with the circuits C, D of the lemma set to $C_{\lambda,0}, C_{\lambda,1}$ respectively, it holds for all non-uniform polynomial-time algorithms $\{A_\lambda\}_\lambda$, for all sufficiently large λ ,

$$F\left(\left(A_\lambda \otimes \text{id}_C\right)(\psi_{\lambda,0}^{\otimes k}, \psi_{\lambda,1}^{\otimes k})\right) \leq \nu = \frac{1}{p(\lambda)}$$

where the algorithm A_λ acts only on the part of the state $|\psi_{\lambda,b}\rangle^{\otimes k}$ kept by the sender after the commitment phase. Thus the original commitment C is $\frac{1}{p(\cdot)}$ -computational binding.

The amplified commitment $C^{\otimes k}$ is statistically hiding since by definition $\rho_{\lambda,0}$ and $\rho_{\lambda,1}$ (the reduced density matrices of the original commitment on register C) have trace distance at most $\text{negl}(\lambda)$ for some negligible function negl . Thus $\rho_{\lambda,0}^{\otimes k}$ and $\rho_{\lambda,1}^{\otimes k}$ (the reduced density matrices of the amplified commitment) have trace distance at most $\text{negl}(\lambda)k(\lambda)$, which is still a negligible function as $k(\lambda)$ is a polynomial.

Thus the amplified commitment scheme $C^{\otimes k}$ has statistical hiding and $\frac{1}{p(\cdot)}$ -computational binding, as required. This shows that (1) \implies (3) and thus concludes the proof of the theorem. \square

Note that [Theorem 8.8](#) is just shy of showing an equivalence between weak commitments and the standard notion of commitments in cryptography, where the adversaries can only break the hiding or binding properties with negligible advantage. To prove this stronger statement, we would need to show that weak commitments implies the existence of a *single* commitment scheme for which an adversary cannot break the binding property with more than $1/p(\lambda)$ for all polynomials p (whereas [Theorem 8.8](#) implies the existence of a commitment scheme that depends on the polynomial p). We conjecture that this stronger amplification holds:

Conjecture 8.9. *Strong statistical hiding and weak computational binding commitment schemes exist if and only if strong statistical hiding and strong computational binding commitment schemes exist.*

We note that this conjecture would essentially be implied by [Open Problem 11](#), in the same way in which [Theorem 8.8](#) is implied by [Theorem 6.8](#).

Commitments and the Uhlmann Transformation Problem. The main result of this section is a close connection between the existence of commitment schemes and the complexity-theoretic assumption that $\text{DISTUHLMANN} \notin \text{avgUnitaryBQP/poly}$.

Theorem 8.10. *If for all negligible functions ν , $\text{DISTUHLMANN}_{1-\nu} \in \text{avgUnitaryBQP/poly}$, then strong statistical hiding, weak computational binding commitments as well as strong statistical binding, weak computational hiding commitments do not exist.*

On the other hand, suppose there exists a negligible function μ such that

- (i) $\text{DISTUHLMANN}_{1-\mu} \notin \text{avgUnitaryBQP/poly}$, and
- (ii) *there exists a uniform polynomial-time computable¹⁸ family $X = \{x_\lambda\}_{\lambda \in \mathbb{N}}$ of $\text{UHLMANN}_{1-\mu}$ instances satisfying the following: there exists a polynomial $q(\lambda)$ such that for every non-uniform*

¹⁸By the uniform polynomial-time computability of X we mean the following: there exists a uniform polynomial-time quantum algorithm that on input 1^λ outputs x_λ .

polynomial-time algorithm $A = (A_\lambda)_\lambda$ where A implements the Uhlmann transformation corresponding to x_λ with error greater than $1/q(\lambda)$ for all sufficiently large λ .

Then there exist quantum commitments with strong statistical hiding and weak computational binding as well as quantum commitments with weak computational hiding and strong statistical binding.

We note that in the second part of [Theorem 8.10](#), technically speaking the assumption that $\text{DISTUHLMANN}_{1-\mu} \notin \text{avgUnitaryBQP/poly}$ is implied by the assumption about the existence of the uniform family X of “hard” instances. However we state it as such in order to highlight the close connection between quantum commitments and whether $\text{DISTUHLMANN}_{1-\text{negl}}$ is in $\text{avgUnitaryBQP/poly}$.

We also note that using hardness amplification for commitments ([Theorem 8.8](#)), the conclusion of the second part of [Theorem 8.10](#) can be revised to imply the existence of quantum commitments where the computational hiding or computational binding property holds with inverse polynomial security.

Proof of [Theorem 8.10](#). We begin with the first part of the theorem. Suppose for contradiction that $\text{DISTUHLMANN}_{1-\nu} \in \text{avgUnitaryBQP/poly}$ for all negligible functions ν and there exists a strong statistical hiding and weak computational binding commitment scheme $C = \{C_{\lambda,b}\}$ (the proof for the other flavor follows from [Proposition 8.7](#)). Let $p(\lambda)$ denote the polynomial from the weak binding property of C , and let $n(\lambda)$ denote the number of qubits of the commitment on security parameter λ . The strong statistical hiding property implies that for some negligible function $\epsilon(\lambda)$ we have

$$F(\rho_{\lambda,0}, \rho_{\lambda,1}) \geq 1 - \epsilon(\lambda),$$

where $\rho_{\lambda,b}$ is the reduced density matrix of the commitment state $|\psi_{\lambda,b}\rangle = C_{\lambda,b}|0 \cdots 0\rangle$ on register C (the register sent by the sender in the commitment phase). Since $C_{\lambda,b}$ are quantum polynomial size circuits, it follows that $\left((1^{n(\lambda)}, C_{\lambda,0}, C_{\lambda,1}), |\psi_{\lambda,0}\rangle\right)$ is a valid instance of $\text{DISTUHLMANN}_{1-\epsilon}$ (by padding with zeroes we can assume that $\{C_{\lambda,b}\}_{b \in \{0,1\}}$ output $2n(\lambda)$ qubits).

Let $\delta(\lambda) = \frac{1}{3p(\lambda)}$. By the assumption that $\text{DISTUHLMANN}_{1-\epsilon} \in \text{avgUnitaryBQP/poly}$ we get that there is a (non-uniform) family of poly(λ)-size circuits A_λ only acting on register R for which

$$\text{td} \left(\left(A_\lambda \otimes \text{id}_C \right) (\psi_{\lambda,0}), \psi_{\lambda,0} \right) \leq \delta(\lambda).$$

By Fuchs-van de Graaf we get

$$F \left(\left(A_\lambda \otimes \text{id}_C \right) (\psi_{\lambda,0}), \psi_{\lambda,0} \right) \geq 1 - 2\delta(\lambda) > 1 - \frac{1}{p(\lambda)},$$

which breaks the $(1 - 1/p)$ -computational binding property of the commitment scheme, a contradiction.

We now prove the second part of the theorem. Let $X = \{x_\lambda\}_{\lambda \in \mathbb{N}}$ be a family of $\text{UHLMANN}_{1-\mu}$ instances satisfying the premise of the second part of the theorem. For each λ , we have $x_\lambda = (1^{n(\lambda)}, D_\lambda, E_\lambda)$ for some polynomial $n(\lambda)$ (since X is uniform polynomial-time computable). Consider the commitment scheme defined by X , i.e. $C := \{C_{\lambda,b}\}_{\lambda,b}$ where for each λ , $C_{\lambda,0} := D_\lambda, C_{\lambda,1} := E_\lambda$. By assumption, we have that $\{C_{\lambda,b}\}_{\lambda,b}$ is a uniform polynomial-size family of circuits each acting on $2n(\lambda)$ qubits. Since x_λ is a valid $\text{UHLMANN}_{1-\mu}$ instance for all λ , the reduced density

matrices $\rho_{\lambda,0}$ and $\rho_{\lambda,1}$ have fidelity at least $1 - \mu(\lambda)$ for some negligible function μ ; applying Fuchs-van de Graaf their trace distance is at most $O(\sqrt{\mu(\lambda)})$, which is still a negligible function. Thus $\{C_{\lambda,b}\}_{\lambda,b}$ satisfies strong statistical hiding.

To show the weak computational binding property, by assumption there exists a polynomial $p(\lambda)$ such that for all non-uniform polynomial time algorithms $A = (A_\lambda)_\lambda$ and for all sufficiently large λ we have

$$\text{td} \left((A_\lambda \otimes \text{id}_{\mathbb{C}})(\psi_{\lambda,0}), \psi_{\lambda,1} \right) \geq \frac{1}{q(\lambda)} .$$

Applying Fuchs-van de Graaf implies that for all λ ,

$$F \left((A_\lambda \otimes \text{id}_{\mathbb{C}})(\psi_{\lambda,0}), \psi_{\lambda,1} \right) \leq 1 - \frac{1}{q(\lambda)^2} .$$

Thus the commitment scheme $\{C_{\lambda,b}\}_{\lambda,b}$ satisfies $(1 - \frac{1}{q(\lambda)^2})$ -computational binding, and thus weak binding, as required.

As mentioned before, the proof for the other flavor follows from [Proposition 8.7](#). This concludes the proof of the theorem. \square

8.2 Unclonable state generators

We introduce the notion of *unclonable state generators*, which abstractly captures the security of unclonable cryptographic primitives such as quantum money [[Wie83](#), [AC12](#)], and quantum copy-protection [[ALL+21](#), [CLLZ21](#)]. Intuitively, an unclonable state generator is an efficient algorithm mapping a classical key k to a quantum state $|\phi_k\rangle$ that cannot be efficiently cloned without the key k . More formally:

Definition 8.11 (State generator). *A (pure-state) state generator $G = (G_\lambda)_\lambda$ is a quantum polynomial-time algorithm that for all $\lambda \in \mathbb{N}$ takes as input a computational basis state $|k\rangle$ with $k \in \{0,1\}^\lambda$ and outputs a pure state $|\phi_k\rangle$.*

Definition 8.12 (Unclonable state generator). *Let $G = (G_\lambda)_\lambda$ be a state generator. Let $t(\lambda)$ be a function. We say that G is a statistical (resp. computational) t -copy unclonable state generator if for all computationally unbounded (resp. polynomial-time) non-uniform algorithms $A = (A_\lambda)_\lambda$,*

$$\Pr \left(\text{measuring } \rho \text{ with } |\phi_k\rangle\langle\phi_k|^{\otimes t(\lambda)+1} \text{ accepts : } \begin{array}{l} k \leftarrow \{0,1\}^\lambda \\ \rho \leftarrow A_\lambda(G_\lambda(k)^{\otimes t(\lambda)}) \end{array} \right) \leq \text{negl}(\lambda) .$$

Equivalently, this can also be written as

$$\mathbb{E}_{\substack{k \leftarrow \{0,1\}^\lambda \\ \rho \leftarrow A_\lambda(G_\lambda(k)^{\otimes t(\lambda)})}} \text{Tr}(|\phi_k\rangle\langle\phi_k|^{\otimes t(\lambda)+1} \rho) \leq \text{negl}(\lambda) .$$

In this section, we give a complexity upper bound on breaking a natural class of unclonable state generators: either an unclonable state generator from this class is information-theoretically secure, or it can be efficiently broken with an oracle to UHLMANN_κ for small $\kappa \ll 1$.

Before we prove this result we first discuss the relationship between unclonable state generators and another primitive known as *one-way state generators*.

8.2.1 Relation with one-way state generators

Morimae and Yamakawa [MY22b] introduced one-way state generators (OWSGs) as a quantum analogue of one-way functions (OWFs). Intuitively speaking, an OWSG is an efficient algorithm that maps a classical key k to a quantum state $|\phi_k\rangle$ that is, in a sense, hard to invert. OWSGs provide another natural way to abstractly capture the security of quantum cryptographic primitives such as pseudorandom states [JLS18] and quantum money schemes [Wie83, Aar09].

We present the original definition of a OWSG, given by [MY22b]. There are more general definitions given by [MY22a], but we stick with the simpler one for now.

Definition 8.13 (One-way state generator). *Let $G = (G_\lambda)_\lambda$ be a state generator. Let $t(\lambda)$ be a function. We say that G is a statistical (resp. computational) t -copy secure OWSG if for all computationally unbounded (resp. polynomial-time) non-uniform algorithms $A = (A_\lambda)_\lambda$,*

$$\Pr \left(\text{measuring } |\phi_k\rangle \text{ with } |\phi_{k'}\rangle\langle\phi_{k'}| \text{ accepts : } \begin{array}{l} k \leftarrow \{0,1\}^\lambda \\ k' \leftarrow A_\lambda(G_\lambda(k)^{\otimes t(\lambda)}) \end{array} \right) \leq \text{negl}(\lambda) .$$

Equivalently, this can also be written as

$$\mathbb{E}_{\substack{k \leftarrow \{0,1\}^\lambda \\ k' \leftarrow A_\lambda(G_\lambda(k)^{\otimes t(\lambda)})}} |\langle\phi_{k'}|\phi_k\rangle|^2 \leq \text{negl}(\lambda) . \quad (8.3)$$

Recent work by Khurana and Tomer [KT23] shows that if there exists a t -copy secure OWSG G for a sufficiently large polynomial $t(\lambda)$, then there exist quantum bit commitment schemes. Put another way, the complexity of breaking t -copy secure OWSGs for sufficiently large $t(\lambda)$ can be efficiently reduced to the complexity of UHLMANN_{1-negl}.

We now compare unclonable state generators with OWSGs.

Proposition 8.14. *Let $t = O(1)$ be a constant independent of the security parameter λ . Let $G(k)$ be a quantum polynomial-time algorithm that outputs a pure state $|\phi_k\rangle$. If G is a t -copy unclonable state generator, then it is a t -copy secure OWSG.*

Proof. Suppose that there was an OWSG inverter A that given t -copies of $|\phi_k\rangle$, outputs a key k' such that $|\langle\phi_{k'}|\phi_k\rangle|^2$ is nonnegligible with nonnegligible probability. Using this inverter A , an adversary can efficiently generate the state $|\phi_{k'}\rangle^{\otimes t+1}$ with nonnegligible probability, and $|\langle\phi_{k'}|\phi_k\rangle|^{2(t+1)}$ is still non-negligible (because t is constant). This violates the unclonability security condition. \square

When t can grow with $t(\lambda)$, the connection between OWSG security and unclonability is less clear: it is not clear whether t -copy secure OWSGs imply t -copy secure unclonable state generators or vice versa.

Thus it is not clear that the results of Khurana and Tomer [KT23] can be extended to show that breaking unclonable state generators efficiently reduces to UHLMANN.

8.2.2 Breaking a class of unclonable state generators

We identify a natural class of state generators, called *real-valued, clean-output* state generators. Intuitively, clean-output means that the state $|\phi_k\rangle$ can be computed from k by a unitary that returns all its ancilla qubits to the zero-state.

Definition 8.15 (Real-valued, clean-output state generator). *A state generator G is clean-output if for all λ the generator G_λ is a unitary such that*

$$|k\rangle \otimes |0 \cdots 0\rangle \mapsto |k\rangle \otimes |\phi_k\rangle \otimes |0 \cdots 0\rangle$$

where $|0 \cdots 0\rangle$ denotes some number of ancilla zeroes. Furthermore, we say that G is real-valued if for all λ and for all $k \in \{0, 1\}^\lambda$, the output state $|\phi_k\rangle$ is a real-valued vector when expanded in the computational basis.

We claim that real-valued, clean-output state generators capture a natural class of unclonable and one-way state generators; here are two well-known examples.

1. *Pseudorandom states*: The canonical constructions of pseudorandom state generators [JLS18, BS19] map keys k to states of the form

$$|\phi_k\rangle = 2^{-n/2} \sum_{x \in \{0,1\}^n} (-1)^{f_k(x)} |x\rangle,$$

where $\{f_k : \{0, 1\}^n \rightarrow \{0, 1\}\}_k$ is a post-quantum pseudorandom function family. Since the f_k are computable by deterministic classical circuits, the states $|\phi_k\rangle$ are cleanly computable. Furthermore they are clearly real-valued as the amplitudes are all $\pm 2^{-n/2}$.

2. *Quantum subspace states*: The constructions of quantum money from [AC12, Zha21] and other unclonable primitives [CLLZ21] make use of generators that produce *subspace states* (and their generalizations called *coset states*). A subspace state generator maps a key k , which is interpreted as a description of linearly independent generators of a random subspace $A \subset \mathbb{F}_2^n$ of dimension $n/2$, to the following state:

$$|\phi_k\rangle = 2^{-n/4} \sum_{x \in A} |x\rangle.$$

It is easy to see that this state can be cleanly computed in polynomial time given the key k , and is clearly real-valued.

Remark 8.16. We note that our proofs will only require a weaker condition than “real-valued”: we will only need that the inner product $\langle \phi_k | \phi_{k'} \rangle$ is real for all choices of k and k' . However, as we have seen above, real-valued state generators are a natural class, so we stick to this stronger requirement for simplicity.

We show that for real-valued, clean-output state generators, t -copy unclonability implies OWSG security for any number of copies t .

Proposition 8.17. *Let $t(\lambda)$ be a polynomial. If G is a real-valued, clean-output statistical (resp. computational) t -copy unclonable state generator then it is a statistical (resp. computational) t -copy OWSG.*

Proof. Suppose for contradiction that a t -copy unclonable state generator G did not have t -copy OWSG security. Let $A = (A_\lambda)_\lambda$ denote an adversary that breaks OWSG security of G . Let \tilde{A}_λ denote a unitary dilation of A_λ . We can write its behavior as

$$\tilde{A}_\lambda |\phi_k\rangle^{\otimes t(\lambda)} \otimes |0\rangle = \sum_{k'} \sqrt{\epsilon_{k,k'}} |\text{aux}_{k,k'}\rangle \otimes |k'\rangle$$

for some auxiliary states $\{|\text{aux}_{k,k'}\rangle\}_{k,k'\in\{0,1\}^\lambda}$ and for every $k \in \{0,1\}^\lambda$ some probabilities $\{\epsilon_{k,k'}\}_{k'\in\{0,1\}^\lambda}$. The condition that A breaks OWSG security means that there exists a polynomial $p(\lambda)$ such that

$$2^{-\lambda} \sum_{k,k'} \epsilon_{k,k'} |\langle \phi_k | \phi_{k'} \rangle|^2 \geq 1/p(\lambda)$$

for infinitely many λ . In words, the left-hand side computes the expected overlap $|\langle \phi_k | \phi_{k'} \rangle|^2$ when k is sampled uniformly at random (which is why there is a normalisation $2^{-\lambda}$) and then k' is sampled according to the distribution $\{\epsilon_{k,k'}\}_{k'}$, which is exactly the quantity on the l.h.s. of Equation (8.3). Then consider the unitary V that first applies \tilde{A} ; then controlled on the state $|k'\rangle$, using the generator G twice, prepares $|\phi_{k'}\rangle^{\otimes 2}$ in an ancilla register; and finally applies the inverse unitary \tilde{A}^\dagger . Note that the unitary V is efficient if \tilde{A} is efficient. Then consider applying V to $t(\lambda)$ copies of $|\phi_k\rangle$ and some ancillas:

$$V |\phi_k\rangle^{\otimes t(\lambda)} \otimes |0\rangle = \sum_{k'} \sqrt{\epsilon_{k,k'}} \tilde{A}_\lambda^\dagger \left(|\text{aux}_{k,k'}\rangle \otimes |k'\rangle \right) \otimes |\phi_{k'}\rangle^{\otimes 2} .$$

We now calculate the average overlap between this state and $|\phi_k\rangle^{\otimes t(\lambda)} \otimes |0\rangle \otimes |\phi_k\rangle^{\otimes 2}$:

$$\begin{aligned} & 2^{-\lambda} \sum_k \left| \langle \phi_k |^{\otimes t(\lambda)} \otimes \langle 0 | \otimes \langle \phi_k |^{\otimes 2} V |\phi_k\rangle^{\otimes t(\lambda)} \otimes |0\rangle \right|^2 \\ &= 2^{-\lambda} \sum_k \left| \left(\sum_{k'} \sqrt{\epsilon_{k,k'}} \langle \text{aux}_{k,k'} | \otimes \langle k' | \otimes \langle \phi_k |^{\otimes 2} \right) \left(\sum_{k''} \sqrt{\epsilon_{k,k''}} |\text{aux}_{k,k''}\rangle \otimes |k''\rangle \otimes |\phi_{k''}\rangle^{\otimes 2} \right) \right|^2 \\ &= 2^{-\lambda} \sum_k \left| \sum_{k'} \epsilon_{k,k'} \langle \phi_k | \phi_{k'} \rangle^2 \right|^2 \\ &\geq \left| 2^{-\lambda} \sum_{k,k'} \epsilon_{k,k'} |\langle \phi_k | \phi_{k'} \rangle|^2 \right|^2 \geq 1/p(\lambda)^2, \end{aligned}$$

where in the last line we used Cauchy-Schwarz and the premise that G is real-valued so that $\langle \phi_k | \phi_{k'} \rangle^2 = |\langle \phi_k | \phi_{k'} \rangle|^2$.

In other words, the unitary V maps $t(\lambda)$ copies of $|\phi_k\rangle$ to have inverse polynomial overlap with $t(\lambda) + 2$ copies of $|\phi_k\rangle$, on average over the key k . Since V is efficient if A is efficient, this breaks the t -copy unclonability security of G . \square

We now give an upper bound on the complexity of breaking real-valued, clean-output state generators; we essentially show that either they have information-theoretic OWSG security, or can be efficiently cloned if $\text{DISTUHLMANN}_\kappa$ is efficiently solvable for inverse polynomial κ .

Theorem 8.18. *Suppose for all polynomials $q(n)$ there exists a non-uniform polynomial-time algorithm $M = (M_x)_x$ and a polynomial $r(n)$ such that for all valid $\text{UHLMANN}_{1/q(n)}$ instances $x = (1^n, C, D)$ we have*

$$\mathbb{F}\left(\text{id} \otimes M_x(|C\rangle\langle C|), |D\rangle\langle D|\right) \geq 1/r(n) .$$

Then for all real-valued, clean-output state generators G and for all polynomials $t(\lambda)$ either:

- G is a t -copy statistical OWSG, or
- the t -copy unclonability security of G can be broken in polynomial time.

The reader may wonder why the assumption of the theorem is not written as $\text{DISTUHLMANN}_{1/p(n)} \in \text{avgUnitaryBQP/poly}$. This is an illustration of how the (distributional) UHLMANN_κ problem differs depending on κ . When κ is very close to 1, then [Proposition 5.8](#) shows that being able to locally map $|C\rangle$ to have fidelity approximately κ with $|D\rangle$ implies that one can solve $\text{DISTUHLMANN}_\kappa$ with small error – and vice versa. However, when κ is small [Proposition 5.8](#) no longer gives meaningful bounds.

Proof. For simplicity we present the proof for $t(\lambda) = 1$; adapting the proof to general polynomials $t(\lambda)$ is straightforward. Suppose the state generator G does not satisfy 1-copy statistical security. Then there exists a (possibly computationally unbounded) algorithm $A = (A_\lambda)_\lambda$ and a polynomial $p(\lambda)$ such that for infinitely many λ :

$$\Pr \left(\text{measuring } |\phi_k\rangle \text{ with } |\phi_{k'}\rangle\langle\phi_{k'}| \text{ accepts : } \begin{array}{l} k \leftarrow \{0,1\}^\lambda \\ k' \leftarrow A_\lambda(G_\lambda(k)) \end{array} \right) \geq 1/p(\lambda) .$$

By the assumption that G computes its outputs cleanly, there exist polynomial-sized quantum circuits C, D that prepare the following states:

$$\begin{aligned} |C\rangle_{\text{KSK}'\text{T}} &:= 2^{-\lambda/2} \sum_{k \in \{0,1\}^\lambda} |k\rangle_{\text{K}} \otimes |\phi_k\rangle_{\text{S}} \otimes |0\rangle_{\text{K}'} \otimes |0\rangle_{\text{T}} \\ |D\rangle_{\text{KSK}'\text{T}} &:= 2^{-\lambda/2} \sum_{k \in \{0,1\}^\lambda} |k\rangle_{\text{K}} \otimes |\phi_k\rangle_{\text{S}} \otimes |0\rangle_{\text{K}'} \otimes |\phi_k\rangle_{\text{T}}^{\otimes 2} . \end{aligned}$$

Let ρ, σ denote the reduced density matrices of $|C\rangle, |D\rangle$ respectively on register K . We now show that $F(\rho, \sigma) \geq 1/p(\lambda)$ by exhibiting a unitary V acting on register $\text{SK}'\text{T}$ such that

$$F(\rho, \sigma) \geq |\langle D | (\text{id}_{\text{K}} \otimes V_{\text{SK}'\text{T}}) |C\rangle|^2 \geq 1/p(\lambda)^2 . \quad (8.4)$$

Consider the unitary purification \tilde{A} of the adversary A ; without loss of generality it can be expressed as follows. For all $k \in \{0,1\}^\lambda$,

$$\tilde{A}_{\text{SK}'} |\phi_k\rangle_{\text{S}} \otimes |0\rangle_{\text{K}'} = \sum_{k'} \sqrt{\epsilon_{k,k'}} |\text{aux}_{k,k'}\rangle_{\text{S}} \otimes |k'\rangle_{\text{K}'}$$

for some auxiliary states $\{|\text{aux}_{k,k'}\rangle\}_{k,k' \in \{0,1\}^\lambda}$ and for some probabilities $\{\epsilon_{k,k'}\}_{k,k' \in \{0,1\}^\lambda}$ satisfying (by the assumption on the adversary)

$$2^{-\lambda} \sum_{k,k'} \epsilon_{k,k'} |\langle \phi_k | \phi_{k'} \rangle|^2 \geq 1/p(\lambda) .$$

Now define the unitary V acting on register $\text{SK}'\text{T}$ that first applies the unitary \tilde{A} to registers TK' ; then, controlled on the state $|k'\rangle$ in register K' , prepares the state $|\phi_{k'}\rangle^{\otimes 2}$ in register T ; and finally applies the inverse unitary \tilde{A}^\dagger . Note that this unitary V is not necessarily efficient because it runs the adversary W . We now verify [Equation \(8.4\)](#):

$$\begin{aligned} & |\langle D | (\text{id}_{\text{A}} \otimes V_{\text{B}}) |C\rangle|^2 \\ &= \left| 2^{-\lambda} \sum_k \left(\sum_{k'} \sqrt{\epsilon_{k,k'}} \langle \text{aux}_{k,k'} | \otimes \langle k' | \otimes \langle \phi_k |^{\otimes 2} \right) \left(\sum_{k''} \sqrt{\epsilon_{k,k''}} |\text{aux}_{k,k''}\rangle \otimes |k''\rangle \otimes |\phi_{k''}\rangle^{\otimes 2} \right) \right|^2 \\ &= \left| 2^{-\lambda} \sum_{k,k'} \epsilon_{k,k'} \langle \phi_k | \phi_{k'} \rangle^2 \right|^2 \geq 1/p(\lambda)^2 \end{aligned}$$

where in the last line we used the premise that G is a real-valued OWSG so that $\langle \phi_k | \phi_{k'} \rangle^2 = |\langle \phi_k | \phi_{k'} \rangle|^2$. Thus $(1^n, C, D)$ is a valid $\text{UHLMANN}_{1/p(\lambda)^2}$ instance for some $n = \text{poly}(\lambda)$.

We have shown that the existence of *some* adversary A breaking the t -copy OWSG security of G implies there is *some* Uhlmann transformation that maps $|C\rangle$ to a state with fidelity at least $1/p(\lambda)^2$ with $|D\rangle$. Now we argue that *all* algorithms $M = (M_x)_x$ that implement an Uhlmann transformation for $\text{UHLMANN}_{1/p(\lambda)^2}$ instances can be used to break the unclonability security of G . In particular, letting M_x be the Uhlmann transformation for instance $x = (1^n, C, D)$, we have

$$F\left((\text{id} \otimes M_x)(|C\rangle\langle C|), |D\rangle\langle D|\right) \geq 1/r(\lambda)$$

for some polynomial $r(\lambda)$. By measuring the K register of both arguments, and using the joint concavity of the fidelity function, we have

$$2^{-\lambda} \sum_k F\left((\text{id} \otimes M_x)(|\phi_k\rangle\langle\phi_k| \otimes |0\rangle\langle 0|), |\phi_k\rangle\langle\phi_k|^{\otimes 3} \otimes |0\rangle\langle 0|\right) \geq 1/r(\lambda),$$

where for notational convenience we have grouped the three copies of $|\phi_k\rangle$ in $|D\rangle$ together. This means that on average over the key k , the algorithm M_x maps single copy of $|\phi_k\rangle$ (plus some zeroes) to three copies of $|\phi_k\rangle$ (plus some zeroes) with fidelity at least $1/r(\lambda)$. This implies that G does not have single-copy unclonability security. \square

8.3 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 she has 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 $\text{DISTSUCCINCTUHLMANN}$, and hence it can be 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 8.19 (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 $x \in \{0, 1\}^*$,¹⁹ the challenger \mathcal{C}_x engages in an interaction with a prover \mathcal{A} (which also gets*

¹⁹Here, 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.

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

Definition 8.20 (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 $\mathcal{C}_x \leftrightarrow \mathcal{A}$. We say that a (possibly inefficient) adversary \mathcal{A} breaks instance x of the assumption (\mathcal{C}, c) with advantage δ if $\Pr(\mathcal{C}_x \leftrightarrow \mathcal{A} \text{ accepts}) \geq c + \delta$.*

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 $(\mathcal{C}^{\text{PRS}}, \frac{1}{2})$ where the instances x specify the security parameter λ as well as a positive integer t . The challenger \mathcal{C}^{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.
3. (*Quantum EFI pairs*) Consider a candidate ensemble of EFI pairs $\{(\rho_{\lambda,0}, \rho_{\lambda,1})\}_\lambda$ [BCQ23]. The assumption here is $(\mathcal{C}^{\text{EFI}}, \frac{1}{2})$. The challenge \mathcal{C}^{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 8.21. *A falsifiable quantum cryptographic assumption (\mathcal{C}, c) is either information-theoretically secure, or breaking the assumption (\mathcal{C}, c) can be reduced to $\text{DISTSUCCINCTUHLMANN}_1$.*

Formally what we mean by “breaking the assumption can be reduced to $\text{DISTSUCCINCTUHLMANN}_1$ ” is the following: there exists an adversary A that is a polynomial time quantum query algorithm with access to a $\text{DISTSUCCINCTUHLMANN}_1$ 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 8.21 is very similar to that of Lemma 7.5: 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 $\text{DISTSUCCINCTUHLMANN}_1$ oracle, so breaking the assumption reduces to $\text{DISTSUCCINCTUHLMANN}_1$. To make the paper more modular, we nonetheless spell out the details.

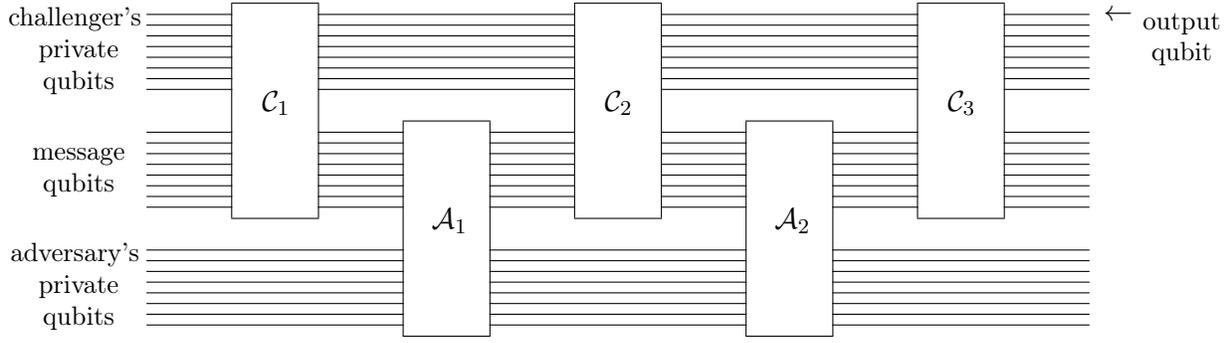


Figure 3: Quantum circuit representation of a 4-message interaction between an efficient challenger and an adversary who seeks to falsify a cryptographic assumption (\mathcal{C}, c) .

Proof of Theorem 8.21. Suppose that (\mathcal{C}, c) is not in fact information-theoretically secure and there exists a possibly inefficient adversary \mathcal{A} with at most $r = \text{poly}(n)$ many rounds of interaction and a polynomial $p(n)$ such that

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

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

- $\rho_{\mathcal{M}_x^j \mathcal{W}_x^j}^{(j)}$ denote the state of the message register \mathcal{M}_x^j and the private workspace \mathcal{W}_x^j of the challenger \mathcal{C}_x at the beginning of the challenger's j 'th turn
- $\sigma_{\mathcal{M}_x^j \mathcal{W}_x^j}^{(j)}$ 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 statePSPACE . Let $q(n) = p(n)/2$ be a polynomial. 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

$$(|\psi_{x,j}\rangle_{\mathcal{M}_x^j \mathcal{W}_x^j \mathcal{P}_x^j})_{x,j}, |\varphi_{x,j}\rangle_{\mathcal{M}_x^j \mathcal{W}_x^j \mathcal{P}_x^j})_{x,j} \in \text{statePSPACE}_{1/q(n)}$$

for some purifying registers \mathcal{P}_x^j that are purifications of intermediate states $\rho_{\mathcal{M}_x^j \mathcal{W}_x^j}^{(j)}$ and $\sigma_{\mathcal{M}_x^j \mathcal{W}_x^j}^{(j)}$ 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 $|\psi_{x,j}\rangle_{\mathcal{M}_x^j \mathcal{W}_x^j \mathcal{P}_x^j} = C^j |0 \dots 0\rangle$ and $|\varphi_{x,j}\rangle_{\mathcal{M}_x^j \mathcal{W}_x^j \mathcal{P}_x^j} = D^j |0 \dots 0\rangle$ are purifications of the reduced state on

the message register M_x^j and challenger register 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.

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

We can therefore interpret the circuit pair (C^j, D^j) as an instance of the SUCCINCTUHLMANN_1 problem, with W^j taking the role of the register that cannot be acted upon by the Uhlmann unitary. Hence, with access to a $\text{DISTSUCCINCTUHLMANN}_1$ -oracle, we can apply an Uhlmann transformation mapping $|\psi_{x,j}\rangle_{M_x^j W_x^j P_x^j}$ to $|\varphi_{x,j}\rangle_{M_x^j W_x^j P_x^j}$ by acting only on registers $M_x^j P_x^j$. This means that with the $\text{DISTSUCCINCTUHLMANN}_1$ -oracle, we can efficiently implement the actions of a successful prover in the interactive protocol. \square

8.4 Open problems

In [Section 8.2](#) we studied the complexity of breaking a special class of *real-valued* state generators. A natural question is whether the real-valued property is without loss of generality. For solving decision problems, it is without loss of generality to use quantum circuits with only real-valued gates [[Shi03](#), [Aha03](#)]; however it is *a priori* possible that protocols where the parties compute with complex-valued gates may allow for stronger security guarantees than if they were restricted to only real-valued gates.

Open Problem 17. Can all unclonable or one-way state generators be made real-valued without loss of generality? Are there quantum cryptographic primitives where the security depends on quantum computing with complex-valued gates?

Open Problem 18. Can [Theorem 8.18](#) be strengthened so that an unclonable/one-way state generator is either statistically secure or is efficiently broken using an oracle for $\text{DISTUHLMANN}_\kappa$ for some range of κ ?

Solving this requires strengthening [Theorem 8.18](#) in two ways: first, getting rid of the real-valued, clean-output conditions, and second, make the two bullets of the “either-or” statement talk about the same type of security (OWSG or unclonability), whereas currently they are different in the statement of [Theorem 8.18](#). We note that Khurana and Tomer [[KT23](#)] show that pure-state OWSGs with $t(\lambda)$ -copy security for sufficiently-large polynomial t implies the existence of quantum commitments (which in turn implies the hardness of DISTUHLMANN).

Morimae and Yamakawa [[MY22a](#), [MY22b](#)] asked whether OWSGs constitute a *minimal assumption* in quantum cryptography. A natural question, in particular, is whether OWSGs are implied by so-called *unclonable cryptographic primitives*, such as quantum money [[Aar09](#), [AC12](#)], quantum copy-protection [[Aar09](#), [CMP20](#), [CLLZ21](#)], or unclonable encryption [[BL20](#), [AKL⁺22](#)], which leverage the quantum no-cloning principle to achieve unforgeable banknotes, programs, and ciphertexts.

Open Problem 19. Do unclonable cryptographic primitives, such as quantum money, copy-protection, or unclonable encryption imply the hardness of the Uhlmann Transformation Problem?

Open Problem 20. Can computationally secure OWSGs be constructed assuming the hardness of $\text{DISTUHLMANN}_{1/p(n)}$ for some polynomial p ?

9 Applications to 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 for a range of parameters.

9.1 Decoding 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 \mathbf{A} to \mathbf{B} is ϵ -decodable if there exists a (not necessarily efficient) quantum algorithm D that takes as input register \mathbf{B} and outputs register \mathbf{A}' isomorphic to \mathbf{A} such that*

$$F\left((D_{\mathbf{B} \rightarrow \mathbf{A}'} \circ \mathcal{N}_{\mathbf{A} \rightarrow \mathbf{B}})(|\Phi\rangle\langle\Phi|_{\mathbf{AR}}), |\Phi\rangle\langle\Phi|_{\mathbf{A}'\mathbf{R}}\right) \geq 1 - \epsilon,$$

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

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. Furthermore, decodable channels most naturally arise in the context of error corrected communication: there, given any noisy channel, the goal is to find an encoding channel such that the concatenation of encoder and noisy channel is decodable. 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 $\mathcal{N} : \mathbf{A} \rightarrow \mathbf{B}$ to be decodable. Recall the definition of a Stinespring dilation of a channel: this is an isometry $V : \mathbf{A} \rightarrow \mathbf{BC}$ such that $\mathcal{N}(X) = \text{Tr}_{\mathbf{C}}(VXV^*)$. We introduce a condition about the *complementary channel* $\mathcal{N}^c(X) := \text{Tr}_{\mathbf{B}}(VXV^*)$ defined relative to a Stinespring dilation V :

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

$$F\left(\mathcal{N}_{\mathbf{A} \rightarrow \mathbf{C}}^c(|\Phi\rangle\langle\Phi|_{\mathbf{AR}}), \mathcal{N}_{\mathbf{A} \rightarrow \mathbf{C}}^c\left(\frac{\text{id}_{\mathbf{A}}}{\dim \mathbf{A}}\right) \otimes \frac{\text{id}_{\mathbf{R}}}{\dim \mathbf{R}}\right) \geq 1 - \epsilon,$$

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 \mathbf{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:

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

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

$$F\left((\text{id} \otimes U) |E\rangle\langle E| (\text{id} \otimes U^\dagger), |F\rangle\langle F|\right) \geq 1 - \epsilon . \quad (9.1)$$

Define the decoding procedure D that maps register B to register A' and behaves as follows: it appends registers $A'R'$ in the $|0\rangle$ state, applies the isometry U to registers $BA'R'$, and then traces out registers BR' to obtain register A' . Since $|E\rangle$ is the result of applying the Stinespring dilation of \mathcal{N} to $|\Phi\rangle$ and appending $|0\rangle_{A'R'}$, and using the fact that tracing out registers BR' does not reduce the fidelity, Equation (9.1) implies that

$$F\left((D_{B \rightarrow A'} \circ \mathcal{N}_{A \rightarrow B})(|\Phi\rangle\langle\Phi|_{AR}), |\Phi\rangle\langle\Phi|_{A'R}\right) \geq 1 - \epsilon ,$$

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

$$\text{Tr}\left(|\Phi\rangle\langle\Phi| (D_{B \rightarrow A'} \circ \mathcal{N}_{A \rightarrow B})(|\Phi\rangle\langle\Phi|_{AR})\right) \geq 1 - \epsilon .$$

Considering the Stinespring dilation $V : A \rightarrow BC$ of \mathcal{N} this is equivalent to

$$\text{Tr}\left((|\Phi\rangle\langle\Phi|_{A'R} \otimes \text{id}_C) D_{B \rightarrow A'}(V |\Phi\rangle\langle\Phi|_{AR} V^\dagger)\right) \geq 1 - \epsilon . \quad (9.2)$$

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

$$F\left(D_{B \rightarrow A'}(V |\Phi\rangle\langle\Phi|_{AR} V^\dagger), |\Phi\rangle\langle\Phi|_{A'R} \otimes \rho_C\right) \geq 1 - \epsilon . \quad (9.3)$$

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

$$F\left(\mathcal{N}_{A \rightarrow C}^c(|\Phi\rangle\langle\Phi|_{AR}), \rho_C \otimes \frac{\text{id}_R}{\dim R}\right) \geq 1 - \epsilon . \quad (9.4)$$

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

$$F\left(\mathcal{N}_{A \rightarrow C}^c\left(\frac{\text{id}_A}{\dim A}\right), \rho_C\right) \geq 1 - \epsilon . \quad (9.5)$$

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

$$F\left(\mathcal{N}_{A \rightarrow C}^c(|\Phi\rangle\langle\Phi|_{AR}), \mathcal{N}_{A \rightarrow C}^c\left(\frac{\text{id}_A}{\dim A}\right) \otimes \frac{\text{id}_R}{\dim R}\right) \geq 1 - 2\sqrt{\epsilon} ,$$

which is the desired decoupling condition. \square

9.1.1 Complexity of the Decodable Channel Problem

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

$$F\left((D_x \circ C)(|\Phi\rangle\langle\Phi|), |\Phi\rangle\langle\Phi|\right) \geq 1 - \delta(|x|),$$

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

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. *$\text{DISTUHLMANN}_{1-\epsilon} \in \text{avgUnitaryBQP}$ for all negligible functions $\epsilon(n)$ if and only if for every negligible function $\epsilon(n)$ and for every polynomial $q(n)$, the ϵ -Decodable Channel Problem is solvable in uniform polynomial time with error $O(1/q(n))$.*

Proof. Upper bound. We start by proving the “only if” direction (if $\text{DISTUHLMANN}_{1-\epsilon}$ is easy, then the Decodable Channel Problem is easy). Let $\epsilon(n)$ be a negligible function and let $q(n)$ be a polynomial. We present an algorithm D that solves the ϵ -Decodable Channel Problem with error $O(1/q(n))$, and is efficient under the assumption about DISTUHLMANN .

Let $x = (1^m, 1^r, C)$ be an instance of the ϵ -Decodable Channel Problem be such that C is a quantum circuit computing an ϵ -decodable channel mapping n qubits (which we label as register A) to r qubits (which we label as register B). Let V denote the unitary purification of C (see Definition 2.7) 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 $|E\rangle_{\text{BCA}'R'}$ and $|F\rangle_{\text{RA}'\text{BC}R'}$ 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 $\text{poly}(|C|)$. 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 $\text{UHLMANN}_{1-2\sqrt{\epsilon}}$ instance (where the registers are divided into two groups CR and BA'R'). Since ϵ is negligible, so is $2\sqrt{\epsilon}$. Therefore $\text{DISTUHLMANN}_{1-2\sqrt{\epsilon}} \in \text{avgUnitaryBQP}$ by assumption, and thus there exists a polynomial-time algorithm $M = (M_y)_y$ that implements $\text{DISTUHLMANN}_{1-2\sqrt{\epsilon}}$ with average-case error $1/q$. By Proposition 5.8, it follows that for $y = (1^k, E, F)$ with $k = \text{poly}(|x|)$, the algorithm M_y satisfies, for sufficiently large k ,

$$F\left((\text{id} \otimes M_y)(|E\rangle\langle E|), |F\rangle\langle F|\right) \geq \left(1 - \frac{1}{q(k)} - O(\epsilon(k)^{1/4})\right)^2 \geq 1 - O(1/q(k)). \quad (9.6)$$

In the second inequality we used the fact that ϵ is a negligible function.

The algorithm $D = (D_x)_x$ behaves as follows on instance $x = (1^m, 1^r, C)$ of the ϵ -Decodable Channel Problem. It receives as input a register B. It first computes the description of the

UHLMANN $_{1-2\sqrt{\epsilon}}$ instance $y = (1^k, E, F)$ described above. It initializes ancilla registers $A'R'$ in the zero state, and then applies the algorithm M_y to registers $BA'R'$. Finally, the algorithm D_x then traces out registers BR' and outputs the remaining register A' .

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

$$\begin{aligned} \left((D_x)_{B \rightarrow A'} \circ C_{A \rightarrow B} \right) (|\Phi\rangle\langle\Phi|_{RA}) &= \text{Tr}_{CBR'} \left((\text{id} \otimes M_y)(|E\rangle\langle E|) \right) \\ |\Phi\rangle\langle\Phi|_{RA'} &= \text{Tr}_{ABCR'} \left(|F\rangle\langle F| \right). \end{aligned}$$

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

$$F \left(\left((D_x)_{B \rightarrow A'} \circ C_{A \rightarrow B} \right) (|\Phi\rangle\langle\Phi|_{RA}), |\Phi\rangle\langle\Phi|_{RA'} \right) \geq F \left((\text{id} \otimes M_y)(|E\rangle\langle E|), |F\rangle\langle F| \right) \geq 1 - O(1/q(k)).$$

Thus we have shown that $D = (D_x)_x$ solves the ϵ -Decodable Channel Problem with error $O(1/q(k))$, and since $k \geq |x|$, this is at most $O(1/q(|x|))$ for sufficiently large $|x|$, 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: we prove the contrapositive and argue that if DISTUHLMANN is 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.

To construct such an encryption channel, we leverage quantum commitments, which we have already discussed in Section 8.1. Theorem 8.10 and Proposition 8.7 almost show that $\text{DISTUHLMANN}_{1-\epsilon} \notin \text{avgUnitaryBQP}$ for some negligible function ϵ implies the existence of strong statistical binding, weak computational hiding commitments. By “almost”, we mean that Theorem 8.10 assumes something stronger, which is that $\text{DISTUHLMANN}_{1-\epsilon}$ is not in $\text{avgUnitaryBQP}/\text{poly}$, and furthermore hard instances of DISTUHLMANN can be efficiently generated. This is needed in order to obtain a bonafide quantum commitment with the requisite properties. However for this lower bound we use a slightly weaker primitive, where we do not need the hard instances to be uniformly generated and for the security to only hold against uniform adversaries. We describe the primitive formally below, and the proof of this implication follows along the same lines as the proof of Theorem 8.10.

Let $\epsilon(n)$ be a negligible function and let $\delta(n) = 1/p(n)$ be an inverse polynomial for which $\text{DISTUHLMANN}_{1-\epsilon} \notin \text{avgUnitaryBQP}_\delta$, and assume towards a contradiction that for every negligible function $\nu(n)$ and every polynomial $q(n)$, the ν -Decodable Channel Problem is solvable in polynomial time by an algorithm $D = (D_x)_x$ with error at most $1/q(n)$.

The following lemma shows that the hardness of DISTUHLMANN implies the existence of families of circuits that can be interpreted as strong statistical binding, *infinitely often* weak computational hiding commitments.

Lemma 9.7. *Let $\epsilon(n)$ be a negligible function. If $\text{DISTUHLMANN}_{1-\epsilon} \notin \text{avgUnitaryBQP}$, then there exists an inverse polynomial $\delta(n) = 1/p(n)$ and a family of circuits $\{C_{x,b}\}_{x \in \{0,1\}^*, b \in \{0,1\}}$ on registers*

BE where $C_{x,b}$ acts on $\text{poly}(|x|)$ qubits satisfying the following properties: for all $x \in \{0,1\}^*$, letting $\rho_{x,b}$ denote the reduced density matrix of $|C_{x,b}\rangle$ on register E,

1. (Always strong statistical binding) $F(\rho_{x,0}, \rho_{x,1}) \leq \epsilon(|x|)$.
2. (Infinitely often weak computational hiding) For all uniform polynomial-time algorithms $A = \{A_x\}_x$, there exist infinitely many x such that

$$|\Pr(A_x(\rho_{x,0}) = 1) - \Pr(A_x(\rho_{x,1}) = 1)| \leq \delta(|x|).$$

We first show how this lemma implies the lower bound for [Theorem 9.6](#). For all $x \in \{0,1\}^*$, $b \in \{0,1\}$ let $|\psi_{x,b}\rangle := C_{x,b}|0 \cdots 0\rangle$. For every $x \in \{0,1\}^*$ define the channel \mathcal{N}_x that does the following: given a qubit register A in the state $|b\rangle$ it prepares the state

$$|\theta_b\rangle_{\text{AXB E}} := \frac{1}{2} \sum_a X^a |b\rangle_{\text{A}} \otimes |a\rangle_{\text{X}} \otimes |\psi_{x,a}\rangle_{\text{BE}}$$

and then traces out registers XB, and outputs registers AE. Note that this channel can be computed by a unitary circuit V_n of size $\text{poly}(|C_{x,0}|, |C_{x,1}|)$.

Claim 9.8. For all $x \in \{0,1\}^*$ the channel \mathcal{N}_x is $8\sqrt{\epsilon(|x|)}$ -decodable.

Proof. Let \mathcal{N}_x^c denote the complementary channel that does the same thing as \mathcal{N}_x except it outputs registers XB and traces out registers AE. Consider applying \mathcal{N}_x^c to qubit A of the maximally entangled state $|\Phi\rangle_{\text{RA}}$. Then the state of registers RXB is as follows:

$$\frac{1}{4} \sum_{b,c,a,a'} |b\rangle\langle c|_{\text{R}} \otimes |a\rangle\langle a'|_{\text{X}} \otimes \text{Tr}_{\text{E}}(|\psi_{x,a}\rangle\langle\psi_{x,a'}|) \otimes \langle c| X^{a'} X^a |b\rangle. \quad (9.7)$$

Fix $a \neq a'$. Then we claim that

$$\|\text{Tr}_{\text{E}}(|\psi_{x,a}\rangle\langle\psi_{x,a'}|)\|_1 = \sqrt{F(\rho_{x,a}, \rho_{x,a'})}$$

where $\rho_{x,b}$ is the reduced density matrix of $|\psi_{x,b}\rangle$ on register E. To see this, let $|\psi_{x,a}\rangle = \sqrt{\rho_{x,a}} \otimes U_a |\Omega\rangle$ where U_a is some unitary on register B, and $|\Omega\rangle_{\text{BE}}$ is an unnormalized maximally entangled state between registers B and E. Then

$$\begin{aligned} \|\text{Tr}_{\text{E}}(|\psi_{x,0}\rangle\langle\psi_{x,1}|)\|_1 &= \|\text{Tr}_{\text{E}}(\sqrt{\rho_{x,0}} \otimes U_0 |\Omega\rangle\langle\Omega| \sqrt{\rho_{x,1}} \otimes U_1^\dagger)\|_1 \\ &= \|U_0 \sqrt{\rho_{x,0}}^\top \sqrt{\rho_{x,1}} U_1^\dagger\|_1 \\ &= \|\sqrt{\rho_{x,0}}^\top \sqrt{\rho_{x,1}}\|_1 = \|\sqrt{\rho_{x,0}} \sqrt{\rho_{x,1}}\|_1 = \sqrt{F(\rho_{x,0}, \rho_{x,1})} \end{aligned}$$

as desired. Here, $^\top$ and $\bar{\cdot}$ denote transpose and complex conjugate with respect to the standard basis, respectively. The third line follows from the unitary invariance of the trace norm, invariance of the trace norm by complex conjugation, and the definition of fidelity.

By the always strong statistical binding of commitment $\{C_{x,b}\}$ the fidelity between $F(\rho_{x,0}, \rho_{x,1})$ is at most $\epsilon(|x|)$. Thus the cross-terms in the state in [Equation \(9.7\)](#) are small and we get that

the state in Equation (9.7) is within $4\sqrt{\epsilon(|x|)}$ trace distance (and thus by Fuchs van-de Graaf, $1 - 8\sqrt{\epsilon(|x|)}$ fidelity) of

$$\frac{\text{id}_{\mathbb{R}}}{2} \otimes \frac{1}{4} \sum_a |a\rangle\langle a|_{\mathbb{X}} \otimes \text{Tr}_{\mathbb{E}}(|\psi_{x,a}\rangle\langle\psi_{x,a}|) = \frac{\text{id}_{\mathbb{R}}}{2} \otimes \mathcal{N}_x^c(\text{id}_{\mathbb{A}}/2) .$$

Therefore the channel \mathcal{N}_x satisfies the $8\sqrt{\epsilon(|x|)}$ -decoupling condition, so by Proposition 9.4, the channel \mathcal{N}_x is $8\sqrt{\epsilon(|x|)}$ -decodable as desired. \square

Suppose for contradiction that there existed a uniform polynomial-time quantum algorithm $D = (D_x)_x$ that solves the $8\sqrt{\epsilon}$ -Decodable Channel Problem with error $1/n$. For every $x \in \{0, 1\}^*$ define $y_x := (1^1, 1^{r_x}, V_x)$ where r_x is the number of output qubits and V_x is the circuit computing channel \mathcal{N}_x . Then for all x ,

$$F((D_x \circ \mathcal{N}_x)(|\Phi\rangle\langle\Phi|_{\mathbb{R}\mathbb{A}}), |\Phi\rangle\langle\Phi|_{\mathbb{R}\mathbb{A}}) \geq 1 - 1/|x| .$$

Applying Fuchs-van de Graaf we get

$$\text{td}((D_x \circ \mathcal{N}_x)(|\Phi\rangle\langle\Phi|_{\mathbb{R}\mathbb{A}}), |\Phi\rangle\langle\Phi|_{\mathbb{R}\mathbb{A}}) \leq 1/\sqrt{|x|} .$$

Measuring the register \mathbb{R} in the standard basis of both arguments does not increase the trace distance. Using this and convexity we have

$$\frac{1}{2} \sum_b \text{td}((D_x \circ \mathcal{N}_x)(|b\rangle\langle b|_{\mathbb{A}}), |b\rangle\langle b|_{\mathbb{A}}) \leq 1/\sqrt{|x|} . \quad (9.8)$$

We now perform a hybrid argument. Define the channel $\mathcal{N}_x^{(0)} := \mathcal{N}_x$. Define the channel $\mathcal{N}_x^{(1)}$ that prepares the state $|\theta_b^{(1)}\rangle$ that is the same as $|\theta_b\rangle$ except the BE register is prepared in the state $|\psi_{x,0}\rangle$ (i.e., independently of a), and then traces out registers $\mathbb{X}\mathbb{B}$. Observe that the output of $\mathcal{N}_x^{(1)}$ on $|b\rangle$ is

$$\frac{1}{2} \sum_a X^a |b\rangle\langle b| X^a \otimes \rho_{x,0} = \frac{\text{id}}{2} \otimes \rho_{x,0} ,$$

i.e., independent of b . Then

$$\begin{aligned} & \frac{1}{2} \sum_b \text{td}((D_x \circ \mathcal{N}_x^{(0)})(|b\rangle\langle b|), (D_x \circ \mathcal{N}_x^{(1)})(|b\rangle\langle b|)) \\ &= \frac{1}{2} \sum_b \text{td}\left(D_x\left(\frac{1}{2} \sum_a X^a |b\rangle\langle b| X^a \otimes \rho_{x,a}\right), D_x\left(\frac{\text{id}}{2} \otimes \rho_{x,0}\right)\right) \\ &= \frac{1}{2} \sum_b \text{td}\left(D_x\left(\frac{1}{2} |\bar{b}\rangle\langle\bar{b}| \otimes \rho_{x,1}\right), D_x\left(\frac{1}{2} |\bar{b}\rangle\langle\bar{b}| \otimes \rho_{x,0}\right)\right) . \end{aligned}$$

By the computational hiding property of $\{C_{x,b}\}$, for infinitely many $x \in \{0, 1\}^*$ this quantity is at most $\delta(|x|)$ (otherwise D_x could be used to distinguish between $\rho_{x,0}$ and $\rho_{x,1}$ with bias better than $\delta(|x|)$).

Combined with Equation (9.8), we have that for infinitely many x ,

$$\frac{1}{2} \sum_b \text{td}((D_x \circ \mathcal{N}_x^{(1)})(|b\rangle\langle b|), |b\rangle\langle b|) \leq 1/\sqrt{|x|} + \delta(|x|) .$$

However since $(D_x \circ \mathcal{N}_x^{(1)})(|b\rangle\langle b|)$ is a density matrix independent of b , this quantity is at least $\frac{1}{2}$, which is a contradiction for sufficiently large $|x|$ since $\delta(|x|)$ is an inverse polynomial.

We finish by establishing the existence of the commitments promised by [Lemma 9.7](#), assuming the hardness of `DISTUHLMANN`.

Proof of [Lemma 9.7](#). Assume that `DISTUHLMANN` $_{1-\epsilon} \notin \text{avgUnitaryBQP}$ for some negligible function $\epsilon(n)$. Then by [Theorem 6.8](#) we have that `DISTUHLMANN` $_{1-\epsilon} \notin \text{avgUnitaryBQP}_{1-\xi}$ for $\xi(n) = n^{-1/16}$. If $x = (1^n, E, F)$ is a valid `UHLMANN` $_{1-\epsilon}$ instance, then we define the circuits $C'_{x,0} := E$ and $C'_{x,1} := F$. Otherwise, define $C'_{x,0}, C'_{x,1}$ to be circuits such that $|C'_{x,0}\rangle_{\text{BE}} = |0^{2|x} \rangle_{\text{BE}}$ and $|C'_{x,1}\rangle_{\text{BE}} = |0^{|x}\rangle_{\text{B}} \otimes |1^{|x}\rangle_{\text{E}}$. By definition and [Proposition 5.8](#) we have that the family of circuits $\{(C'_{x,0}, C'_{x,1})\}_{x \in \{0,1\}^*}$ satisfies

1. (*Always strong statistical hiding*) For all $x \in \{0,1\}^*$, we have $F(\sigma_{x,0}, \sigma_{x,1}) \geq 1 - \epsilon(|x|)$ where $\sigma_{x,b}$ is the reduced density matrix of $|C'_{x,b}\rangle$ on register `B`.

This is because either x is a valid `UHLMANN` $_{1-\epsilon}$ instance or $C'_{x,0}, C'_{x,1}$ were set to be trivial circuits that satisfy this condition.

2. (*Infinitely often weak computational binding*) For all uniform polynomial time algorithms $A = (A_x)_x$ there exists a polynomial $p(n)$ such that the following holds for infinitely many x :

$$F((\text{id}_{\text{B}} \otimes A_x) |C'_{x,0}\rangle\langle C'_{x,0}|, |C'_{x,1}\rangle\langle C'_{x,1}|) \leq \frac{1}{p(|x|)}.$$

Thus we can think of the collection of circuit pairs $\{(C'_{x,0}, C'_{x,1})\}_x$ as a “pseudo-commitment” that always has strong statistical hiding, and has weak computational binding infinitely often.

By performing the same flavor switching transformation (see [Proposition 8.7](#)) to each instance $(C'_{x,0}, C'_{x,1})$ of this pseudo-commitment, we get another family of circuit pairs $\{(C_{x,0}, C_{x,1})\}_x$ satisfying

1. (*Always strong statistical binding*) For all $x \in \{0,1\}^*$, for all quantum circuits A acting on `B`,

$$F((A \otimes \text{id}_{\text{E}}) |C_{x,0}\rangle\langle C_{x,0}|, |C_{x,1}\rangle\langle C_{x,1}|) \leq 2\epsilon(|x|)^2.$$

2. (*Infinitely often weak computational hiding*) For all uniform polynomial-time algorithms $A = (A_x)_x$, the following holds for infinitely many x :

$$|\Pr(A_x(\rho_{x,0}) = 1) - \Pr(A_x(\rho_{x,1}) = 1)| \leq \sqrt{1/p(|x|)}$$

where $\rho_{x,b}$ is the reduced density matrix of $|C_{x,b}\rangle$ on register `E`.

We make use of Uhlmann’s theorem to rephrase the statistical binding property in terms of the fidelity between the reduced states on register `E`. Namely, by Uhlmann’s theorem, we have that for all x

$$F(\rho_{x,0}, \rho_{x,1}) = \sup_A F((A \otimes \text{id}_{\text{E}}) |C_{x,0}\rangle\langle C_{x,0}|, |C_{x,1}\rangle\langle C_{x,1}|).$$

The statistical binding property ensures that this is at most $2\epsilon(|x|)^2 \leq \epsilon(|x|)$. This concludes the proof. □

□

□

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 equivalent to the complexity of performing 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 9.9 (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 $|\psi\rangle_{\text{AR}}$ of ρ (where R is the purifying register), we have

$$\text{td}\left((D \circ E)(\psi), \psi\right) \leq \delta$$

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 equivalent to the complexity of the Uhlmann Transformation Problem.

9.2.1 Information-theoretic compression

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 just one of a rich zoo of entropy measures that are used in the setting of non-asymptotic quantum information theory [Tom13]. In this section we consider the following entropy measures:

Definition 9.10 (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

$$H_{\min}(\text{A}|\text{B})_\psi := -\log \inf_{\sigma \in \text{Pos}(\text{B}): \psi_{\text{AB}} \leq \text{id}_{\text{A}} \otimes \sigma_{\text{B}}} \text{Tr}(\sigma)$$

The ϵ -smoothed conditional min-entropy is

$$H_{\min}^\epsilon(\text{A}|\text{B})_\psi := \sup_{\sigma: P(\sigma, \psi) \leq \epsilon} H_{\min}(\text{A}|\text{B})_\sigma,$$

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

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

The ϵ -smoothed conditional max-entropy is

$$H_{\max}^{\epsilon}(\mathbf{A}|\mathbf{B})_{\psi} := \inf_{\sigma : \text{td}(\sigma, \psi) \leq \epsilon} H_{\max}(\mathbf{A}|\mathbf{B})_{\sigma}.$$

- The Rényi 2-entropy of register A conditioned on register B of the state ψ is [Dup10, Definition 2.11]

$$H_2(\mathbf{A}|\mathbf{B})_{\psi} := -\log \inf_{\sigma > 0} \text{Tr} \left(\left((\text{id}_{\mathbf{A}} \otimes \sigma_{\mathbf{B}})^{-1/2} \psi_{\mathbf{AB}} \right)^2 \right)$$

where the infimum is over all positive definite density operators σ acting on register B. The ϵ -smoothed conditional Rényi 2-entropy is

$$H_2^{\epsilon}(\mathbf{A}|\mathbf{B})_{\psi} := \sup_{\sigma : \text{td}(\sigma, \psi) \leq \epsilon} H_2(\mathbf{A}|\mathbf{B})_{\sigma}.$$

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 9.11 (Relations between the entropy measures). *Let $\epsilon \geq 0$ and let $|\psi\rangle_{\mathbf{ABC}}$ be a tripartite pure state. The following relationships hold:*

- (Duality relation) $H_{\min}^{\epsilon}(\mathbf{A}|\mathbf{B})_{\psi} = -H_{\max}^{\epsilon}(\mathbf{A}|\mathbf{C})_{\psi}$. We note that this duality relation only holds when ψ is a pure state on registers ABC.
- (Bounds for conditional min/max-entropy) Both $H_{\min}^{\epsilon}(\mathbf{A}|\mathbf{B})_{\psi}$ and $H_{\max}^{\epsilon}(\mathbf{A}|\mathbf{B})_{\psi}$ are bounded below by $-\log \text{rank}(\psi_{\mathbf{A}})$, and bounded above by $\log \text{rank}(\psi_{\mathbf{A}})$.
- (Isometric invariance) For all isometries V mapping register A to A' we have $H_{\min}(\mathbf{A}|\mathbf{B})_{\psi} = H_{\min}(\mathbf{A}'|\mathbf{B})_{V\psi V^{\dagger}}$.
- (Min- versus 2-entropy) $H_{\min}(\mathbf{A}|\mathbf{B})_{\psi} \leq H_2(\mathbf{A}|\mathbf{B})_{\psi}$.
- (Operational interpretation of min-entropy) When $\psi_{\mathbf{AB}}$ is diagonal (i.e., it corresponds to a bipartite probability distribution $p(a, b)$), $2^{-H_{\min}(\mathbf{A}|\mathbf{B})_{\psi}} = \sum_b p(b) \max_a p(a|b)$, 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 $\sigma \in \mathbf{S}(\mathbf{D})$, we have $H_{\max}^{\epsilon}(\mathbf{A})_{\psi} \leq H_{\max}^{\epsilon}(\mathbf{AD})_{\psi \otimes \sigma}$.

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 [Dup10, 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 $\psi_{\mathbf{A}} \mapsto \psi_{\mathbf{A}} \otimes \sigma_{\mathbf{D}}$, which is clearly trace-preserving. \square

Having established the definitions and properties of these entropy measures, we can now state and prove the characterization of the fundamental limits on one-shot compression for quantum states.

Theorem 9.12 (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 $\epsilon_2 := (\delta/40)^4$.

Proof. Lower bound. We first prove the lower bound $H_{\max}^{2\delta^{1/4}}(\rho) \leq K^\delta(\rho)$. Let (E, D) denote a pair of quantum circuits that compresses ρ to $s = K^\delta(\rho)$ qubits with error δ . Let $|\psi\rangle_{\text{AR}}$ denote a purification of ρ . Then using the Fuchs-van de Graaf inequality we get that

$$F\left((D \circ E)(\psi), \psi\right) \geq 1 - 2\delta. \quad (9.9)$$

Let $\hat{E} : \text{A} \rightarrow \text{CE}$, $\hat{D} : \text{C} \rightarrow \text{AF}$ denote the unitary purifications of the channels corresponding to E and D , respectively. Then by Uhlmann's theorem, since $(\hat{D}\hat{E} \otimes \text{id}_{\text{R}})|\psi\rangle_{\text{RA}}$ is a purification of $(D \circ E)(\psi)$ and $|\psi\rangle_{\text{AR}}$ is pure, Equation (9.9) implies that there exists a pure state $|\theta\rangle_{\text{EF}}$ such that

$$1 - 2\delta \leq F\left((D \circ E)(\psi), \psi\right) = F\left((\hat{D} \circ \hat{E})(\psi), \psi_{\text{AR}} \otimes \theta_{\text{EF}}\right) \leq F\left(\text{Tr}_{\text{BC}}\left(\hat{D} \circ \hat{E}(\psi)\right), \rho_{\text{A}} \otimes \theta_{\text{F}}\right).$$

The last inequality follows from monotonicity of the fidelity under partial trace. By Fuchs-van de Graaf we have

$$\text{td}\left(\text{Tr}_{\text{BC}}(\hat{D} \circ \hat{E}(\psi)), \rho_{\text{A}} \otimes \theta_{\text{F}}\right) \leq \sqrt{2\delta}. \quad (9.10)$$

Next consider the following entropy bounds using the properties given by Proposition 9.11:

$$\begin{aligned} s = \dim(\text{C}) &\geq -H_{\min}(\text{C}|\text{RE})_{\hat{E}|\psi} \\ &= -H_{\min}(\text{AF}|\text{RE})_{\hat{D}\hat{E}|\psi} \\ &= H_{\max}(\text{AF})_{\hat{D}\hat{E}|\psi} \\ &\geq H_{\max}^{2\delta^{1/4}}(\text{AF})_{\rho_{\text{B}} \otimes \theta_{\text{R}}} \\ &\geq H_{\max}^{2\delta^{1/4}}(\text{A})_{\rho}. \end{aligned}$$

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 (9.10) 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, Dup10, DBWR14, BCT16]); we use the following one due to Dupuis (together with the standard fact that Clifford unitaries form a 2-design).

Theorem 9.13 (Decoupling Theorem, Theorem 3.8 of [Dup10]). *Let ρ_{AB} be a density matrix, $\mathcal{T} : S(A) \rightarrow S(E)$ be a completely positive superoperator, $\omega_{EA'} = (\mathcal{T} \otimes \text{id}_{A'}) (\Phi_{AA'})$ (where Φ denotes the maximally entangled state), and $\epsilon \geq 0$. Then*

$$\int \|(\mathcal{T} \circ U)(\rho_{AB}) - \omega_E \otimes \rho_B\|_1 dU \leq 2^{-\frac{1}{2}H_2^\epsilon(A'|E)_\omega - \frac{1}{2}H_2^\epsilon(A|B)_\rho} + 8\epsilon$$

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 $\omega_{EA'} = (\mathcal{T} \otimes \text{id}_{A'}) (\Phi_{AA'})$. This can be seen to be

$$\omega_{EA'} = \sum_{y \in \{0,1\}^{n-s}} |yy\rangle\langle yy|_{EA'_1} \otimes 2^{-s} \text{id}_{A'_2}$$

where A' is subdivided into two registers $A'_1 A'_2$ with A'_1 isomorphic to E . The entropy $H_2^\epsilon(A'|E)_\omega$ can be calculated as follows:

$$H_2^\epsilon(A'|E)_\omega \geq H_2(A'|E)_\omega \geq H_{\min}(A'|E)_\omega .$$

The first inequality follows from the definition of the smoothed 2-entropy. The second inequality follows from Proposition 9.11. Note that $\omega_{A'E}$ 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 $H_{\min}(A'|E) = s$.

Now we bound the entropy $H_2^\epsilon(A|R)_\rho$. Since ρ_{AR} is pure, Proposition 9.11 gives us

$$-H_2^\epsilon(A|R)_\rho \leq -H_{\min}^\epsilon(A|R)_\rho = H_{\max}^\epsilon(A)_\rho .$$

By Theorem 9.13, by averaging there exists a Clifford unitary U such that

$$\|(\mathcal{T} \circ U)(\rho_{AR}) - \omega_E \otimes \rho_R\|_1 \leq 2^{-\frac{1}{2}(s - H_{\max}^\epsilon(A)_\rho)} + 8\epsilon := \nu .$$

Consider the following two purifications:

1. $|\Phi\rangle_{EE'} \otimes |\rho\rangle_{AR}$ where $|\Phi\rangle_{EE'}$ denotes the maximally entangled state on two isomorphic registers E, E' . This is a purification of the density matrix $\omega_E \otimes \rho_R$.
2. $|\theta\rangle_{EE'CF} := \sum_y |y\rangle_E \otimes (\Pi_y U \otimes \text{id}_R) |\rho\rangle_{AR} \otimes |0\rangle_F$ where Π_y is the projection that maps A into $E'C$ 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 $(\mathcal{T} \circ U)(\rho_{AR})$.

By Fuchs-van de Graaf and Uhlmann's theorem there exist a partial isometry V mapping registers $E'A$ to $CE'F$ such that

$$\text{td}\left(V(\Phi_{EE'} \otimes \rho_{AR})V^\dagger, \theta_{EE'CRF}\right) \leq \sqrt{2\nu}.$$

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

$$\left|\text{Tr}(P(\Phi_{EE'} \otimes \rho_{AR})) - 1\right| \leq \text{td}\left(P(\Phi_{EE'} \otimes \rho_{AR})P, \theta_{EE'CRF}\right) \leq \text{td}\left(V(\Phi_{EE'} \otimes \rho_{AR})V^\dagger, \theta_{EE'CRF}\right) \leq \sqrt{2\nu}.$$

Let τ denote the post-measurement state of $\Phi_{EE'} \otimes \rho_{AR}$ after measuring the projector P ; by the Gentle Measurement Lemma [Win99] we have $\text{td}(\tau, \Phi_{EE'} \otimes \rho_{AR}) \leq 4\nu^{1/4}$. Thus

$$\begin{aligned} \text{td}\left(\Xi(\Phi_{EE'} \otimes \rho_{AR}), \theta_{EE'CRF}\right) &\leq \text{td}\left(\Xi(\Phi_{EE'} \otimes \rho_{AR}), \Xi(\tau)\right) + \text{td}\left(\Xi(\tau), V\tau V^\dagger\right) \\ &\quad + \text{td}\left(V\tau V^\dagger, V(\Phi_{EE'} \otimes \rho_{AR})V^\dagger\right) + \text{td}\left(V(\Phi_{EE'} \otimes \rho_{AR})V^\dagger, \theta_{EE'CRF}\right) \\ &\leq 4\nu^{1/4} + 4\nu^{1/4} + \sqrt{2\nu} \leq 10\nu^{1/4}, \end{aligned} \tag{9.11}$$

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

$$\text{td}\left(\Phi_{EE'} \otimes \rho_{AR}, \Lambda(\theta_{EE'CRF})\right) \leq 10\nu^{1/4}.$$

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 (9.11) and using that the trace distance is non-increasing under quantum operations we have

$$\sum_y 2^{-(n-s)} \text{td}\left(\Xi(|y\rangle\langle y|_{E'} \otimes |\rho\rangle\langle\rho|_{AR}), 2^{n-s}\alpha_y |y\rangle\langle y|_{E'} \otimes |\rho_{U,y}\rangle\langle\rho_{U,y}|_{CR} \otimes |0\rangle\langle 0|_F\right) \leq 10\nu^{1/4},$$

where $\alpha_y := \|\Pi_y U |\rho\rangle_{AR}\|^2$ and the pure state $|\rho_{U,y}\rangle_{RC}$ is defined so that

$$\alpha_y^{-1/2} \Pi_y U |\rho\rangle_{AR} = |y\rangle_{E'} \otimes |\rho_{U,y}\rangle_{CR}.$$

By averaging, there exists a $y^* \in \{0, 1\}^{n-s}$ such that

$$\text{td}\left(\Xi(|y^*\rangle\langle y^*|_{E'} \otimes |\rho\rangle\langle\rho|_{AR}), 2^{n-s}\alpha_{y^*} |y^*\rangle\langle y^*|_{E'} \otimes |\rho_{U,y^*}\rangle\langle\rho_{U,y^*}|_{CR} \otimes |0\rangle\langle 0|_F\right) \leq 10\nu^{1/4}.$$

This also implies that $|2^{n-s}\alpha_{y^*} - 1| \leq 10\nu^{1/4}$ so thus

$$\text{td}\left(\Xi(|y^*\rangle\langle y^*|_{E'} \otimes |\rho\rangle\langle\rho|_{AR}), |y^*\rangle\langle y^*|_{E'} \otimes |\rho_{U,y^*}\rangle\langle\rho_{U,y^*}|_{CR} \otimes |0\rangle\langle 0|_F\right) \leq 10\nu^{1/4}. \tag{9.12}$$

Define the following quantum circuits:

1. The circuit E acts on register A and behaves as follows: it appends the state $|y^*\rangle$ in register E' , applies the channel Ξ , and then traces out registers $E'F$. In other words, it implements the following channel:

$$E(\sigma_A) = \text{Tr}_{E'F}\left(\Xi(|y^*\rangle\langle y^*|_{E'} \otimes \sigma_A)\right).$$

2. The circuit D takes as input register \mathbf{C} and behaves as follows: it appends the state $|y^*\rangle$ in register \mathbf{E}' and $|0\rangle$ in register \mathbf{F} , applies the channel Λ , and then traces out register \mathbf{E}' . In other words, it implements the following channel:

$$D(\tau_{\mathbf{C}}) = \text{Tr}_{\mathbf{E}'}\left(\Lambda(|y^*\rangle\langle y^*|_{\mathbf{E}'} \otimes \tau_{\mathbf{C}} \otimes |0\rangle\langle 0|_{\mathbf{F}})\right).$$

Then Equation (9.12) implies that

$$\begin{aligned} \text{td}\left(E(|\rho\rangle\langle\rho|_{\mathbf{AR}}), |\rho_{U,y^*}\rangle\langle\rho_{U,y^*}|_{\mathbf{CR}}\right) &\leq 10\nu^{1/4} \\ \text{td}\left(|\rho\rangle\langle\rho|_{\mathbf{AR}}, D(|\rho_{U,y^*}\rangle\langle\rho_{U,y^*}|_{\mathbf{CR}})\right) &\leq 10\nu^{1/4}. \end{aligned}$$

Put together this means

$$\text{td}\left((D \circ E)(|\rho\rangle\langle\rho|_{\mathbf{AR}}), |\rho\rangle\langle\rho|_{\mathbf{AR}}\right) \leq 20\nu^{1/4}.$$

Although we have defined the circuits E, D in terms of the purification $|\rho\rangle_{\mathbf{AR}}$, observe that Uhlmann's theorem implies that the same circuits works for *all* purifications of $\rho_{\mathbf{A}}$. Thus, since the output of channel E is register \mathbf{C} which has size s qubits, this shows that (E, D) compresses ρ to s qubits with error $20\nu^{1/4}$. By our choice of $s = H_{\max}^{\epsilon}(\mathbf{B})_{\rho} + 8 \log \frac{4}{\delta}$ and $\epsilon = (\delta/40)^4$, this error is at most δ . \square

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

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

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].²⁰ Thus Theorem 9.12 applied to tensor product states $\rho^{\otimes k}$ recovers Schumacher compression [Sch95], using a proof that does not appeal to typical subspaces and the method of types.

9.2.2 Complexity of near-optimal compression

We now initiate the study of the computational complexity of compressing 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 9.14 (Compression as a computational task). *Let $\epsilon, \eta : \mathbb{N} \rightarrow [0, 1]$ 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 $\rho_x := C(|0 \dots 0\rangle\langle 0 \dots 0|)$ to at most $H_{\max}^{\epsilon(n)}(\rho_x) + O(\log \frac{1}{\epsilon(n)})$ qubits with error at most $\eta(n)$.*

²⁰In 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 9.15 (Near-optimal compression via Uhlmann transformations). *Let $\epsilon(n)$ be a negligible function. If $\text{DISTUHLMANN}_{1-\epsilon} \in \text{avgUnitaryBQP/poly}$, then for all polynomials $q(n)$ there exists a pair of non-uniform 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 $\rho_x = C(|0 \dots 0\rangle\langle 0 \dots 0|)$. Let $\epsilon = \epsilon(n)$. The proof of the upper bound of [Theorem 9.12](#) involves the following two states:

$$\begin{aligned} |F\rangle &:= |\Phi\rangle_{\text{EE}'} \otimes |\rho\rangle_{\text{AR}}, \\ |G\rangle &:= \sum_y |y\rangle_{\text{E}} \otimes (\Pi_y U \otimes \text{id}_{\text{R}}) |\rho\rangle_{\text{AR}} \otimes |0\rangle_{\text{F}}. \end{aligned}$$

(The state $|G\rangle$ was called $|\theta\rangle$ in [Theorem 9.12](#)). Here, $|\Phi\rangle_{\text{EE}'}$ denotes the maximally entangled state on EE' , $|\rho\rangle_{\text{AR}}$ 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 9.12](#) 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 $\text{UHLMANN}_{1-\epsilon}$ instance. Since $\text{DISTUHLMANN}_{1-\epsilon} \in \text{avgUnitaryBQP/poly}$ by assumption there exists $\text{poly}(n, |C|)$ -size circuit L mapping registers $\text{E}'\text{A}$ to $\text{E}'\text{CF}$ and a channel completion Ξ of the canonical Uhlmann transformation V corresponding to $(|F\rangle, |G\rangle)$ such that

$$\text{td}\left((\text{id} \otimes L)(|F\rangle\langle F|), (\text{id} \otimes \Xi)(|F\rangle\langle F|)\right) \leq \frac{1}{r(n)}$$

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 $\text{poly}(n, |C|)$ -size circuit M and a channel completion Λ of the Uhlmann transformation V^\dagger corresponding to $(|G\rangle, |F\rangle)$ such that

$$\text{td}\left((\text{id} \otimes M)(|G\rangle\langle G|), (\text{id} \otimes \Lambda)(|G\rangle\langle G|)\right) \leq \frac{1}{r(n)}.$$

The proof of [Theorem 9.12](#) shows that there exists a pair of circuits (E_x^*, D_x^*) that compresses ρ_x to $s = H_{\max}^\epsilon(\rho_x) + O(\log \frac{1}{\epsilon})$ qubits with error ϵ . Notice that the circuits E_x^*, D_x^* are $\text{poly}(n)$ -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 $\text{poly}(n, |C|)$ -sized circuits. Using L, M instead of the channels Ξ, Λ incurs at most $O(1/r(n))$ error, i.e., $\text{td}\left((D_x \circ E_x)(|\rho\rangle\langle \rho|_{\text{AR}}), (D_x^* \circ E_x^*)(|\rho\rangle\langle \rho|_{\text{AR}})\right) \leq 2/r(n)$. Therefore

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

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

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 9.16 (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 $k \in \{0, 1\}^\lambda$ 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*

$$\left| \Pr_{k \leftarrow \{0,1\}^\lambda} \left[A_\lambda^{O_{\psi_k}}(G_\lambda(k)^{\otimes t(\lambda)}) = 1 \right] - \Pr_{|\vartheta\rangle \leftarrow \text{Haar}_{m(\lambda)}} \left[A_\lambda^{O_\vartheta}(|\vartheta\rangle\langle\vartheta|^{\otimes t(\lambda)}) = 1 \right] \right| \leq \epsilon(\lambda),$$

where $O_\psi := \text{id} - 2|\psi\rangle\langle\psi|$ 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 key length 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 9.17 (Hardness of near-optimal compression). *Let $\epsilon(n)$ be a function. Let $m(\lambda)$ be a function satisfying*

$$m(\lambda) > \lambda + O\left(\log \frac{1}{\epsilon(m(\lambda))}\right) + 2$$

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 9.17](#), 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:

$$|\varphi_\lambda\rangle_{\text{KQA}} := 2^{-\lambda/2} \sum_{k \in \{0,1\}^\lambda} |k\rangle_{\text{K}} \otimes |\tau_\lambda\rangle_{\text{Q}} \otimes |\psi_k\rangle_{\text{A}}$$

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 $R := KQ$. 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 9.11](#) we have $H_{\max}^\epsilon(\rho_\lambda) \leq \lambda$.

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 $\text{poly}(\lambda)$ -sized circuit. Therefore (E_x, D_x) runs in $\text{poly}(\lambda)$ time and compresses ρ_λ to $r_\lambda := H_{\max}^\epsilon(\rho_\lambda) + O\left(\log \frac{1}{\epsilon(m(\lambda))}\right) \leq \lambda + O\left(\log \frac{1}{\epsilon(m(\lambda))}\right)$ qubits. By assumption we have

$$\text{td}\left((D_x \circ E_x)(|\varphi_\lambda\rangle\langle\varphi_\lambda|), |\varphi_\lambda\rangle\langle\varphi_\lambda|\right) \leq \frac{1}{2} .$$

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

$$\mathbb{E}_k \text{td}\left((D_x \circ E_x)(|\psi_k\rangle\langle\psi_k|), |\psi_k\rangle\langle\psi_k|\right) \leq \frac{1}{2} . \quad (9.13)$$

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 $O_\theta = \text{id} - 2|\theta\rangle\langle\theta|$. It then

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

From [Equation \(9.13\)](#) 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 $\text{poly}(\lambda)$ time, by the pseudorandomness property of G the probability that A_λ accepts $|\vartheta\rangle$ is at least $\frac{1}{2} - \text{negl}(\lambda)$.

On the other hand we show that since a Haar-random state cannot be compressed, A_λ cannot accept with high probability. Let $R := 2^{r_\lambda}$ 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

$$\int_{\vartheta} \text{Tr}\left((D \circ E)(|\vartheta\rangle\langle\vartheta|) |\vartheta\rangle\langle\vartheta|\right) d\vartheta = \int_{\vartheta} \text{Tr}\left(E(|\vartheta\rangle\langle\vartheta|) D^*(|\vartheta\rangle\langle\vartheta|)\right) d\vartheta$$

where D^* denotes the *adjoint channel* corresponding to D ; it is the unique superoperator mapping register A' to B satisfying $\text{Tr}(XD(Y)) = \text{Tr}(D^*(X)Y)$ for all operators X, Y . Viewing $E \otimes D^*$ as a superoperator mapping registers $A_1 A_2$ to $B_1 B_2$ and letting $S_{B_1 B_2}$ denote the swap operator on registers $B_1 B_2$ the above is equal to

$$\text{Tr}\left(S_{B_1 B_2}(E \otimes D^*)\left(\int_{\vartheta} |\vartheta\rangle\langle\vartheta|^{\otimes 2} d\vartheta\right)\right) .$$

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 $\frac{1}{2}(\text{id} + S)$ 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

$$\begin{aligned}
& \frac{1}{M(M+1)} \text{Tr} \left(S_{B_1 B_2} (E \otimes D^*) (\text{id}_{A_1 A_2} + S_{A_1 A_2}) \right) \\
& \leq \frac{1}{M(M+1)} \text{Tr} \left((E \otimes D^*) (\text{id}_{A_1 A_2} + S_{A_1 A_2}) \right) \\
& = \frac{1}{M(M+1)} \left[\text{Tr} \left((E \otimes D^*) (\text{id}_{A_1 A_2}) \right) + \text{Tr} \left((E \otimes D^*) (S_{A_1 A_2}) \right) \right] \\
& = \frac{1}{M(M+1)} \left[\text{Tr} \left(\text{id}_{A_1} \otimes D^* (\text{id}_{A_2}) \right) + \text{Tr} \left((\text{id}_{A_1} \otimes D^*) (S_{A_1 A_2}) \right) \right] \\
& = \frac{1}{M(M+1)} \left[\text{Tr} \left(\text{id}_{A_1} \right) \text{Tr} \left(D^* (\text{id}_{A_2}) \right) + \text{Tr} \left(D^* (\text{id}_{A_2}) \right) \right] \\
& = \frac{1}{M(M+1)} \left[RM + R \right] \\
& = R/M = 2^{-(m(\lambda) - \lambda - O(\log 1/\epsilon))} \leq \frac{1}{4}.
\end{aligned}$$

The second line follows from the fact that $|\text{Tr}(A^\dagger B)| \leq \|A\|_\infty \|B\|_1$ 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 , $\text{Tr}(D^*(\text{id}_{A_2})) = \text{Tr}(\text{id}_B) = R$. 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 $\frac{1}{2} - \text{negl}(\lambda)$ 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. \square

We compare our hardness result with the upper bound proved in [Theorem 9.15](#). As an example, let $\epsilon(n) = 2^{-\log^2(n)}$, which is a negligible function. Then roughly, if $\text{DISTUHLMANN}_{1-\epsilon}$ is easy, then compressing to $H_{\max}^\epsilon(\rho) + O(\log 1/\epsilon) = H_{\max}^\epsilon(\rho) + O(\log^2(n))$ 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 $H_{\max}^\epsilon(\rho) + O(\log^2(n))$ 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 [MY22b]. 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 9.15](#). 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 21. Is the complexity of optimal compression equivalent to the complexity of the Uhlmann Transformation Problem?

9.3 Complexity of classical Shannon tasks?

Given the results in this section, the reader may naturally wonder about the complexity of *classical* Shannon tasks. For example, one can consider the problems of decoding noisy classical channels and optimally compressing classical information. The complexity of both these tasks appears to be essentially *equivalent* to the existence of one-way functions, which provides some evidence that the hardness of the Uhlmann Transformation Problem could be regarded as the natural quantum analogue of the existence of one-way functions.

We sketch this equivalence for these two Shannon theory problems. The classical analogue of the Decodable Channel Problem is as follows. A decodable classical channel N is a classical circuit that takes as input two strings (x, r) where both x and r are sampled from the uniform distribution, and outputs a string y such that with high probability over (x, r) , the original message x is information-theoretically recoverable. The task is to recover the original message x given the output y of the channel.

Impagliazzo and Levin [IL89] showed that if all one-way functions can be inverted in polynomial time with high probability, then there exists a *distributional inverter* that, given an output y of the channel N , finds a uniformly random preimage (x, r) . The decodability of N ensures that the computed x is the original message with high probability. Conversely, if one-way functions exist then pseudorandom generators exist [HILL99]. The channel N that takes the input x and computes a pseudorandom generator on it is not efficiently decodable in polynomial time.

We now turn to compression. Interestingly, the complexity of compression – and other Shannon theory tasks – was already discussed in Yao’s seminal 1982 paper introducing the theory of pseudorandomness [Yao82]. In modern day terms, Yao argued that the existence of pseudorandom generators (which follows from the existence of one-way functions [HILL99]) gives rise to efficiently sampleable distributions X that cannot be efficiently compressed to their Shannon entropy $H(X)$. Conversely, a recent work of [HMS23] shows that if one-way functions do not exist, every efficiently sampleable distribution X can be compressed to a prefix-free encoding of at most $H(X) + 2$ bits.

These two examples motivate asking the broader question: what is the complexity of other fundamental classical Shannon theory tasks, such as obtaining capacity-achieving encoders and decoders for a given classical channel (which is provided in the form of a randomized circuit), or performing distributed source coding? Is the complexity of these tasks all equivalent to the hardness of one-way functions? To our knowledge there has not been a systematic study of the complexity of classical Shannon theory tasks, aside from a few isolated discussions [Yao82, Lip94].

Open Problem 22. Can the complexity of *classical* Shannon theory tasks be characterized?

9.4 Open problems

We end this section with some additional open questions. First, the complexity result about compression is stated in terms of the non-uniform complexity class $\text{avgUnitaryBQP/poly}$. The main reason for this is that the upper bound (i.e., if DISTUHLMANN is easy, then compression is also easy) involves hardcoding some information that depends on the instance of the problem.

Open Problem 23. Can the assumptions in the upper bound result for compression (Theorem 9.15) be improved to be about uniform unitary complexity classes (namely, avgUnitaryBQP)?

This may require finding a new proof approach for the upper bound.

In this section we considered two basic quantum Shannon theory tasks. 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 24. What is the complexity of other quantum Shannon theory tasks, such as achieving capacity over a noisy channel, entanglement distillation, or quantum state redistribution?

We remark that the problem of proving complexity lower bounds on entanglement distillation appears to be conceptually challenging as it requires reasoning about LOCC protocols.

10 Applications to Computational Tasks in High-Energy Physics

In this section, we discuss connections between the Uhlmann Transformation Problem and computational tasks motivated by questions in high-energy physics. We first discuss 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. Then, we discuss the *interference detection task* as formalized by Aaronson, Atia, and Susskind [AAS20]: this is the problem of detecting the interference between two orthogonal states $|\psi\rangle$ and $|\varphi\rangle$, i.e. whether the states are in an equal plus or minus superposition. One of the motivations for considering this problem is the task of physically distinguishing between superpositions of spacetime geometries in the AdS/CFT correspondence [AAS20]. We show that solving the interference detection problem between two orthogonal **statePSPACE** states reduces to **SUCCINCTUHLMANN₁** in polynomial time.

10.1 Black hole radiation decoding

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 $|EPR\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ 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 $SZK \not\subseteq BQP$ – 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 $SZK \subseteq BQP$ 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 $P = PSPACE$. 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 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].

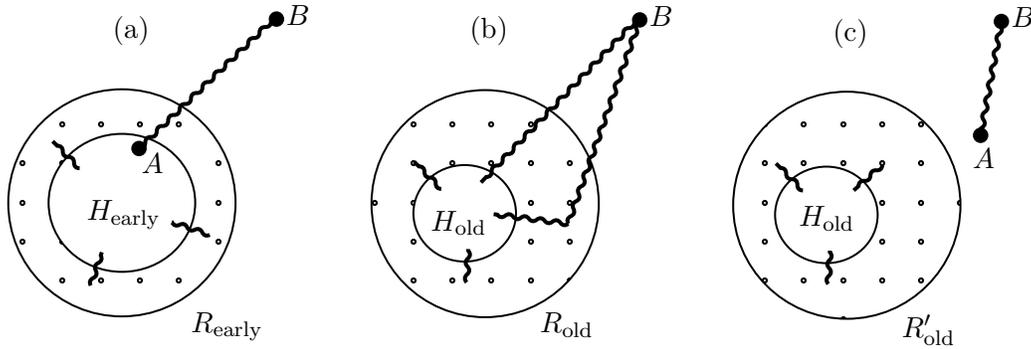


Figure 4: Decoding black hole radiation. (a) Qubit A , maximally entangled with qubit B , falls into an early black hole H_{early} , which is entangled with some early Hawking radiation R_{early} . (b) After evaporating much of its mass, the old black hole H_{old} is entangled with the radiation R_{old} which is entangled with the qubit B . (c) By performing a computation on the radiation only, the partner qubit A can be decoded.

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*

$$|\psi\rangle_{\text{BHR}} := (\text{id}_B \otimes P_{AG \rightarrow HR}) |\text{EPR}\rangle_{BA} \otimes |0\rangle_G .$$

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 $(\text{id} \otimes D)(|\psi\rangle\langle\psi|)$, we have

$$F\left(|\text{EPR}\rangle\langle\text{EPR}|_{AB}, \rho_{AB}\right) \geq 1 - \epsilon$$

i.e., measuring the registers BA in the Bell basis yields the state $|\text{EPR}\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ 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 4](#) 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. *$\text{DISTUHLMANN}_{1-\epsilon} \in \text{avgUnitaryBQP}$ for all negligible functions $\epsilon(n)$ if and only if for all inverse polynomials $\delta(n)$ the $\epsilon(n)$ -black hole radiation decoding task is solvable in polynomial-time with error $\delta(n)$.*

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 $P : \text{AG} \rightarrow \text{HR}$ 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 . \square

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.

10.2 Interference detection

In this section, we consider the computational task of *interference detection* between orthogonal PSPACE states. Aaronson, Atia, and Susskind [[AAS20](#)] recently proved the following folklore observation, sometimes called the *swapping-distinguishing equivalence*: if one can detect the interference between two orthogonal states $|\psi\rangle$ and $|\varphi\rangle$, i.e. whether the states are in an equal superposition

$$\frac{|\psi\rangle + |\varphi\rangle}{\sqrt{2}} \quad \text{and} \quad \frac{|\psi\rangle - |\varphi\rangle}{\sqrt{2}},$$

then one can also *swap* between $|\psi\rangle$ and $|\varphi\rangle$, and vice versa. We first review the swapping-distinguishing equivalence shown by Aaronson, Atia, and Susskind [[AAS20](#)].

Theorem 10.5 ([[AAS20](#)], Theorem 1). *Suppose that $|\psi\rangle$ and $|\varphi\rangle$ are n -qubit orthogonal states. Then, the following two statements are equivalent:*

- There exists a “swapping” unitary U such that

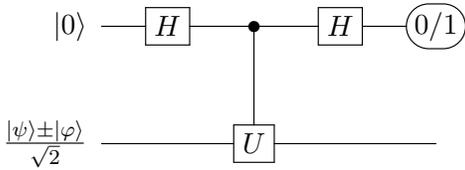
$$U |\psi\rangle = |\varphi\rangle \quad \text{and} \quad U |\varphi\rangle = |\psi\rangle .$$

- There exists an “interference detector” unitary V that perfectly distinguishes between

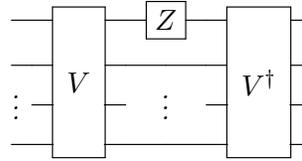
$$\frac{|\psi\rangle + |\varphi\rangle}{\sqrt{2}} \quad \text{and} \quad \frac{|\psi\rangle - |\varphi\rangle}{\sqrt{2}} .$$

Specifically, by “distinguish” we mean that V takes one of the two states as input and stores its guess for which state it received as the first qubit of its output.

Moreover, constructing V from U (and vice versa) only incurs a constant multiplicative factor in terms of circuit complexity. The conversion uses the following circuits:



Circuit for interference detection unitary V using a controlled-swap (controlled- U) operation.



Circuit for swapping unitary U using the interference detector unitary V and its inverse.

We now formalize the task of detecting interference between orthogonal statePSPACE states as the following problem, where the input consists of two orthogonal statePSPACE states.

Definition 10.6 (Interference detection between orthogonal statePSPACE states). *We say that a quantum algorithm $A = (A_x)_x$ solves the INTERFERENCEDETECTION task if for all $x = (1^n, \hat{C}, \hat{D})$ where \hat{C} and \hat{D} are succinct descriptions of unitary quantum circuits C and D acting on n qubits such that the states $|C\rangle := C |0^n\rangle$ and $|D\rangle := D |0^n\rangle$ are orthogonal, the circuit A_x perfectly distinguishes between the superpositions*

$$\frac{|C\rangle + |D\rangle}{\sqrt{2}} \quad \text{and} \quad \frac{|C\rangle - |D\rangle}{\sqrt{2}} .$$

Remark 10.7. One can also relax Definition 10.6 to allow the algorithm A to distinguish between the two superpositions imperfectly, but for simplicity we focus on the perfect case. We also note that A is solving a “quantum-input decision problem” in the sense that we only care about a single bit of its output, but, in contrast to traditional decision problems, its input is one of two quantum states.

The motivation behind this definition of INTERFERENCEDETECTION is the following. It is an interesting task only if the two states $|C\rangle, |D\rangle$ for which we are trying to swap or determine the phase are in some sense highly complex. For example if $|C\rangle, |D\rangle$ were computable by polynomial sized circuits then one could efficiently swap or detect the phase by applying C^\dagger and then checking whether the result is all zeroes. On the other hand, suppose that $|C\rangle, |D\rangle$ were the results of some very long computations. An example that motivated Aaronson, Atia, and Susskind is if $|C\rangle, |D\rangle$

represent distinct spacetime geometries that were produced by a complex physical process (such as black hole formation) after a long amount of time. What is the complexity of detecting whether one is a *superposition* of the two spacetime geometries? [Theorem 10.5](#) shows that this is the same complexity as mapping from one spacetime to another.

Thus in our definition we incorporate the high complexity of the states $|C\rangle, |D\rangle$ by allowing them to be generated by a polynomial space computation. One could also consider the interference detection problem for other classes of states; we leave this for future work.

We now upper bound the complexity of solving INTERFERENCEDETECTION (for statePSPACE states). We show that INTERFERENCEDETECTION polynomial-time reduces to DISTSUCCINCTUHLMANN₁, in a sense made precise in the following theorem.

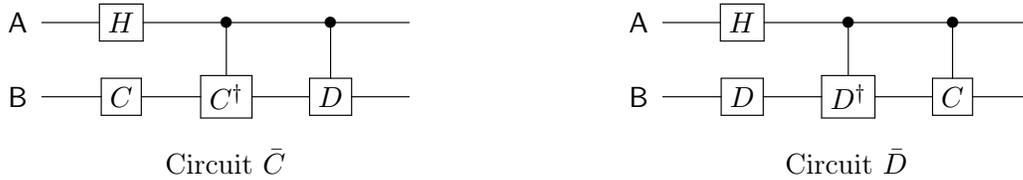
Theorem 10.8. *There exists a polynomial-time query algorithm A with access to a DISTSUCCINCTUHLMANN₁ oracle that solves INTERFERENCEDETECTION.*

Proof. Consider an instance $x = (1^n, \hat{C}, \hat{D})$, where C, D are succinct descriptions of unitary quantum circuits C, D such that $|C\rangle, |D\rangle$ are orthogonal n qubit states. First, we show how to construct circuits C', D' to obtain a swapping unitary with

$$U |C\rangle = |D\rangle \quad \text{and} \quad U |D\rangle = |C\rangle$$

with a single call to the oracle for DISTSUCCINCTUHLMANN₁. Next, we show how to modify C' and D' in order to obtain a controlled- U unitary instead which suffices for interference detection according to the swapping and distinguishing equivalence from [Theorem 10.5](#).

Let A be a single-qubit register initialized to $|0\rangle$, and let B be an n -qubit register initialized to $|0^n\rangle$. We first construct circuits \bar{C}, \bar{D} acting on $n + 1$ qubits as follows:



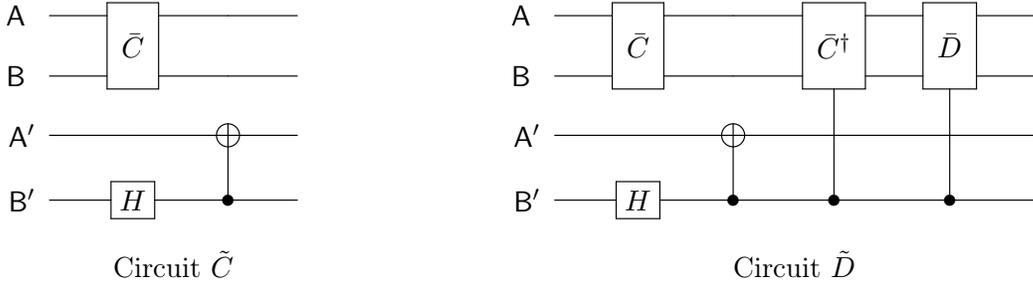
In other words, the circuits \bar{C}, \bar{D} produce the following states

$$\begin{aligned} \bar{C} |0\rangle_A \otimes |0^n\rangle_B &= \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |C\rangle_B + |1\rangle_A \otimes |D\rangle_B), \\ \bar{D} |0\rangle_A \otimes |0^n\rangle_B &= \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |D\rangle_B + |1\rangle_A \otimes |C\rangle_B). \end{aligned}$$

Since $|C\rangle$ and $|D\rangle$ are orthogonal, the reduced states in system A are equal to $\frac{\text{id}}{2}$ in both cases. Therefore, with a single call to the oracle for DISTSUCCINCTUHLMANN₁ with respect to the circuits C' and D' , we obtain swapping unitary $U \in L(B)$ such that

$$U |C\rangle = |D\rangle \quad \text{and} \quad U |D\rangle = |C\rangle .$$

We now construct circuits \tilde{C} and \tilde{D} which allow us to obtain a controlled- U operation with a single call to DISTSUCCINCTUHLMANN₁. The circuits are defined as follows:



We now consider the pure states generated by \tilde{C} and \tilde{D} when applied to $n + 2$ qubits initialized to $|0\rangle$. Let A' and B' be single qubit registers initialized to $|0\rangle$. First, by applying \tilde{C} to $|0^{n+2}\rangle$, we obtain the following state

$$|\tilde{C}\rangle_{AA'BB'} = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |\text{EPR}\rangle_{A'B'} \otimes |C\rangle_B + |1\rangle_A \otimes |\text{EPR}\rangle_{A'B'} \otimes |D\rangle_B).$$

Moreover, by applying \tilde{D} to $|0^{n+2}\rangle$, we obtain the state

$$|\tilde{D}\rangle_{AA'BB'} = \left(\sum_{c \in \{0,1\}} |c\rangle\langle c|_{B'} \otimes \bar{D}_{AB}^c \right) \left(\sum_{b \in \{0,1\}} |b\rangle\langle b|_{B'} \otimes (\bar{C}^\dagger)_{AB}^b \right) |\tilde{C}\rangle_{AA'BB'}.$$

Let us now define density operators

$$\rho_{AA'BB'} = |\tilde{C}\rangle\langle\tilde{C}|_{AA'BB'} \quad \text{and} \quad \sigma_{AA'BB'} = |\tilde{D}\rangle\langle\tilde{D}|_{AA'BB'}.$$

Because $|C\rangle$ and $|D\rangle$ are orthogonal, the reduced states $\rho_{AA'}$ and $\sigma_{AA'}$ satisfy

$$\rho_{AA'} = \sigma_{AA'} = \frac{\text{id}_{AA'}}{4}.$$

By Uhlmann's theorem there exists a unitary \tilde{U} acting on registers $B'B$ such that $|\tilde{D}\rangle = (\text{id}_{AA'} \otimes \tilde{U}_{B'B}) |\tilde{C}\rangle$. In particular, the unitary \tilde{U} satisfies

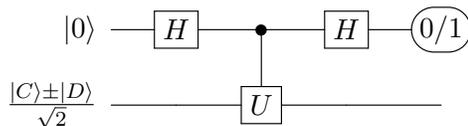
$$\begin{aligned} \tilde{U} |0\rangle_{B'} |C\rangle_B &= |0\rangle_{B'} |C\rangle_B \\ \tilde{U} |0\rangle_{B'} |D\rangle_B &= |0\rangle_{B'} |D\rangle_B \\ \tilde{U} |1\rangle_{B'} |C\rangle_B &= |1\rangle_{B'} |D\rangle_B \\ \tilde{U} |1\rangle_{B'} |D\rangle_B &= |1\rangle_{B'} |C\rangle_B. \end{aligned}$$

Hence, \tilde{U} acts as the controlled- U operator of the form

$$\tilde{U} = \sum_{c \in \{0,1\}} |c\rangle\langle c|_{B'} \otimes U_B^c,$$

where U is the swapping unitary from before. Therefore, we can use the following circuit to perfectly distinguish between $\frac{|C\rangle+|D\rangle}{\sqrt{2}}$ and $\frac{|C\rangle-|D\rangle}{\sqrt{2}}$ with a single call to the oracle for

$\text{DISTSUCCINCTUHLMANN}_1$ with respect to the circuits \tilde{C} and \tilde{D} and the state $|+\rangle \otimes \frac{|C\rangle \pm |D\rangle}{\sqrt{2}}$.



□

10.3 Open problems

We conclude with some open problems related to the physics-inspired applications considered in this section.

Open Problem 25. Does the complexity of any of the information processing tasks discussed in this paper (e.g., compression) have any ramifications for holography or models of quantum gravity? May [May19] has recently suggested that information tasks performable in the bulk are also performable on the boundary of the AdS/CFT correspondence. Does this correspondence also preserve the complexity of the task?

Open Problem 26. What is the complexity of INTERFERENCEDETECTION? Can we argue that it is hard for some unitary complexity class? For example, can we use the equivalence in Theorem 10.5 to argue that $\text{DISTSUCCINCTUHLMANN}_1$ reduces to INTERFERENCEDETECTION, thereby rendering the two tasks equivalent?

Open Problem 27. What is the complexity of INTERFERENCEDETECTION with states drawn from some other state complexity class (e.g., a state complexity analogue of QMA or SZK)?

References

- [AA17] Yosi Atia and Dorit Aharonov. “Fast-forwarding of Hamiltonians and exponentially precise measurements”. In: *Nature Communications* 8.1 (2017), p. 1572. DOI: [10.1038/s41467-017-01637-7](https://doi.org/10.1038/s41467-017-01637-7) (cit. on p. 31).
- [AA23] Anurag Anshu and Srinivasan Arunachalam. *A survey on the complexity of learning quantum states*. 2023. arXiv: [2305.20069](https://arxiv.org/abs/2305.20069) (cit. on p. 17).
- [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](https://doi.org/10.1098/rspa.2007.0113) (cit. on p. 17).
- [Aar09] Scott Aaronson. “Quantum Copy-Protection and Quantum Money”. In: *2009 24th Annual IEEE Conference on Computational Complexity* (2009). DOI: [10.1109/ccc.2009.42](https://doi.org/10.1109/ccc.2009.42) (cit. on pp. 87, 94).
- [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](https://doi.org/10.1007/s00224-013-9527-3) (cit. on p. 25).
- [Aar16] Scott Aaronson. *The Complexity of Quantum States and Transformations: From Quantum Money to Black Holes*. 2016. arXiv: [1607.05256](https://arxiv.org/abs/1607.05256) (cit. on pp. 5, 92, 113).

- [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](https://arxiv.org/abs/2009.07450) (cit. on pp. 16, 113, 115).
- [ABV23] Rotem Arnon-Friedman, Zvika Brakerski, and Thomas Vidick. *Computational Entanglement Theory*. 2023. arXiv: [2310.02783](https://arxiv.org/abs/2310.02783) (cit. on p. 14).
- [AC12] Scott Aaronson and Paul Christiano. “Quantum Money from Hidden Subspaces”. In: *Proceedings of the Forty-Fourth Annual ACM Symposium on Theory of Computing*. 2012, pp. 41–60. DOI: [10.1145/2213977.2213983](https://doi.org/10.1145/2213977.2213983) (cit. on pp. 13, 86, 88, 94).
- [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](https://doi.org/10.1038/s41467-021-27922-0) (cit. on p. 5).
- [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](https://doi.org/10.1098/rspa.2009.0202) (cit. on pp. 4, 113).
- [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](https://doi.org/10.1109/CCC.2007.26) (cit. on p. 92).
- [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](https://doi.org/10.1103/PhysRevA.70.052328) (cit. on p. 108).
- [Aha03] Dorit Aharonov. *A Simple Proof that Toffoli and Hadamard are Quantum Universal*. 2003. arXiv: [quant-ph/0301040](https://arxiv.org/abs/quant-ph/0301040) (cit. on p. 94).
- [AJW18] Anurag Anshu, Rahul Jain, and Naqeeb 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](https://doi.org/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](https://doi.org/10.4086/toc.2007.v003a007) (cit. on pp. 6, 17, 76).
- [AKL⁺22] Prabhanjan Ananth, Fatih Kaleoglu, Xingjian Li, Qipeng Liu, and Mark Zhandry. “On the Feasibility of Unclonable Encryption, and More”. In: *Advances in Cryptology – CRYPTO 2022*. 2022, pp. 212–241. DOI: [10.1007/978-3-031-15979-4_8](https://doi.org/10.1007/978-3-031-15979-4_8) (cit. on p. 94).
- [ALL⁺21] Scott Aaronson, Jiahui Liu, Qipeng Liu, Mark Zhandry, and Ruizhe Zhang. “New Approaches for Quantum Copy-Protection”. In: *Advances in Cryptology – CRYPTO 2021*. 2021, pp. 526–555. DOI: [10.1007/978-3-030-84242-0_19](https://doi.org/10.1007/978-3-030-84242-0_19) (cit. on pp. 13, 86).
- [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](https://doi.org/10.1007/JHEP02(2013)062) (cit. on pp. 15, 113).

- [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](https://doi.org/10.1007/978-3-031-15802-5_8) (cit. on pp. 4, 12, 13, 109).
- [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, 24:1–24:21. DOI: [10.4230/LIPIcs.ITCS.2023.24](https://doi.org/10.4230/LIPIcs.ITCS.2023.24) (cit. on pp. 12, 92, 98, 114, 115).
- [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](https://doi.org/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](https://doi.org/10.1109/TIT.2016.2516006) (cit. on p. 105).
- [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](https://doi.org/10.1007/BF01200056) (cit. on p. 34).
- [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, 63:1–63:2. DOI: [10.4230/LIPIcs.ITCS.2020.63](https://doi.org/10.4230/LIPIcs.ITCS.2020.63) (cit. on p. 15).
- [Bha13] Rajendra Bhatia. *Matrix Analysis*. Vol. 169. Springer New York, 2013. DOI: [10.1007/978-1-4612-0653-8](https://doi.org/10.1007/978-1-4612-0653-8) (cit. on p. 56).
- [BL20] Anne Broadbent and Sébastien Lord. “Uncloneable Quantum Encryption via Oracles”. en. In: 2020. DOI: [10.4230/LIPIcs.TQC.2020.4](https://doi.org/10.4230/LIPIcs.TQC.2020.4) (cit. on p. 94).
- [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](https://doi.org/10.1145/3406325.3451109) (cit. on p. 17).
- [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](https://doi.org/10.1007/978-3-031-38554-4_2) (cit. on pp. 4, 15, 114, 115).
- [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](https://doi.org/10.1103/PhysRevD.93.086006) (cit. on p. 15).
- [BS19] Zvika Brakerski and Omri Shmueli. “(Pseudo) Random Quantum States with Binary Phase”. In: *Theory of Cryptography*. 2019, pp. 229–250. DOI: [10.1007/978-3-030-36030-6_10](https://doi.org/10.1007/978-3-030-36030-6_10) (cit. on p. 88).
- [CLLZ21] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. “Hidden Cosets and Applications to Unclonable Cryptography”. In: *Advances in Cryptology – CRYPTO 2021*. 2021, pp. 556–584. DOI: [10.1007/978-3-030-84242-0_20](https://doi.org/10.1007/978-3-030-84242-0_20) (cit. on pp. 13, 86, 88, 94).

- [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](https://doi.org/10.1007/3-540-44987-6_5) (cit. on p. 82).
- [CMP20] Andrea Coladangelo, Christian Majenz, and Alexander Poremba. *Quantum copy-protection of compute-and-compare programs in the quantum random oracle model*. 2020. arXiv: [2009.13865](https://arxiv.org/abs/2009.13865) (cit. on p. 94).
- [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](https://doi.org/10.1007/s00220-014-1990-4) (cit. on p. 105).
- [Dup10] Frédéric Dupuis. *The decoupling approach to quantum information theory*. 2010. arXiv: [1004.1641](https://arxiv.org/abs/1004.1641) (cit. on pp. 15, 103, 105).
- [FF93] Joan Feigenbaum and Lance Fortnow. “Random-Self-Reducibility of Complete Sets”. In: *SIAM Journal on Computing* 22.5 (1993), pp. 994–1005. DOI: [10.1137/0222061](https://doi.org/10.1137/0222061) (cit. on pp. 11, 78).
- [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](https://doi.org/10.1145/3564246.3585198) (cit. on pp. 12, 82).
- [GMN22] François Le Gall, Masayuki Miyamoto, and Harumichi Nishimura. *Distributed Merlin-Arthur Synthesis of Quantum States and Its Applications*. 2022. arXiv: [2210.01389](https://arxiv.org/abs/2210.01389) (cit. on p. 34).
- [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](https://doi.org/10.1145/276698.276852) (cit. on p. 36).
- [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](https://doi.org/10.1145/1993636.1993651) (cit. on pp. 13, 91).
- [Hai09] Iftach Haitner. “A Parallel Repetition Theorem for Any Interactive Argument”. In: *2009 50th Annual IEEE Symposium on Foundations of Computer Science*. 2009, pp. 241–250. DOI: [10.1109/FOCS.2009.50](https://doi.org/10.1109/FOCS.2009.50) (cit. on p. 10).
- [Har13] Aram W. Harrow. *The Church of the Symmetric Subspace*. 2013. arXiv: [1308.6595](https://arxiv.org/abs/1308.6595) (cit. on p. 111).
- [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](https://doi.org/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](https://doi.org/10.1007/JHEP06(2013)085) (cit. on pp. 4, 15, 113, 114).
- [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](https://doi.org/10.1142/S1230161208000043) (cit. on pp. 4, 105).

- [HILL99] Johan Håstad, Russell Impagliazzo, Leonid A. Levin, and Michael Luby. “A Pseudorandom Generator from any One-way Function”. In: *SIAM J. Comput.* 28.4 (1999), pp. 1364–1396. DOI: [10.1137/S0097539793244708](https://doi.org/10.1137/S0097539793244708) (cit. on p. 112).
- [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](https://doi.org/10.1038/s41567-020-0932-7) (cit. on p. 17).
- [HMS23] Iftach Haitner, Noam Mazon, and Jad Silbak. “Incompressibility and Next-Block Pseudentropy”. In: *14th Innovations in Theoretical Computer Science Conference, ITCS 2023, January 10-13, 2023, MIT, Cambridge, Massachusetts, USA*. Vol. 251. 2023, pp. 66:1–66:18. DOI: [10.4230/LIPIcs.ITCS.2023.66](https://doi.org/10.4230/LIPIcs.ITCS.2023.66) (cit. on p. 112).
- [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](https://doi.org/10.1007/978-3-031-30545-0_22) (cit. on pp. 12, 82, 83).
- [HPWP10] Johan Håstad, Rafael Pass, Douglas Wikström, and Krzysztof Pietrzak. “An Efficient Parallel Repetition Theorem”. In: *Theory of Cryptography*. 2010, pp. 1–18. DOI: [10.1007/978-3-642-11799-2_1](https://doi.org/10.1007/978-3-642-11799-2_1) (cit. on p. 10).
- [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](https://doi.org/10.1109/SFCS.1989.63483) (cit. on pp. 17, 112).
- [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](https://doi.org/10.1109/SCT.1995.514853) (cit. on p. 17).
- [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](https://doi.org/10.1145/2049697.2049704) (cit. on pp. 4, 10).
- [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](https://doi.org/10.1007/978-3-319-96878-0_5) (cit. on pp. 15, 16, 87, 88, 92, 109).
- [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](https://doi.org/10.1145/3485628) (cit. on p. 34).
- [KA04] Elham Kashefi and Carolina Moura Alves. *On the Complexity of Quantum Languages*. 2004. arXiv: [quant-ph/0404062](https://arxiv.org/abs/quant-ph/0404062) (cit. on p. 5).
- [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](https://doi.org/10.1038/s41534-017-0013-7) (cit. on p. 71).
- [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](https://doi.org/10.1145/3564246.3585225) (cit. on pp. 4, 5, 12, 13, 109).

- [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, 2:1–2:20. DOI: [10.4230/LIPIcs.TQC.2021.2](https://doi.org/10.4230/LIPIcs.TQC.2021.2) (cit. on pp. 4, 5, 12, 13, 109).
- [KRS09] Robert König, 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](https://doi.org/10.1109/TIT.2009.2025545) (cit. on p. 103).
- [KT23] Dakshita Khurana and Kabir Tomer. *Commitments from Quantum One-Wayness*. 2023. arXiv: [2310.11526](https://arxiv.org/abs/2310.11526) (cit. on pp. 13, 87, 94).
- [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](https://doi.org/10.1145/335305.335387) (cit. on pp. 4, 8).
- [KW20] Sumeet Khatri and Mark M. Wilde. *Principles of Quantum Communication Theory: A Modern Approach*. 2020. arXiv: [2011.04672](https://arxiv.org/abs/2011.04672) (cit. on p. 13).
- [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](https://doi.org/10.1016/S0167-2789(98)00053-0) (cit. on pp. 4, 11, 82).
- [Lip94] Richard J. Lipton. “A new approach to information theory”. In: *STACS 94*. 1994, pp. 699–708. DOI: [10.1007/3-540-57785-8_183](https://doi.org/10.1007/3-540-57785-8_183) (cit. on p. 112).
- [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](https://doi.org/10.1038/nphys3029) (cit. on pp. 10, 71, 72).
- [LMW23] Alex Lombardi, Fermi Ma, and John Wright. *A one-query lower bound for unitary synthesis and breaking quantum cryptography*. 2023. arXiv: [2310.08870](https://arxiv.org/abs/2310.08870) (cit. on pp. 4–6, 13, 17).
- [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](https://doi.org/10.1109/FOCS46700.2020.00118) (cit. on p. 17).
- [May19] Alex May. “Quantum tasks in holography”. In: *Journal of High Energy Physics* 2019.10 (2019), p. 233. DOI: [10.1007/JHEP10\(2019\)233](https://doi.org/10.1007/JHEP10(2019)233) (cit. on p. 119).
- [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](https://doi.org/10.1103/PhysRevLett.78.3414) (cit. on pp. 4, 11, 82).
- [MY22a] Tomoyuki Morimae and Takashi Yamakawa. *One-Wayness in Quantum Cryptography*. 2022. arXiv: [2210.03394](https://arxiv.org/abs/2210.03394) (cit. on pp. 12, 87, 94).
- [MY22b] 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](https://doi.org/10.1007/978-3-031-15802-5_10) (cit. on pp. 4, 12, 13, 16, 81, 87, 94, 111).

- [MY23] Tony Metger and Henry Yuen. $\text{stateQIP} = \text{statePSPACE}$. 2023. arXiv: [2301.07730](https://arxiv.org/abs/2301.07730) (cit. on pp. [7](#), [10](#), [11](#), [37–39](#), [63](#), [69](#), [70](#), [75–77](#), [93](#)).
- [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](https://doi.org/10.1007/978-3-540-45146-4_6) (cit. on pp. [12](#), [13](#), [91](#)).
- [NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. DOI: [10.1017/CB09780511976667](https://doi.org/10.1017/CB09780511976667) (cit. on p. [20](#)).
- [Oka96] Tatsuoaki 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](https://doi.org/10.1145/237814.238016) (cit. on p. [36](#)).
- [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](https://doi.org/10.1007/3-540-63165-8_160) (cit. on p. [16](#)).
- [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](https://doi.org/10.1142/9789814536752) (cit. on p. [15](#)).
- [Raz98] Ran Raz. “A Parallel Repetition Theorem”. In: *SIAM Journal on Computing* 27.3 (1998), pp. 763–803. DOI: [10.1137/S0097539795280895](https://doi.org/10.1137/S0097539795280895) (cit. on p. [10](#)).
- [Ren22] Joseph M. Renes. “Quantum Information Theory. Concepts and Methods”. In: 2022. DOI: [10.1515/9783110570250](https://doi.org/10.1515/9783110570250) (cit. on pp. [13](#), [95](#)).
- [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, 112:1–112:4. DOI: [10.4230/LIPIcs.ITCS.2022.112](https://doi.org/10.4230/LIPIcs.ITCS.2022.112) (cit. on pp. [5](#), [7](#), [10](#), [11](#), [20](#), [33](#), [63](#), [71](#), [76](#)).
- [Sch95] Benjamin Schumacher. “Quantum coding”. In: *Physical Review A* 51 (4 1995), pp. 2738–2747. DOI: [10.1103/PhysRevA.51.2738](https://doi.org/10.1103/PhysRevA.51.2738) (cit. on pp. [15](#), [107](#)).
- [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](https://doi.org/10.1002/j.1538-7305.1948.tb01338.x) (cit. on p. [15](#)).
- [Shi03] Yaoyun Shi. “Both Toffoli and Controlled-NOT Need Little Help to Do Universal Quantum Computing”. In: *Quantum Information & Computation* 3.1 (2003), pp. 84–92. URL: <https://dl.acm.org/doi/10.5555/2011508.2011515> (cit. on p. [94](#)).
- [Sus16] Leonard Susskind. “Computational complexity and black hole horizons”. In: *Fortschritte der Physik* 64.1 (2016), pp. 24–43. DOI: [10.1002/prop.201500092](https://doi.org/10.1002/prop.201500092) (cit. on p. [15](#)).
- [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](https://doi.org/10.1145/636865.636868) (cit. on p. [62](#)).
- [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](https://doi.org/10.1109/TIT.2009.2032797) (cit. on p. [107](#)).

- [Tom13] Marco Tomamichel. *A Framework for Non-Asymptotic Quantum Information Theory*. 2013. arXiv: [1203.2142](#) (cit. on pp. [15](#), [102–104](#)).
- [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 p. [4](#)).
- [VW16] Thomas Vidick and John Watrous. “Quantum Proofs”. In: *Foundations and Trends® in Theoretical Computer Science* 11.1-2 (2016), pp. 1–215. DOI: [10.1561/04000000068](#) (cit. on p. [31](#)).
- [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](#), [34](#)).
- [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. [9](#), [34](#), [36](#), [63](#)).
- [Wie83] Stephen Wiesner. “Conjugate Coding”. In: *SIGACT News* 15.1 (1983), pp. 78–88. DOI: [10.1145/1008908.1008920](#) (cit. on pp. [13](#), [86](#), [87](#)).
- [Wil13] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013. DOI: [10.1017/CB09781139525343](#) (cit. on pp. [13](#), [19](#), [39](#), [42](#)).
- [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. [106](#)).
- [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](#), [12](#), [81–83](#)).
- [Yao82] Andrew Chi-Chih Yao. “Theory and application of trapdoor functions”. In: *23rd Annual Symposium on Foundations of Computer Science*. 1982, pp. 80–91. DOI: [10.1109/SFCS.1982.45](#) (cit. on p. [112](#)).
- [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. [15](#)).
- [Zha21] Mark Zhandry. “Quantum Lightning Never Strikes the Same State Twice. Or: Quantum Money from Cryptographic Assumptions”. In: *Journal of Cryptology* 34.1 (2021), p. 6. DOI: [10.1007/s00145-020-09372-x](#) (cit. on p. [88](#)).