Local transformations of bipartite entanglement are rigid

John Bostanci[1], Tony Metger[2], and Henry Yuen[1]

[1]Columbia University
[2]ETH Zurich

Abstract

Uhlmann's theorem is a fundamental result in quantum information theory that quantifies the optimal overlap between two bipartite pure states after applying local unitary operations (called *Uhlmann transformations*). We show that optimal Uhlmann transformations are *rigid* – in other words, they must be unique up to some well-characterized degrees of freedom. This rigidity is also *robust*: Uhlmann transformations achieving near-optimal overlaps must be close to the unique optimal transformation (again, up to well-characterized degrees of freedom). We describe two applications of our robust rigidity theorem: (a) we obtain better interactive proofs for synthesizing Uhlmann transformations and (b) we obtain a simple, alternative proof of the Gowers-Hatami theorem on the stability of approximate representations of finite groups.

1 Introduction

Let $|C\rangle, |D\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ denote bipartite pure states; let A denote the first subsystem and B denote the second subsystem. What is the closest that one can get to $|D\rangle$ by performing a unitary on subsystem B of the state $|C\rangle$? Uhlmann's theorem [Uhl76] quantifies the optimal overlap achievable:

$$\mathrm{F}(\rho, \sigma) = \max_U |\langle D| \mathbb{1} \otimes U |C\rangle|, \tag{1}$$

where ρ and σ denote the reduced density matrices on subsystem A of $|C\rangle$ and $|D\rangle$ respectively, the function $\mathrm{F}(\rho, \sigma) = \mathrm{Tr}(\sqrt{\rho^{1/2}\sigma\rho^{1/2}})$ denotes the fidelity between the two states, and the maximization is over all unitary transformations acting on subsystem B. We call a unitary U achieving equality in Equation (1) an *Uhlmann transformation*.

Given the ubiquity of Uhlmann's theorem throughout quantum information science, it seems worthwhile to study the mathematical and computational properties of Uhlmann transforms. Many natural questions arise: how unique are Uhlmann transformations? How robust are they to perturbations of the underlying states $|C\rangle, |D\rangle$? What is the complexity of performing Uhlmann transformations on a quantum computer? Can difficult Uhlmann transformations be used for cryptography? The latter two questions were recently studied by Metger and Yuen [MY23] and Bostanci, et al. [BEM+23], who investigate a theory of state and unitary complexity, respectively.

This paper studies the first two questions concerning the uniqueness and robustness of Uhlmann transformations. At first glance, Uhlmann transformations are not generally unique. For example, suppose that the reduced density matrix of $|C\rangle$ on subsystem B does not have full support. Then any Uhlmann transformation can behave arbitrarily on the orthogonal complement of the support,

while remaining optimal. What if we disregard these trivial degrees of freedom, however – could Uhlmann transformations be unique in some other meaningful way?

We provide an answer via *canonical Uhlmann transformations*, first defined by Metger and Yuen [MY23]. For every pair of bipartite states $(|C\rangle, |D\rangle)$, this is the operator

$$W := \mathrm{sgn}(\mathrm{Tr}_{\mathsf{A}}(|D\rangle\langle C|)) \tag{2}$$

where Tr_{A} denotes tracing out register A and $\mathrm{sgn}(\cdot)$ denotes the following function: for a matrix X with singular value decomposition $X = U\Sigma V^*$, we define $\mathrm{sgn}(X) := U\mathrm{sgn}(\Sigma)V^*$ where U, V are unitary operators and $\mathrm{sgn}(\Sigma)$ denotes the projection onto the eigenvectors of Σ with positive eigenvalues (i.e., the support of Σ). The canonical transformation W is a partial isometry[1]; it is unitary if and only if both reduced states ρ, σ (of $|C\rangle, |D\rangle$, respectively) are invertible.

The following was proven by Bostanci, et al. [BEM+23, Proposition 6.3] in their investigation of the computational complexity of implementing Uhlmann transformations:

Lemma 1.1. *The canonical Uhlmann transformation W satisfies $|\langle D| \mathbb{1} \otimes W |C\rangle| = \mathrm{F}(\rho, \sigma)$, and furthermore for all partial isometries R such that $|\langle D| \mathbb{1} \otimes R |C\rangle| = \mathrm{F}(\rho, \sigma)$, we have that $W^*W \leq R^*R$ in the positive semidefinite ordering.*

In other words, the canonical Uhlmann transformation defined in Equation (2) achieves the optimal overlap between $|C\rangle$ and $|D\rangle$, and furthermore any other partial isometry achieving the optimal overlap must be supported on the domain of W. This is a rather weak statement, however: when R is unitary, then $W^*W \leq R^*R = \mathbb{1}$ is satisfied for *all* partial isometries W.

A stronger statement is the following:

Claim 1.2. *For all partial isometries R such that $\langle D| \mathbb{1} \otimes R |C\rangle = \mathrm{F}(\rho, \sigma)$, we have that*

$$\mathbb{1} \otimes W |C\rangle = \mathbb{1} \otimes RW^*W |C\rangle \ .$$

This says that *any* optimal Uhlmann transformation, when restricted to the support of W, must behave identically to W on the state $|C\rangle$. This provides some justification in calling the W in Equation (2) the "canonical" Uhlmann transformation corresponding to $|C\rangle, |D\rangle$.

Claim 1.2 is in fact a special case of a more general *robust rigidity* theorem that we prove in this paper. Roughly speaking, the theorem (Theorem 1.6 below) states that any transformation R that achieves *approximately*-optimal fidelity (meaning that $|\langle D| \mathbb{1} \otimes R |C\rangle| \geq \mathrm{F}(\rho, \sigma) - \epsilon$) must be *approximately* the canonical Uhlmann transformation W. This is analogous to rigidity results for some quantum information processing tasks such as nonlocal games [MY03, MYS12, ŠB20] and superdense coding [NY23]. These results show that the only way for a quantum operation to achieve near-optimal performance according to some metric (e.g., winning probability in a nonlocal game, or decoding probability in superdense coding) is if, in fact, it is close to a canonical strategy or protocol.

First we give a way to quantify the rigidity of canonical Uhlmann transformations.

Definition 1.3. *Let $|C\rangle, |D\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ be pure bipartite states with respective reduced density matrices ρ, σ on the subsystem A. Then we say the corresponding canonical Uhlmann transformation W defined in Equation (2) has $\delta(\epsilon)$-*robust rigidity *if, for all $\epsilon > 0$, for all unitaries R such that*

$$\langle D| \mathbb{1} \otimes R |C\rangle \geq \mathrm{F}(\rho, \sigma) - \epsilon \ ,$$

[1] A partial isometry can be thought of as the restriction of a unitary to a subspace. More formally, an operator W is a partial isometry if W^*W is a projection.

we have

$$\|\mathbb{1} \otimes (W - R)W^* W \left|C\right\rangle\|^2 \leq \delta(\epsilon) \ .$$

Thus, bounds on the function $\delta(\epsilon)$ of an Uhlmann transformation quantifies the extent to which the exact rigidity statement of Claim 1.2 can be made robust.

Remark 1.4. The reader may notice an apparent asymmetry between $|C\rangle$ and $|D\rangle$ in Claim 1.2 and Definition 1.3. This is motivated by an operational interpretation of Uhlmann's theorem: starting with $|C\rangle$, how close can we get to $|D\rangle$ by acting on subsystem B? The choice of starting with $|C\rangle$ versus $|D\rangle$ is significant, as the canonical Uhlmann transformation can have different robustness functions depending on this choice (see Section 4.2 for an example).

Remark 1.5. The reader may also wonder about the role of W^*W in Definition 1.3, which is the projection onto the image of W. The image of W may not be fully contained in the support of subsystem B of $|C\rangle$ or $|D\rangle$. Interestingly, this projection is necessary in the statement of rigidity: *any* unitary completion of the partial isometry W achieves the optimal fidelity, as shown in Claim 3.3. In other words, it is possible to behave arbitrarily outside the image of W, and still attain the optimal fidelity.

Our main result is a general bound on the rigidity of Uhlmann transformations.

Theorem 1.6 (Robust rigidity of Uhlmann transformations)**.** *Let $|C\rangle, |D\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ be pure bipartite states with respective reduced density matrices ρ, σ on the subsystem A. The corresponding canonical Uhlmann transformation W satisfies the following:*

1. *(**Completeness**). For all unitary completions U of W, we have*

$$|\left\langle D\right| \mathbb{1} \otimes U \left|C\right\rangle| = \mathrm{F}(\rho, \sigma) \ .$$

2. *(**Rigidity**). W has $\delta(\epsilon)$-robust rigidity for $\delta(\epsilon) = \left(\frac{2\kappa}{\eta}\right)\epsilon$ where $\kappa = \|\rho^{-1/2} P \rho^{1/2}\|_\infty^2$ with P being the projection onto $\mathrm{Image}(\rho^{1/2}\sigma\rho^{1/2})$, and η is the smallest nonzero eigenvalue of the matrix geometric mean $\rho^{-1}\#\sigma$.*

For readers who are not familiar with the (beautiful notion of the) matrix geometric mean we provide a brief introduction in Section 1.1.

Thus, the canonical Uhlmann transformation is indeed robustly rigid, up to some blow-up that depends on two parameters η and κ (called the *spectral gap* and *obliqueness*, respectively) of the reduced density matrices ρ, σ. Intuitively, the obliqueness parameter κ is a measure of a combination of non-commutativity and non-invertibility of ρ, σ and the spectral gap parameter η is a measure of how "well-conditioned" the matrix geometric mean $\rho^{-1}\#\sigma$ is (which one can think of as a notion of "ratio" between σ and ρ).

Remark 1.7. Suppose either

1. The density matrices ρ, σ commute, or
2. The density matrices ρ, σ are invertible.

Then the obliqueness parameter κ is equal to 1, and the robustness bound only depends on the spectral gap η of $\rho^{-1}\#\sigma$.

In Sections 4.2 and 4.4 respectively we further show that some dependence on the spectral gap parameter η and the obliqueness parameter κ in Theorem 1.6 is necessary.

1.1 Matrix geometric mean

The matrix geometric mean is a noncommutative generalization of the geometric mean $\sqrt{ab}$ of two nonnegative numbers a, b. If A, B are commuting positive semidefinite matrices, then the matrix geometric mean $A\#B$ is defined as $A^{1/2}B^{1/2}$. For general positive definite (i.e., all eigenvalues are strictly positive) matrices A, B, the matrix geometric mean $A\#B$ is defined as

$$A\#B := A^{1/2}(A^{-1/2}BA^{-1/2})^{1/2}A^{1/2} \ . \tag{3}$$

For positive definite matrices A, B the matrix geometric mean enjoys many pleasant properties, including

1. $A\#B$ is positive definite.
2. $A\#B = B\#A$.
3. $A\#B$ is the unique positive solution to the equation $XA^{-1}X = B$.
4. If X is invertible, then $X(A\#B)X^{-1} = (XAX^{-1})\#(XBX^{-1})$.
5. $A\#B \leq \frac{1}{2}(A + B)$, a noncommutative analogue of the arithmetic-geometric mean inequality.
6. $\Phi(A)\#\Phi(B) \leq \Phi(A\#B)$ for all positive maps Φ.

Proofs of these properties can be found in [Bha09, Chapter 4]. For more applications of the matrix geometric mean in quantum information theory, see [CS20, FF21, LWWZ24].

For noninvertible A, B (but still positive *semi*definite), the matrix geometric mean $A\#B$ is typically defined as a limit of geometric means of sequences of strictly positive matrices converging to A, B; however, in this case not all of the properties listed above are satisfied. For example, the symmetry property $A\#B = B\#A$ need not hold.

In this paper we do not use this limit definition, and instead stick to Equation (3) as the definition for the matrix geometric mean for *all* positive semidefinite matrices A, B, with the inverses now being Moore-Penrose pseudoinverses. Although it does not satisfy all the properties listed above, it satisfies a few important properties that are needed for the proof of Theorem 1.6; for example, as we will show in Claim 3.1, when the density matrices ρ, σ are real, the canonical Uhlmann transformation can equivalently be expressed in terms of a matrix geometric mean:

$$W = Y^*(\rho^{1/2}\sigma^{1/2})^{-1}\rho^{1/2}(\rho^{-1}\#\sigma)\rho^{1/2}X$$

for some unitary operators X, Y (see the start of Section 3 for their definitions). Furthermore, the fidelity between ρ and σ can also be written as $\mathrm{F}(\rho, \sigma) = \mathrm{Tr}((\rho^{-1}\#\sigma)\rho)$ (see e.g. [CS20]).

1.2 Applications

Given the centrality of Uhlmann transformations, the rigidity statement in Theorem 1.6 may be of interest in its own right, but it also turns out to be a useful technical tool for other applications. To illustrate this, we briefly discuss applications of our robust rigidity theorem to unitary complexity theory and approximate representation theory.

The complexity of the Uhlmann Transformation Problem. Bostanci, et al. [BEM+23] defined the Uhlmann Transformation Problem, a computational task associated to implementing canonical Uhlmann transformations corresponding to a pair $(|C\rangle, |D\rangle)$ whose circuit descriptions are given. They introduced a framework for unitary complexity theory in order to properly describe the complexity of performing Uhlmann transformations: for the special case that the pair $(|C\rangle, |D\rangle)$ have identical reduced density matrices (i.e., $\mathrm{F}(\rho, \sigma) = 1$), the Uhlmann Transformation Problem is complete for $\mathsf{avgUnitaryHVPZK}$, a unitary complexity class that captures *perfect zero knowledge* in the unitary synthesis setting [BEM+23, Theorem 6.1]. They left open the challenge of characterizing the complexity of canonical Uhlmann transformations for general values of $\mathrm{F}(\rho, \sigma)$.

In Section 5.1 we present a simple 2-round quantum interactive synthesis protocol for the Uhlmann Transformation Problem (for all values of the fidelity of the reduced density matrices) – this improves upon the 8-round protocol that arises from the machinery of proving $\mathsf{avgUnitaryPSPACE} = \mathsf{avgUnitaryQIP}$ in [BEM+23]. The soundness of our 2-round protocol crucially depends on the robust Uhlmann rigidity theorem. We believe that this could be helpful for better understanding the complexity of the Uhlmann Transformation Problem in the future.

Approximate representation theory. In the mathematics literature, results such as Theorem 1.6 are known as *stability* results: if an object A approximately satisfies some constraints, then is it close (in the appropriate metric) to an object B that *exactly* satisfies those constraints [Ula60]? In Section 5.2, we show that our robust Uhlmann rigidity theorem is powerful enough to derive other stability results – in particular, we show that the Gowers-Hatami theorem on the stability of approximate representations of finite groups [GH15] is an easy consequence of Theorem 1.6. Our proof suggests a possible "mechanical template" for proving other kinds of stability results: first, define the appropriate pair of pure states $(|C\rangle, |D\rangle)$, show that the canonical Uhlmann transformation is the ideal, "exact" object, and then use robust Uhlmann rigidity to conclude that all approximate objects are close to the ideal, exact object. We note that our approach of proving the Gowers-Hatami theorem is reminiscent of Metger, Natarajan, Zhang's alternate proof of it [MNZ24].

1.3 Related work

A weaker rigidity theorem. Bostanci, et al. [BEM+23] proved the following rigidity theorem for Uhlmann transformations, where the robustness itself depends on the fidelity between the reduced states:

Theorem 1.8 (Weak Uhlmann rigidity)**.** *Let $|C\rangle, |D\rangle$ be pure bipartite states with reduced density matrices ρ, σ on the first subsystem. Then for all unitaries R such that*

$$\langle D| \mathbb{1} \otimes R |C\rangle \geq \mathrm{F}(\rho, \sigma) - \epsilon \ ,$$

we have that

$$\|\mathbb{1} \otimes (W - R) |C\rangle\|^2 \leq 8\Big(1 - \mathrm{F}(\rho, \sigma) + \sqrt{\epsilon}\Big)$$

where W is the corresponding canonical Uhlmann transformation.

Remark 1.9. Technically, the theorem is stated in greater generality in [BEM+23] for arbitrary channels rather than unitaries; we specialize the theorem statement for this paper.

Suppose the fidelity $\mathrm{F}(\rho, \sigma)$ is equal to 1. In our language, Theorem 1.8 implies that the canonical Uhlmann transformation W has robust rigidity $\delta(\epsilon) \leq 8\sqrt{\epsilon}$. (At first glance, it may seem rather nice that there is no dependence on the spectral gap η or the obliqueness parameter κ, but note that in this special case of $\mathrm{F}(\rho, \sigma) = 1$, the two density matrices are identical and therefore $\eta = \kappa = 1$.) Thus Theorem 1.8 implies a robust rigidity bound for the perfect fidelity setting.[2]

However, when $\mathrm{F}(\rho, \sigma)$ is strictly less than 1, then the rigidity bound of Theorem 1.8 becomes trivial as $\epsilon \to 0$; the upper bound on the closeness of R and W is always at least $8(1 - \mathrm{F}(\rho, \sigma))$, a quantity that is a constant compared to ϵ. Furthermore this gives trivial upper bounds whenever $\mathrm{F}(\rho, \sigma) \leq 7/8$.

Our main theorem (Theorem 1.6), on the other hand, gives a nontrivial rigidity bound no matter what $\mathrm{F}(\rho, \sigma)$ is.

Rigidity in quantum information theory. This paper is inspired by rigidity in nonlocal games (also known as *self-testing* in the nonlocal game literature), which is the phenomenon that for many nonlocal games of interest (such as the CHSH game or the Magic Square game), near-optimal strategies must be close to a canonical optimal strategy [MY03, MYS12, MS12]. There is also a long line of work studying various aspects of rigidity in nonlocal games; we refer the reader to the extensive survey of [ŠB20]. Nonlocal game rigidity is a powerful tool in quantum cryptography and quantum complexity theory, with applications ranging from classical verification of quantum computations [RUV13] to settling the complexity of quantum multiprover interactive proofs [JNV+21].

Stability of polar decompositions. The rigidity of Uhlmann transformations is loosely related to the *stability of polar decompositions*, a topic that has been studied extensively in numerical analysis [Hig86]. Every square matrix A admits a polar decomposition $A = UP$ where U (the "polar factor" of A) is a partial isometry and P is a positive semidefinite matrix. How do the polar factors of a matrix A and a perturbation $A + \Delta A$ compare with each other, as a function of A and the perturbation ΔA? This is a central question to the study of numerical algorithms for computing the polar decomposition.

The connection with the Uhlmann transformation is as follows. The canonical Uhlmann transformation W for a pair $(|C\rangle, |D\rangle)$ of states with corresponding density matrices ρ, σ can be derived from the polar decomposition of the matrix $A = \sqrt{\rho}\sqrt{\sigma}$. Perturbing the states ρ, σ (and consequently the states $|C\rangle, |D\rangle$) will perturb the canonical Uhlmann transformation W; this relationship is governed by the stability of the polar decomposition of A.[3]

However, the robust rigidity of Uhlmann transformations studied in this paper is a different notion of stability. Here, we do not consider perturbations of the states $|C\rangle, |D\rangle$; we are asking whether all *approximate* Uhlmann transformations R for a pair of states $(|C\rangle, |D\rangle)$ must be close to a unique *exact* Uhlmann transformation.

1.4 Summary

Uhlmann transformations, which are local transformations of bipartite (pure state) entanglement, are fundamental in quantum information theory. In this paper we showed that Uhlmann transfor-

[2] We note that in the $\mathrm{F}(\rho, \sigma) = 1$ case Theorem 1.6 implies a quadratically-better robustness function $\delta(\epsilon) = 2\epsilon$.

[3] See Section 4 for an illustration of how the canonical Uhlmann transformation is a sensitive function of the states $|C\rangle, |D\rangle$.

mations possess a robust form of *rigidity*: near-optimal entanglement transformations must close (in a well-defined sense) to a unique optimal transformation. This unique optimal transformation is the canonical Uhlmann transformation introduced by [MY23], and our result gives further justification to calling it "canonical."

We showed that the robustness of the rigidity theorem inherently depends on two parameters called the spectral gap and obliqueness, which are functions of the underlying pure states $|C\rangle, |D\rangle$. An interesting open question is whether there is a general "rounding" procedure that converts any pair of states $(|C\rangle, |D\rangle)$ into a nearby pair $(|\tilde{C}\rangle, |\tilde{D}\rangle)$ with controlled spectral gap and controlled obliqueness. In Section 4.3, we provide a rounding lemma that only controls the spectral gap.

Finally, we presented two applications of our robust rigidity theorem. The first is to unitary complexity theory, where we can improve the round complexity required for the task of synthesizing canonical Uhlmann transformations in the regime where the fidelity between the reduced states is not 1. Second, we demonstrate that the robust rigidity theorem is a very general form of robustness that can be used to derive other stability theorems. As an example, we re-derive the stability of approximate group representations by reducing to the robust rigidity of the canonical Uhlmann transformation between a specific pair of states. Given the ubiquity of Uhlmann transformations in protocols across quantum information theory and quantum complexity theory, developing an understanding of their rigidity properties should unlock further applications and deeper insight into the ways that bipartite entanglement can be locally transformed.

2 Notation and facts about states and matrices

For a square matrix A,

1. A^{-1} denotes its Moore-Penrose pseudoinverse,
2. A^* denotes its conjugate transpose,
3. $\overline{A}$ denotes its entrywise complex conjugate (with respect to the standard basis),
4. $A^\top$ denotes its transpose (with respect to the standard basis).
5. $\mathrm{Image}(A)$ denotes its image, i.e., $\mathrm{span}\{A|v\rangle\}$,
6. $\mathrm{Dom}(A)$ denotes its domain, i.e., the orthogonal complement of the kernel of A,
7. $\|A\|_1$ denotes its Schatten-1 norm, i.e., $\mathrm{Tr}(\sqrt{A^*A})$,
8. $\|A\|_\infty$ denotes its operator norm, i.e., its largest singular value.

Note that $\mathrm{Image}(A^*A) = \mathrm{Dom}(A) = \mathrm{Image}(A^*)$.

Throughout we let $|\Omega\rangle = \sum_{i=1}^d |i\rangle \otimes |i\rangle$ denote the unnormalized maximally entangled state on $\mathbb{C}^d \otimes \mathbb{C}^d$. We recall the well-known "reflection" property of maximally entangled states:

Claim 2.1. *For all operators A acting on $\mathbb{C}^d$, we have*

$$A \otimes \mathbb{1} |\Omega\rangle = \mathbb{1} \otimes A^\top |\Omega\rangle \ .$$

Next we express every bipartite pure state in terms of the maximally entangled state.

Claim 2.2. *Every pure bipartite state $|C\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ whose reduced density matrix on the first register is ρ can be written as*

$$|C\rangle = \sqrt{\rho} \otimes X \, |\Omega\rangle$$

for some unitary operator X.

Proof. Let $|C\rangle = \sum_{i=1}^d \lambda_i \, |a_i\rangle \otimes |b_i\rangle$ denote a Schmidt decomposition of $|C\rangle$, so the reduced state is $\rho = \sum_i \lambda_i^2 \, |a_i\rangle\langle a_i|$. Let $X = \sum_{i=1}^d |b_i\rangle\langle \overline{a_i}|$ where $|\overline{a_i}\rangle$ denotes the complex conjugate of $|a_i\rangle$. The claim follows since the unnormalized maximally entangled state $|\Omega\rangle$ can be equivalently expressed as

$$|\Omega\rangle = \sum_{i=1}^d |a_i\rangle \otimes |\overline{a_i}\rangle \ .$$

□

Lemma 2.3 (Schur complement lemma)**.** *Let M be the following block matrix:*

$$M = \begin{pmatrix} A & B \\ B^* & C \end{pmatrix} \ .$$

Then M is positive semidefinite if and only if $A \geq 0$ and $(\mathbb{1} - AA^{-1})B = 0$ and $C \geq B^* A^{-1} B$.

Proofs of this can be found in, e.g., [BV04, Appendix A.5.5] and [Bha09, Chapter 1].

2.1 Semidefinite programming

A *semidefinite program (SDP) in standard form* is specified by self-adjoint matrices $B \in \mathbb{C}^{m \times m}, C^{n \times n}$, and a Hermiticity-preserving[4] superoperator Φ mapping operators on $\mathbb{C}^n$ to operators on $\mathbb{C}^m$, and corresponds to the following optimization problem:

$$\begin{aligned} \underset{X}{\text{maximize}} \quad & \mathrm{Tr}(CX) \\ \text{subject to} \quad & \Phi(X) = B \\ & X \geq 0 \end{aligned}$$

where X ranges over all positive semidefinite operators on $\mathbb{C}^n$.

The *dual SDP* of the standard-form program above is

$$\begin{aligned} \text{minimize} \quad & \mathrm{Tr}(BY) \\ \text{subject to} \quad & \Phi^*(Y) \geq C \\ & Y \text{ Hermitian} \end{aligned}$$

where Φ^* denotes the *adjoint* of the superoperator Φ (meaning that Φ^* is the unique superoperator satisfying $\langle Y, \Phi(X)\rangle = \langle \Phi^*(Y), X\rangle$ for all operators $X \in \mathbb{C}^{n \times n}, Y \in \mathbb{C}^{m \times m}$).

Weak SDP duality states that the objective value of the dual SDP is always an upper bound on the objective value of the primal SDP. We refer the reader to Watrous's textbook for a detailed treatment of SDPs in the context of quantum information [Wat18].

[4] This means that if X is self-adjoint, then so is $\Phi(X)$.

3 Rigidity of Uhlmann transforms

We now prove the main theorem of the paper, Theorem 1.6, which for convenience we restate here.

Theorem 1.6 (Robust rigidity of Uhlmann transformations)**.** *Let $|C\rangle, |D\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ be pure bipartite states with respective reduced density matrices ρ, σ on the subsystem A. The corresponding canonical Uhlmann transformation W satisfies the following:*

1. *(**Completeness**). For all unitary completions U of W, we have*

$$|\langle D| \mathbb{1} \otimes U |C\rangle| = \mathrm{F}(\rho, \sigma) \ .$$

2. *(**Rigidity**). W has $\delta(\epsilon)$-robust rigidity for $\delta(\epsilon) = \left(\frac{2\kappa}{\eta}\right)\epsilon$ where $\kappa = \|\rho^{-1/2} P \rho^{1/2}\|_\infty^2$ with P being the projection onto $\mathrm{Image}(\rho^{1/2}\sigma\rho^{1/2})$, and η is the smallest nonzero eigenvalue of the matrix geometric mean $\rho^{-1}\#\sigma$.*

Let $|C\rangle, |D\rangle$ be bipartite pure states. For notational convenience, we let ρ, σ denote the entry-wise *complex conjugates* of the reduced density matrices of $|C\rangle, |D\rangle$ on the subsystem A respectively – it is easy to verify that $\mathrm{F}(\overline{\rho}, \overline{\sigma}) = \mathrm{F}(\rho, \sigma)$. Then by Claim 2.2, we can write

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

for some unitary operators X, Y.

For simplicity, we prove Theorem 1.6 for the special case that $X = Y = \mathbb{1}$. This is without loss of generality: if Theorem 1.6 holds for a pair $|C\rangle = \sqrt{\overline{\rho}} \otimes \mathbb{1} |\Omega\rangle, |D\rangle = \sqrt{\overline{\sigma}} \otimes \mathbb{1} |\Omega\rangle$ with canonical Uhlmann transformation W, then it is easy to see that Theorem 1.6 holds also for $|C\rangle = \sqrt{\overline{\rho}} \otimes X |\Omega\rangle, |D\rangle = \sqrt{\overline{\sigma}} \otimes Y |\Omega\rangle$ with canonical Uhlmann transformation $\widetilde{W} = YWX^*$.

Thus, for the rest of this section we assume $X = Y = \mathbb{1}$.

3.1 Properties of the canonical Uhlmann transformation

First, we establish equivalent expressions for the canonical Uhlmann transformation in terms of the reduced density matrices ρ, σ.

Claim 3.1. *When $X = Y = \mathbb{1}$, the following expressions are equivalent definitions of the canonical Uhlmann transformation W for the pair $(|C\rangle, |D\rangle)$:*

- $W = \mathrm{sgn}(\sqrt{\sigma}\sqrt{\rho})$.
- $W = (\rho^{1/2}\sigma^{1/2})^{-1}\rho^{1/2}(\rho^{-1}\#\sigma)\rho^{1/2}$.

Proof. From the reflection property of maximally entangled states, we have

$$|C\rangle = \mathbb{1} \otimes (\sqrt{\overline{\rho}})^\top |\Omega\rangle$$
$$|D\rangle = \mathbb{1} \otimes (\sqrt{\overline{\sigma}})^\top |\Omega\rangle \ .$$

On the other hand, since ρ is positive semidefinite, we have

$$(\sqrt{\overline{\rho}})^\top = \sqrt{\overline{\rho}^\top} = \sqrt{\rho^*} = \sqrt{\rho}$$

and similarly $(\sqrt{\overline{\sigma}})^\top = \sqrt{\sigma}$. Thus, recalling the definition of W from Equation (2), we have

$$\begin{aligned} W &= \mathrm{sgn}(\mathrm{Tr}_{\mathsf{A}}(|D\rangle\langle C|)) \\ &= \mathrm{sgn}(\mathrm{Tr}_{\mathsf{A}}((\mathbb{1} \otimes \sqrt{\sigma})\,|\Omega\rangle\langle\Omega|\,(\mathbb{1} \otimes \sqrt{\rho}))) \\ &= \mathrm{sgn}(\sqrt{\sigma}\sqrt{\rho}) \end{aligned}$$

where the third line uses the fact that the partial trace of $|\Omega\rangle\langle\Omega|$ is the identity matrix.

Let $U\Sigma V^*$ denote the singular value decomposition of the product $\sqrt{\sigma}\sqrt{\rho}$. Then $\mathrm{sgn}(\sqrt{\sigma}\sqrt{\rho}) = U\mathrm{sgn}(\Sigma)V^*$ by definition. On the other hand,

$$\begin{aligned} (\rho^{1/2}\sigma^{1/2})^{-1}\rho^{1/2}(\rho^{-1}\#\sigma)\rho^{1/2} &= (\rho^{1/2}\sigma^{1/2})^{-1}(\rho^{1/2}\sigma\rho^{1/2})^{1/2} \\ &= (V\Sigma U^*)^{-1}(V\Sigma^2 V^*)^{1/2} \\ &= U\Sigma^{-1}V^*V\Sigma V^* \\ &= U\mathrm{sgn}(\Sigma)V^* \\ &= \mathrm{sgn}(\sqrt{\sigma}\sqrt{\rho}) \end{aligned}$$

where the first line uses that

$$\rho^{1/2}(\rho^{-1}\#\sigma)\rho^{1/2} = \rho^{1/2}\rho^{-1/2}(\rho^{1/2}\sigma\rho^{1/2})^{1/2}\rho^{-1/2}\rho^{1/2} = (\rho^{1/2}\sigma\rho^{1/2})^{1/2}\ .$$

To see this, we use two facts:

1. $\rho^{1/2}\rho^{-1/2}$ is the projection onto $\mathrm{Image}(\rho)$
2. $\mathrm{Image}\Big((\rho^{1/2}\sigma\rho^{1/2})^{1/2}\Big) = \mathrm{Image}\Big(\rho^{1/2}\sigma\rho^{1/2}\Big) \subseteq \mathrm{Image}(\rho)$.

Therefore $\rho^{1/2}\rho^{-1/2}$ acts as the identity on $(\rho^{1/2}\sigma\rho^{1/2})^{1/2}$. This concludes the proof of the claim. □

Claim 3.2. *The following hold:*

1. *WW^* is the projection onto* $\mathrm{Image}(\sigma^{1/2}\rho\sigma^{1/2})$*, and*
2. *W^*W is the projection onto* $\mathrm{Image}(\rho^{1/2}\sigma\rho^{1/2})$*.*

Proof. These items follow from the proof of Claim 3.1, which established that $W = \mathrm{sgn}(\sqrt{\sigma}\sqrt{\rho})$. Let $\sqrt{\sigma}\sqrt{\rho}$ have singular value decomposition $U\Sigma V^*$. Then $W = U\mathrm{sgn}(\Sigma)V^*$. Therefore

$$WW^* = U\mathrm{sgn}(\Sigma)U^*$$

which is the projection onto the image of $\sigma^{1/2}\rho\sigma^{1/2} = U\Sigma U^*$. Similarly, $W^*W = V\mathrm{sgn}(\Sigma)V^*$ which is the projection onto the image of $\rho^{1/2}\sigma\rho^{1/2} = V\Sigma V^*$.

□

We verify the completeness property of the canonical Uhlmann transformation.

Claim 3.3. *For all unitary completions U of W, we have $\langle D| \mathbb{1} \otimes U |C\rangle = \mathrm{F}(\rho, \sigma)$.*

Proof. First, observe that

$$\langle D| \mathbb{1} \otimes W |C\rangle = \mathrm{Tr}(\sigma^{1/2} W \rho^{1/2}) = \mathrm{Tr}(\rho^{1/2}\sigma^{1/2}\,\mathrm{sgn}(\sigma^{1/2}\rho^{1/2})) = \mathrm{Tr}((\rho^{1/2}\sigma\rho^{1/2})^{1/2}) = \mathrm{F}(\rho, \sigma)$$

where we used the fact that for all square matrices A, $\mathrm{Tr}(A\,\mathrm{sgn}(A^*)) = \mathrm{Tr}(\sqrt{AA^*})$ and we used the definition of the fidelity function.

Now let $U = W + E$ be a unitary completion of W. Suppose for sake of contradiction that $\langle D| \mathbb{1} \otimes U |C\rangle \neq \mathrm{F}(\rho, \sigma)$. Then this implies that $\langle D| \mathbb{1} \otimes E |C\rangle \neq 0$. Let $e^{i\theta}$ be a complex phase such that $e^{i\theta} \langle D| \mathbb{1} \otimes E |C\rangle$ is a strictly positive number. Then consider the unitary $U' = W + e^{i\theta} E$. Then

$$\langle D| \mathbb{1} \otimes U' |C\rangle = \mathrm{F}(\rho, \sigma) + e^{i\theta} \langle D| \mathbb{1} \otimes E |C\rangle > \mathrm{F}(\rho, \sigma)$$

which contradicts Uhlmann's theorem. □

3.2 The rigidity proof

Now we prove that the canonical Uhlmann transformation W has $\delta(\epsilon)$-robust rigidity for $\delta(\epsilon) = (2\kappa/\eta)\epsilon$. We do this by setting up a semidefinite program (SDP) whose objective is to maximize the distance

$$\|\mathbb{1} \otimes W |C\rangle - \mathbb{1} \otimes RW^*W |C\rangle\|^2$$

when ranging over all unitary operators R satisfying $\langle D| \mathbb{1} \otimes R |C\rangle \geq \mathrm{F}(\rho, \sigma) - \epsilon$. We analyze the dual SDP, which is a minimization problem, and provide a feasible solution whose objective is $2\kappa\epsilon/\eta$, which by (weak) SDP duality gives an upper bound on the objective value of the primal SDP.

For convenience, we present some helpful notation for the rest of the proof:

- W is the canonical Uhlmann transformation corresponding to $(|C\rangle, |D\rangle)$,
- $A = \sqrt{\sigma}\sqrt{\rho}$,
- $P = W^*W$ is the projection onto $\mathrm{Image}(\rho^{1/2}\sigma\rho^{1/2})$ by Claim 3.2.

The robustness function $\delta(\epsilon)$ of W can be cast as the optimum of the following optimization problem (P), where R ranges over all matrices.

$$\begin{aligned} \underset{R}{\text{maximize}} \quad & \|\mathbb{1} \otimes (W - R)P |C\rangle\|^2 \\ \text{subject to} \quad & \langle D| \mathbb{1} \otimes R |C\rangle \geq \mathrm{F}(\rho, \sigma) - \epsilon \\ & R^*R = \mathbb{1}\,. \end{aligned} \tag{P}$$

The next claim shows how to recast this optimization problem as a standard-form SDP.

Claim 3.4. *Let ω denote the value of the following SDP:*

$$\begin{aligned} \underset{X}{\textit{maximize}} \quad & \mathrm{Tr}(CX) \\ \textit{subject to} \quad & \Phi(X) = B \\ & X \geq 0 \end{aligned} \tag{Primal SDP}$$

where X is a block-matrix $\begin{pmatrix} X_1 & R \\ R^* & X_2 \end{pmatrix}$*, the matrix* $C = \frac{1}{2}\begin{pmatrix} 0 & -W\rho P \\ -P\rho W^* & 0 \end{pmatrix}$*, Φ is the Hermiticity-preserving superoperator*

$$\Phi(X) = \begin{pmatrix} X_1 & & \\ & X_2 & \\ & & \frac{1}{2}\mathrm{Tr}(RA^*) + \frac{1}{2}\mathrm{Tr}(R^*A) \end{pmatrix},$$

where $A = \sigma^{1/2}\rho^{1/2}$*, and* $B = \begin{pmatrix} \mathbb{1} & & \\ & \mathbb{1} & \\ & & \mathrm{F}(\rho,\sigma) - \epsilon \end{pmatrix}$*. Then* $2(\omega + \mathrm{Tr}(P\rho))$ *is an upper bound to the optimal value of the optimization problem (P).*

Proof. We first relax the constraint on $R^*R = \mathbb{1}$ in (P) to $R^*R \leq \mathbb{1}$; an upper bound for this relaxed optimization problem is also an upper bound for (P). Using Lemma 2.3 we observe that $R^*R \leq \mathbb{1}$ is equivalent to $\begin{pmatrix} \mathbb{1} & R \\ R^* & \mathbb{1} \end{pmatrix} \geq 0$.

Next, we observe that we can replace the condition $\langle D|\, \mathbb{1} \otimes R\, |C\rangle \geq \mathrm{F}(\rho,\sigma) - \epsilon$ in (P) by $\langle D|\, \mathbb{1} \otimes R\, |C\rangle = \mathrm{F}(\rho,\sigma) - \epsilon$, i.e., the maximizer in (P) will always satisfy this condition with equality. This is because any R that achieves a better-than-necessary fidelity can be perturbed in a way that lowers the fidelity, but does not decrease the distance $\|\mathbb{1} \otimes (W - R)P\, |C\rangle\|^2$ from the optimal Uhlmann transform. Secondly, the condition $\langle D|\, \mathbb{1} \otimes R\, |C\rangle = \mathrm{F}(\rho,\sigma) - \epsilon$ implicitly imposes that R is chosen such that $\langle D|\, \mathbb{1} \otimes R\, |C\rangle$ is real; we can relax this condition to $\Re\, \langle D|\, \mathbb{1} \otimes R\, |C\rangle = \mathrm{F}(\rho,\sigma) - \epsilon$, or equivalently

$$\frac{1}{2}\mathrm{Tr}(RA^*) + \frac{1}{2}\mathrm{Tr}(R^*A) = \mathrm{F}(\rho,\sigma) - \epsilon\,,$$

where $A = \sigma^{1/2}\rho^{1/2}$.

Third, we turn to the objective function in (P). Using that $P = W^*W$ is a projection and $PW^* = W^*$, as well as the condition $R^*R \leq \mathbb{1}$, we get

$$\begin{aligned} \|\mathbb{1} \otimes (W - R)P\, |C\rangle\|^2 &= \langle C|\, \mathbb{1} \otimes PW^*WP\, |C\rangle + \langle C|\, \mathbb{1} \otimes RR^*RP\, |C\rangle - 2\Re\, \langle C|\, PW^*RP\, |C\rangle \\ &\leq 2\,\mathrm{Tr}(P\rho) - \big(\mathrm{Tr}(RP\rho W^*) + \mathrm{Tr}(W\rho PR^*)\big)\,. \end{aligned}$$

Thus we see that the optimization problem (P) is upper-bounded the following SDP, except the objective value is scaled by 2 and shifted by a constant $2\mathrm{Tr}(P\rho)$:

$$\begin{aligned} \text{maximize} \quad & -\tfrac{1}{2}\mathrm{Tr}(RP\rho W^*) - \tfrac{1}{2}\mathrm{Tr}(W\rho PR^*) \\ \text{subject to} \quad & \begin{pmatrix} \mathbb{1} & R \\ R^* & \mathbb{1} \end{pmatrix} \geq 0 \\ & \frac{1}{2}\mathrm{Tr}(RA^*) + \frac{1}{2}\mathrm{Tr}(R^*A) = \mathrm{F}(\rho,\sigma) - \epsilon\,. \end{aligned}$$

Putting this SDP into standard form yields Claim 3.4. □

We now analyze the dual of (Primal SDP).

Claim 3.5. *The following is the SDP dual of (Primal SDP):*

$$\begin{aligned} \underset{Y}{\textit{minimize}} \quad & \mathrm{Tr}(Y_1) + \mathrm{Tr}(Y_2) + \alpha(\mathrm{F}(\rho,\sigma) - \epsilon) \\ \textit{subject to} \quad & \begin{pmatrix} Y_1 & \frac{1}{2}\alpha A \\ \frac{1}{2}\alpha A^* & Y_2 \end{pmatrix} \geq \frac{1}{2}\begin{pmatrix} & -W\,\rho P \\ -P\rho\,W^* & \end{pmatrix} \\ & Y \textit{ Hermitian} . \end{aligned} \tag{Dual SDP}$$

where Y ranges over all block matrices of the form $\begin{pmatrix} Y_1 & * & * \\ * & Y_2 & * \\ * & * & \alpha \end{pmatrix}$ *with $\alpha \in \mathbb{R}$.*

Proof. Taking the dual of (Primal SDP) we get

$$\begin{aligned} \text{minimize} \quad & \mathrm{Tr}(BY) \\ \text{subject to} \quad & \Phi^*(Y) \geq C \\ & Y \text{ Hermitian} \end{aligned}$$

We compute the adjoint Φ^*. For all block matrices $Y = \begin{pmatrix} Y_1 & * & * \\ * & Y_2 & * \\ * & * & \alpha \end{pmatrix}$ where α is a scalar, we claim that Φ^* evaluated on Y is given by

$$\Phi^*(Y) = \begin{pmatrix} Y_1 & \frac{1}{2}\alpha A \\ \frac{1}{2}\alpha A^* & Y_2 \end{pmatrix} .$$

We can verify that this is the adjoint because

$$\mathrm{Tr}(Y\Phi(X)) = \mathrm{Tr}(Y_1X_1) + \mathrm{Tr}(Y_2X_2) + \frac{1}{2}\alpha\mathrm{Tr}(RA^*) + \frac{1}{2}\alpha\mathrm{Tr}(R^*A) = \mathrm{Tr}(\Phi^*(Y)X) .$$

It then follows from weak SDP duality that an upper bound on the value of the dual SDP is also an upper bound on the value of the primal SDP. □

We now consider feasible certificates for (Dual SDP), which give *upper bounds* on the value of (Dual SDP), which by weak SDP duality gives upper bounds on the value of (Primal SDP).

Claim 3.6. *For all $\alpha \in \mathbb{R}$, the matrix*

$$Y = \begin{pmatrix} \sqrt{T^*T} & & \\ & T(\sqrt{T^*T})^{-1}T^* & \\ & & \alpha \end{pmatrix}$$

is feasible for (Dual SDP), where $T = \frac{1}{2}\left(\alpha A^* + P\rho W^*\right)$, and the corresponding value of the objective function is

$$2\|T\|_1 + \alpha(\mathrm{F}(\rho,\sigma) - \epsilon) .$$

Proof. Our choice of Y is manifestly self-adjoint, so we only need to check that it satisfies the constraint

$$\begin{pmatrix} Y_1 & \frac{1}{2}\alpha A \\ \frac{1}{2}\alpha A^* & Y_2 \end{pmatrix} \geq \frac{1}{2}\begin{pmatrix} & -W\,\rho P W \\ -P\rho\, W^* & \end{pmatrix} .$$

For our choice of Y, this is equivalent to

$$\begin{pmatrix} \sqrt{T^*T} & T^* \\ T & T(\sqrt{T^*T})^{-1}T^* \end{pmatrix} \geq 0 .$$

This follows easily from Lemma 2.3. The only non-trivial condition to check is that $(\mathbb{1}-\sqrt{T^*T}(\sqrt{T^*T})^{-1})T^* = 0$. This holds because $\sqrt{T^*T}(\sqrt{T^*T})^{-1}$ is the projector onto $\mathrm{Dom}(\sqrt{T^*T}) = \mathrm{Dom}(T^*T) = \mathrm{Dom}(T) = \mathrm{Image}(T^*)$.

The value achieved by this Y is

$$\begin{aligned} \mathrm{Tr}(Y_1) + \mathrm{Tr}(Y_2) + \alpha(\mathrm{F}(\rho,\sigma) - \epsilon) &= \mathrm{Tr}(\sqrt{T^*T}) + \mathrm{Tr}(T(\sqrt{T^*T})^{-1}T^*) + \alpha(\mathrm{F}(\rho,\sigma) - \epsilon) \\ &= 2\|T\|_1 + \alpha(\mathrm{F}(\rho,\sigma) - \epsilon) , \end{aligned}$$

where the last line holds because $\mathrm{Tr}(T(\sqrt{T^*T})^{-1}T^*) = \mathrm{Tr}(\sqrt{T^*T}(\sqrt{T^*T})^{-1}\sqrt{T^*T}) = \mathrm{Tr}(\sqrt{T^*T}) = \|T\|_1$ by the properties of the pseudoinverse. □

Recall that $\kappa = \|\rho^{-1/2}P\rho^{1/2}\|_\infty^2$ and η is the smallest nonzero eigenvalue of $\rho^{-1}\#\sigma$. The next claim computes a bound on the value of the dual SDP for $\alpha = -\kappa/\eta$.

Claim 3.7. *Let $\alpha = -\kappa/\eta$. Then for the feasible solution Y given by Claim 3.6 achieves value $(\kappa/\eta)\epsilon - \mathrm{Tr}(P\rho)$.*

Proof. By definition of T, we have

$$2\|T\|_1 = \|\alpha A^* + P\rho W^*\|_1 = \|\alpha A^* W + P\rho P\|_1 .$$

This is because we can write $W = QU$ for some projection Q and a unitary U. The projection Q is equal to WW^*, which by Claim 3.2 is the projection onto $\mathrm{Image}(\sigma^{1/2}\rho\sigma^{1/2})$, or equivalently onto $\mathrm{Dom}(\rho^{1/2}\sigma^{1/2})$. Thus $A^* = \rho^{1/2}\sigma^{1/2}Q = A^*Q$ and $W^* = W^*Q$. The equality then follows by unitary invariance of the trace norm.

For our choice of α, $2\|T\|_1$ is equal to

$$\|P\rho P - (\kappa/\eta)A^*W\|_1 = \|(\kappa/\eta)A^*W - P\rho P\|_1 .$$

We will argue that

$$(\kappa/\eta)A^*W - P\rho P \geq 0 \tag{4}$$

in the positive semidefinite ordering. This will complete the proof of the claim because then the objective value of the dual SDP is equal to

$$\begin{aligned} \|(\kappa/\eta)A^*W - P\rho P\|_1 + \alpha(\mathrm{F}(\rho,\sigma) - \epsilon) &= \mathrm{Tr}((\kappa/\eta)A^*W - P\rho P) + \alpha(\mathrm{F}(\rho,\sigma) - \epsilon) \\ &= (\kappa/\eta)\mathrm{Tr}(A^*W) - \mathrm{Tr}(P\rho) - (\kappa/\eta)\mathrm{F}(\rho,\sigma) + (\kappa/\eta)\epsilon \\ &= (\kappa/\eta)\epsilon - \mathrm{Tr}(P\rho) \end{aligned}$$

as desired. The last line follows because $\mathrm{Tr}(A^*W) = \mathrm{F}(\rho, \sigma)$ as shown in the proof of Claim 3.3.

We now prove Equation (4). The proof of Claim 3.1 shows that $W = (\rho^{1/2}\sigma^{1/2})^{-1}(\rho^{1/2}\sigma\rho^{1/2})^{1/2}$. Thus

$$A^*W = \rho^{1/2}(\rho^{-1}\#\sigma)\rho^{1/2} \ ,$$

because $A^*(A^*)^{-1}$ is equal to the projection onto $\mathrm{Image}(\rho^{1/2}\sigma^{1/2})$. From this expression we see that A^*W is self-adjoint.

We now argue that

$$\mathrm{Dom}(\rho^{-1/2}P\rho P\rho^{-1/2}) \subseteq \mathrm{Dom}(\rho^{-1}\#\sigma) \ . \tag{5}$$

This is equivalent to showing that

$$\ker(\rho^{-1/2}P\rho P\rho^{-1/2}) \supseteq \ker(\rho^{-1}\#\sigma) \ .$$

Let $|v\rangle$ be a vector in $\ker(\rho^{-1}\#\sigma)$, which implies

$$\langle v|\, \rho^{-1/2}(\rho^{1/2}\sigma\rho^{1/2})^{1/2}\rho^{-1/2}\, |v\rangle = 0 \ .$$

This implies that the vector $\rho^{-1/2}\,|v\rangle \in \ker((\rho^{1/2}\sigma\rho^{1/2})^{1/2})$. On the other hand, $\ker((\rho^{1/2}\sigma\rho^{1/2})^{1/2}) = \ker(\rho^{1/2}\sigma\rho^{1/2})$, so therefore $P\rho^{-1/2}\,|v\rangle = 0$. This implies that $|v\rangle \in \ker(\rho^{-1/2}P\rho P\rho^{-1/2})$, as desired.

Let $\Pi_{\mathrm{Dom}(\rho^{-1/2}P\rho P\rho^{-1/2})}$ and $\Pi_{\mathrm{Dom}(\rho^{-1}\#\sigma)}$ denote the projections onto the specified domains. Thus

$$\begin{aligned}
\rho^{-1/2}P\rho P\rho^{-1/2} &\leq \kappa\, \Pi_{\mathrm{Dom}(\rho^{-1/2}P\rho P\rho^{-1/2})} \\
&\leq \kappa\, \Pi_{\mathrm{Dom}(\rho^{-1}\#\sigma)} \\
&\leq \frac{\kappa}{\eta}\rho^{-1}\#\sigma \ .
\end{aligned}$$

The first line follows from the definition of κ, the second line follows from Equation (5), and the third line follows because η is the smallest non-zero eigenvalue of $\rho^{-1}\#\sigma$.

To conclude, we can conjugate by $\rho^{1/2}$ (which preserves the operator inequality) to get

$$P\rho P \leq \frac{\kappa}{\eta}\rho^{1/2}(\rho^{-1}\#\sigma)\rho^{1/2} = \frac{\kappa}{\eta}A^*W$$

as desired. This uses the fact that $\rho^{1/2}\rho^{-1/2}P = P\rho^{-1/2}\rho^{1/2} = P$, as shown in the proof of Claim 3.1.

□

Combining Claim 3.7 with Claim 3.4 shows that the optimal value of (P) is at most

$$2(\omega + \mathrm{Tr}(P\rho)) \leq \left(\frac{2\kappa}{\eta}\right)\epsilon$$

as desired. This concludes the proof of the rigidity property of Theorem 1.6.

4 Sensitivity of Uhlmann transformations

In this section we present several examples that illustrate the *sensitivity* of the canonical Uhlmann transformation. Some of these examples will demonstrate that it is necessary for the rigidity bound of Theorem 1.6 to depend on both the spectral gap η as well as the obliqueness κ.

4.1 Canonical Uhlmann transformation is not a smooth function of input states

The canonical Uhlmann transformation W is not a smoothly-varying function of the states $|C\rangle, |D\rangle$. It is instructive to consider the following two-qutrit example:

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

The canonical Uhlmann transformation W corresponding to $(|C\rangle, |D\rangle)$ is simply the identity operator on $\mathbb{C}^3$. On the other hand, the Uhlmann transformation $\tilde{W}$ corresponding to $(|\tilde{C}\rangle, |D\rangle)$ 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 $|C\rangle - |\tilde{C}\rangle$ has norm at most ϵ, which can be arbitrarily small.

4.2 The dependence on the spectral gap parameter η

The parameter η in Theorem 1.6 can be viewed as quantifying how "well-conditioned" the pair of states $(|C\rangle, |D\rangle)$ are. We now present an example of a pair of states $(|C\rangle, |D\rangle)$ that

1. Shows the dependence on the spectral gap η in the rigidity bound of Theorem 1.6 is necessary, and

2. Demonstrates a scenario where the canonical Uhlmann transformation W corresponding to the pair $(|C\rangle, |D\rangle)$ has a different robustness than the Uhlmann transformation W^* corresponding to the flipped pair $(|D\rangle, |C\rangle)$.

Lemma 4.1. *For all even $d \in \mathbb{N}$ and for all $\eta > 0$, there exists a pair $(|C\rangle, |D\rangle)$ of d-dimensional states with reduced density matrices ρ, σ respectively such that*

1. $\mathrm{F}(\rho, \sigma) \geq \frac{1}{2}$,

2. *The smallest nonzero eigenvalue of $\rho^{-1}\#\sigma$ is η.*

3. *Let W denote the canonical Uhlmann transformation for $(|C\rangle, |D\rangle)$. For all $0 < \epsilon < 1$ there exists a unitary R such that*
$$\langle D|\, \mathbb{1} \otimes R\, |C\rangle \geq \mathrm{F}(\rho, \sigma) - \epsilon$$
but
$$\|\mathbb{1} \otimes (W - R)W^* W\, |C\rangle\, \|^2 \geq 2\epsilon/\eta \ .$$

4. *Let W^* denote the canonical Uhlmann transformation for $(|D\rangle, |C\rangle)$. For all unitaries Q such that*
$$\langle C|\, \mathbb{1} \otimes Q\, |D\rangle \geq \mathrm{F}(\rho, \sigma) - \epsilon$$
we have
$$\|\mathbb{1} \otimes (W^* - Q)WW^*\, |D\rangle\, \|^2 \leq 2\sqrt{2}\epsilon \ .$$

Proof. Fix η and let $\delta = \eta^2/2$. Let $A = \{1, 2, \ldots, d/2\}$ and $B = \{d/2+1, \ldots, d\}$. Consider the pair of states

$$|C\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |i\rangle \otimes |i\rangle \ , \qquad |D\rangle = \sum_{i=1}^{d} \sqrt{\sigma_i}\, |i\rangle \otimes |i\rangle$$

where $\sigma_i = 2(1-\delta)/d$ if $i \in A$ and $\sigma_i = 2\delta/d$ otherwise. Let σ be the diagonal matrix with entries (σ_i), and let $\rho = \mathbb{1}/d$ denote the maximally mixed state. By construction ρ, σ are the reduced density matrices of $|C\rangle, |D\rangle$ on register A, respectively.

The fidelity between ρ, σ is

$$\mathrm{F}(\rho, \sigma) = \sum_i \sqrt{\sigma_i/d} = \frac{d}{2}\Big(\sqrt{2(1-\delta)/d^2} + \sqrt{2\delta/d^2}\Big) = \sqrt{\frac{1-\delta}{2}} + \sqrt{\frac{\delta}{2}} \geq \frac{1}{2} \ .$$

The canonical Uhlmann transformation W for $(|C\rangle, |D\rangle)$ is the following:

$$W = \mathrm{sgn}(\mathrm{Tr}_{\mathsf{A}}(|D\rangle\langle C|)) = \mathrm{sgn}\Big(\sum_i \sqrt{\frac{\sigma_i}{d}}\, |i\rangle\langle i|\Big) = \mathbb{1} \ .$$

Here we used that $\sigma_i > 0$ for all i. Similarly, the canonical Uhlmann transformation W^* for $(|D\rangle, |C\rangle)$ is also the identity matrix. However their robustnesses are different.

Robustness of W. The matrix geometric mean $\rho^{-1}\#\sigma$ is a diagonal matrix whose entries are $\sqrt{d\sigma_i}$. The smallest nonzero eigenvalue is $\sqrt{2\delta} = \eta$. Since ρ, σ commute, the obliqueness parameter κ is equal to 1.

Let $0 < \tau < 1$. Let $G \subseteq B$ be a subset such that $|G|/|B| \geq \tau$. Consider the following Uhlmann transformation R: it acts as identity on the basis states $|i\rangle$ for $i \notin G$, and applies a *derangement* (i.e., a permutation without any fixed points) on the basis states in G. The performance of this Uhlmann transformation is

$$\langle D|\, \mathbb{1} \otimes R\, |C\rangle = \sum_{i \notin G} \sqrt{\rho_i \sigma_i} \geq \frac{d}{2}\sqrt{\frac{2(1-\delta)}{d^2}} + \frac{(1-\epsilon)d}{2}\sqrt{\frac{2\delta}{d^2}} = \sqrt{\frac{1-\delta}{2}} + (1-\tau)\sqrt{\frac{\delta}{2}}$$

Thus, the fidelity deficit of R is $\epsilon = \tau\sqrt{\delta/2}$. On the other hand, we can evaluate the distance of R from $W = \mathbb{1}$ (when evaluated on $|C\rangle$ and using the fact that $W^*W = \mathbb{1}$):

$$\|\, |C\rangle - \mathbb{1} \otimes R\, |C\rangle \,\|^2 = 2\Big\| \sum_{i \in G} \frac{1}{d} \Big\|^2 = 2|G|/d \geq \tau \ .$$

This exactly matches the robust rigidity upper bound given by Theorem 1.6, which is

$$\delta(\epsilon) = (2\kappa/\eta)\epsilon = \frac{2}{\sqrt{2\delta}}\sqrt{\frac{\delta}{2}}\tau = \tau \ .$$

Thus, when the parameter η is very small, there exist near-optimal Uhlmann transformations that can be far away from the canonical one, when measured on $|C\rangle$.

Robustness of W^*. Now we investigate the robustness of the canonical Uhlmann transformation for the opposite state transformation (going from $|D\rangle$ to $|C\rangle$). The matrix geometric mean $\sigma^{-1}\#\rho$ has diagonal entries $\frac{1}{\sqrt{d\sigma_i}}$, and thus the smallest nonzero eigenvalue is $\eta' = \frac{1}{\sqrt{2(1-\delta)}} \geq \frac{1}{\sqrt{2}}$. The obliqueness parameter κ' is still 1.

Thus, by Theorem 1.6, any unitary Q such that

$$\langle C| \mathbb{1} \otimes Q |D\rangle \geq \mathrm{F}(\rho, \sigma) - \epsilon$$

must satisfy

$$\| |D\rangle - \mathbb{1} \otimes Q |D\rangle \|^2 \leq (2/\eta')\epsilon \leq 2\sqrt{2}\,\epsilon \ .$$

Therefore the rigidity of the *opposite* state transformation (from $|D\rangle$ to $|C\rangle$) is much more robust when measured on $|D\rangle$.

□

4.3 A rounding lemma for the spectral gap

Lemma 4.1 shows that the dependence on the spectral gap η in the rigidity of Uhlmann transformations is unavoidable. In the following, we show that every pair of states $(|C\rangle, |D\rangle)$, which might have a very small spectral gap η, is *close* to another pair of states $(|\tilde{C}\rangle, |\tilde{D}\rangle)$ with a better spectral gap $\tilde{\eta}$. We call this a *rounding lemma* for the spectral gap parameter.

Lemma 4.2 (Rounding lemma for the spectral gap)**.** *For all $0 < \eta < 1$, for all pure bipartite states $|C\rangle, |D\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ with reduced density matrices ρ, σ on subsystem A, there exist bipartite states $|\tilde{C}\rangle, |\tilde{D}\rangle$ with reduced density matrices $\tilde{\rho}, \tilde{\sigma}$ such that*

1. *The smallest nonzero eigenvalue of $\tilde{\rho}^{-1}\#\tilde{\sigma}$ is at least η, and*
2. *Both $|\langle \tilde{D}|D\rangle|^2$ and $\langle \tilde{C}|C\rangle|^2$ are at least $1 - \eta^2$.*

Proof. Let $|C\rangle, |D\rangle$ be two states such that

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

First we argue that $|C\rangle, |D\rangle$ are arbitrarily close to states $|\hat{C}\rangle, |\hat{D}\rangle$ where the corresponding reduced density matrices $\hat{\rho}, \hat{\sigma}$ are invertible. Define

$$\hat{\rho} = (1-\delta)\rho + \delta\frac{\mathbb{1}}{d}, \qquad \hat{\sigma} = (1-\delta)\sigma + \delta\frac{\mathbb{1}}{d}$$

and define

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

Clearly, $|\langle \hat{C}|C\rangle|^2 = \mathrm{Tr}(\sqrt{\hat{\rho}}\sqrt{\rho})^2 \geq 1 - \delta$ where we used the fact that $\sqrt{\hat{\rho}} \geq \sqrt{(1-\delta)}\sqrt{\rho}$ in the positive semidefinite ordering. Similarly, $|\langle \hat{D}|D\rangle|^2 \geq 1 - \delta$. Note that for any nonzero value of δ, the density matrices $\hat{\sigma}, \hat{\rho}$ are invertible.

Thus we assume without loss of generality that ρ, σ are invertible to begin with. We now show there exists a density matrix $\tilde{\sigma}$ that is $O(\eta)$-close to σ such the least nonzero eigenvalue of $\rho^{-1}\#\tilde{\sigma}$ is at least η.

Let Π denote the projection onto the eigenspace of $\rho^{-1}\#\sigma$ with eigenvalues at least η. Then

$$\mathrm{Tr}((\mathbb{1}-\Pi)(\rho^{-1}\#\sigma)\rho) \leq \eta \ .$$

On the other hand, by direct calculation we have that for invertible ρ, σ,

$$(\rho^{-1}\#\sigma)\rho = (\rho^{-1}\#\sigma)\rho(\rho^{-1}\#\sigma)(\rho\#\sigma^{-1}) = \sigma(\rho\#\sigma^{-1}) \ .$$

Next, $\mathbb{1}-\Pi$ projects onto the eigenspace of $\rho\#\sigma^{-1}$ with eigenvalues at least $1/\eta$. Therefore

$$\mathrm{Tr}((\mathbb{1}-\Pi)(\rho^{-1}\#\sigma)\rho) = \mathrm{Tr}(\sigma(\rho\#\sigma^{-1})(\mathbb{1}-\Pi)) \geq \frac{1}{\eta}\mathrm{Tr}(\sigma(\mathbb{1}-\Pi)) \ .$$

Thus $\mathrm{Tr}(\sigma(\mathbb{1}-\Pi)) \leq \eta^2$. Let $\tilde{\sigma} = \Pi\sigma\Pi/\mathrm{Tr}(\Pi\sigma)$. By the Gentle Measurement Lemma (see [Wat18, Corollary 3.15]), $\mathrm{F}(\sigma,\tilde{\sigma}) \geq \sqrt{1-\eta^2}$. We now evaluate

$$\rho^{-1}\#\tilde{\sigma} = \beta\Big((\rho^{-1}\#\Pi\sigma\Pi)\Big) = \beta\rho^{-1/2}\Big(\rho^{1/2}\Pi\sigma\Pi\rho^{1/2}\Big)^{1/2}\rho^{-1/2} \ .$$

Claim 4.3. *Suppose B, X are positive semidefinite matrices and let A be strictly positive. Then if*

$$\begin{pmatrix} A & X \\ X & B \end{pmatrix} \geq 0$$

then for all projections Π that commute with X we have

$$A^{1/2}(A^{-1/2}\Pi B\Pi A^{-1/2})^{1/2}A^{1/2} \geq \Pi X\Pi \ .$$

Proof. By conjugating with $\begin{pmatrix} \mathbb{1} & 0 \\ 0 & \Pi \end{pmatrix}$ we get

$$\begin{pmatrix} A & \Pi X\Pi \\ \Pi X\Pi & \Pi B\Pi \end{pmatrix} = \begin{pmatrix} A & X\Pi \\ \Pi X & \Pi B\Pi \end{pmatrix} \geq 0 \ .$$

Here we used that $\Pi X = X\Pi = \Pi X\Pi$ since Π is a projector and X and Π commute by assumption. By the Schur complement lemma (Lemma 2.3) we have

$$\Pi B\Pi \geq \Pi X\Pi A^{-1}\Pi X\Pi \ .$$

Conjugating by $A^{-1/2}$ and using operator monotonicity of the square root we have

$$(A^{-1/2}\Pi B\Pi A^{-1/2})^{1/2} \geq A^{-1/2}\Pi X\Pi A^{-1/2} \ .$$

Since A is invertible we can multiply both sides by $A^{1/2}$ and get

$$A^{1/2}(A^{-1/2}\Pi B\Pi A^{-1/2})^{1/2}A^{1/2} \geq \Pi X\Pi \ .$$

□

Using this preceding Claim with $A = \rho^{-1}, B = \sigma, X = \rho^{-1}\#\sigma$ and $\Pi = \Pi$ (which commutes with X) we get

$$\rho^{-1}\#\tilde{\sigma} \geq \beta\Pi(\rho^{-1}\#\sigma)\Pi \ .$$

Therefore $\rho^{-1}\#\tilde{\sigma}$ has a larger spectral gap than $\Pi(\rho^{-1}\#\sigma)\Pi$ since β is at least 1.

□

4.4 The dependence on the obliqueness parameter κ

We now show that the dependence on the parameter κ is also necessary in the rigidity bound of Theorem 1.6. Recall that P is the projection onto the image of $\rho^{1/2}\sigma\rho^{1/2}$. The intuition behind the obliqueness parameter $\kappa = \|\rho^{-1/2}P\rho^{1/2}\|_\infty^2$ is less clear than that of η (at least, to us).

First, note that the operator $\rho^{-1/2}P\rho^{1/2}$ is a projection operator, in that

$$(\rho^{-1/2}P\rho^{1/2})^2 = \rho^{-1/2}P\rho^{1/2} \ .$$

However, it is not necessarily self-adjoint, in which case it is called an *oblique* projection. The spectral norm of oblique projections are always at least one, but can be much larger.

One can think of κ as measuring some combination of how noncommuting and noninvertible ρ and σ are; if either (a) ρ, σ commute or (b) ρ, σ are invertible, then κ is always 1 (like in the example constructed in Lemma 4.1). On the other hand, we can construct examples of pairs of states where the spectral norm parameter κ can be arbitrarily large, and the robustness of the canonical Uhlmann transformation must depend on κ and ϵ (albeit in a way that doesn't yet match the upper bounds given by Theorem 1.6).

Lemma 4.4. *For all $d \in \mathbb{N}$, for all $\kappa \geq 1$, and for all $0 < \epsilon \leq \kappa^{-1/2}$, there exists a pair $(|C\rangle, |D\rangle)$ of d-dimensional states with reduced density matrices ρ, σ respectively such that*

1. *The parameter κ satisfies $\kappa = \|\rho^{-1/2}P\rho^{1/2}\|_\infty^2$ where P is the projection onto the image of $\rho^{1/2}\sigma\rho^{1/2}$,*
2. *The smallest nonzero eigenvalue η of $\rho^{-1}\#\sigma$ is at least 1,*
3. *There exists a unitary R and an ϵ (depending on η) such that*

$$\langle D| \mathbb{1} \otimes R |C\rangle = \mathrm{F}(\rho, \sigma) - \epsilon$$

but

$$\|(\mathbb{1} \otimes (W - R)W^* W |C\rangle\|^2 \geq \kappa\, \epsilon^2 \ .$$

Proof. Let ρ be an invertible density matrix, and let $\sigma = |\sigma\rangle\langle\sigma|$ be an arbitrary pure state. First, we calculate the corresponding quantities κ and η for these density matrices.

Claim 4.5. *Let P denote the projection onto the image of $\rho^{1/2}\sigma\rho^{1/2}$. We have that*

1. $\kappa = \|\rho^{-1/2}P\rho^{1/2}\|_\infty^2 = \frac{\langle\sigma|\rho^2|\sigma\rangle}{\langle\sigma|\rho|\sigma\rangle^2}$
2. *The smallest nonzero eigenvalue η of $\rho^{-1}\#\sigma$ is $\frac{1}{\sqrt{\langle\sigma|\rho|\sigma\rangle}}$.*

Proof. First we compute

$$\rho^{1/2}\sigma\rho^{1/2} = \frac{\rho^{1/2}\,|\sigma\rangle\langle\sigma|\,\rho^{1/2}}{\langle\sigma|\,\rho\,|\sigma\rangle}\,\langle\sigma|\,\rho\,|\sigma\rangle \ .$$

The operator P projects onto this pure state, so we can write the projection as

$$P = \frac{\rho^{1/2}\,|\sigma\rangle\langle\sigma|\,\rho^{1/2}}{\langle\sigma|\,\rho\,|\sigma\rangle} \ .$$

We now compute the κ parameter, which is the operator norm of the following matrix

$$\rho^{-1/2} P \rho P \rho^{-1/2} = |\sigma\rangle\langle\sigma| \cdot \frac{\langle\sigma|\,\rho^2\,|\sigma\rangle}{\langle\sigma|\,\rho\,|\sigma\rangle^2} \ .$$

For pure $\sigma = |\sigma\rangle\langle\sigma|$, we have that for any vector $|\alpha\rangle$,

$$\rho^{1/2}\sigma\rho^{1/2}\,|\alpha\rangle = \langle\sigma|\,\rho^{1/2}\,|\alpha\rangle \cdot \rho^{1/2}\,|\sigma\rangle \ ,$$

so $\mathrm{Image}(\rho^{1/2}\sigma\rho^{1/2})$ is spanned solely by the vector $\rho^{1/2}\,|\sigma\rangle$. Hence, P is the normalized projector onto this vector:

$$P = \frac{\rho^{1/2}\,|\sigma\rangle\langle\sigma|\,\rho^{1/2}}{\langle\sigma|\,\rho\,|\sigma\rangle} \ .$$

On the other hand, the η parameter can be computed as follows. The matrix geometric mean $\rho^{-1}\#\sigma$ can be computed as

$$\rho^{-1/2}(\rho^{1/2}\sigma\rho^{1/2})^{1/2}\rho^{-1/2} = \frac{|\sigma\rangle\langle\sigma|}{\sqrt{\langle\sigma|\,\rho\,|\sigma\rangle}} \ .$$

Thus the smallest nonzero eigenvalue is $\frac{1}{\sqrt{\langle\sigma|\rho|\sigma\rangle}}$. □

Define the pure states

$$|C\rangle = \mathbb{1} \otimes \sqrt{\rho}\,|\Omega\rangle \ , \qquad |D\rangle = |\overline{\sigma}\rangle \otimes |\sigma\rangle$$

where $|\overline{\sigma}\rangle$ denotes the entry-wise complex conjugate of $|\sigma\rangle$ with respect to the standard basis. Note that $\overline{\rho}, \overline{\sigma}$ are the reduced density matrices of $|C\rangle, |D\rangle$ on the first register, respectively, where $\overline{\rho}, \overline{\sigma}$ denote the entry-wise complex conjugate of the density matrices ρ, σ, respectively.

The canonical Uhlmann transformation W for the pair $(|C\rangle, |D\rangle)$ is

$$W = \mathrm{sgn}(\mathrm{Tr}_{\mathsf{A}}(|D\rangle\langle C|)) = |\sigma\rangle\langle v|$$

where $|v\rangle = \rho^{1/2}\,|\sigma\rangle / \sqrt{\langle\sigma|\,\rho\,|\sigma\rangle}$. We can verify that this achieves the Uhlmann fidelity between the states $|C\rangle, |D\rangle$:

$$\langle D|\,\mathbb{1} \otimes W\,|C\rangle = \langle v|\,\rho^{1/2}\,|\sigma\rangle = \sqrt{\langle\sigma|\,\rho\,|\sigma\rangle} = \mathrm{F}(\rho,\sigma) = \mathrm{F}(\overline{\rho},\overline{\sigma}) \ .$$

We now analyze the extent to which the canonical Uhlmann transformation W is rigid. Let $|\hat{v}\rangle$ be a state such that $\langle v|\hat{v}\rangle = 1 - \epsilon/\mathrm{F}(\rho,\sigma)$, and let $|\hat{v}\rangle = |v\rangle + |\tau\rangle$ for some subnormalized vector $|\tau\rangle$. Consider the following partial isometry

$$R = |\sigma\rangle\langle\hat{v}| + |\sigma^{\perp}\rangle\langle\hat{v}^{\perp}|$$

where $|\hat{v}\rangle, |\hat{v}^{\perp}\rangle$ are orthogonal and $|\sigma\rangle, |\sigma^{\perp}\rangle$ are orthogonal. Then

$$\langle D|\,\mathbb{1} \otimes R\,|C\rangle = \langle\hat{v}|\,\rho^{1/2}\,|\sigma\rangle = \langle v|\,\rho^{1/2}\,|\sigma\rangle + \langle\tau|\,\rho^{1/2}\,|\sigma\rangle = \mathrm{F}(\rho,\sigma)(1 + \langle\tau|v\rangle) = \mathrm{F}(\rho,\sigma) - \epsilon \ .$$

On the other hand, we have

$$\mathbb{1} \otimes W \left|C\right\rangle = \sqrt{\overline{\rho}} \left|\overline{v}\right\rangle \otimes \left|\sigma\right\rangle$$
$$\mathbb{1} \otimes RW^*W \left|C\right\rangle = (\mathbb{1} \otimes R \left|v\right\rangle\left\langle v\right|)(\sqrt{\overline{\rho}} \otimes \mathbb{1}) \left|\Omega\right\rangle = \sqrt{\overline{\rho}} \left|\overline{v}\right\rangle \otimes R \left|v\right\rangle$$

where $\left|\overline{v}\right\rangle$ denotes the complex conjugate of $\left|v\right\rangle$. Now,

$$R \left|v\right\rangle = \left|\sigma\right\rangle \left\langle \hat{v}|v\right\rangle + \left|\sigma^{\perp}\right\rangle \left\langle \hat{v}^{\perp}|v\right\rangle$$

so that

$$\begin{aligned}
\left\| \mathbb{1} \otimes (W - RW^*W) \left|C\right\rangle \right\| &= \left\| \left|\sigma\right\rangle (1 - \left\langle \hat{v}|v\right\rangle) - \left|\sigma^{\perp}\right\rangle \left\langle \hat{v}^{\perp}|v\right\rangle \right\| \cdot \left\| \sqrt{\overline{\rho}} \left|\overline{v}\right\rangle \right\| \\
&= \sqrt{|\left\langle \tau|v\right\rangle|^2 + |\left\langle \hat{v}^{\perp}|v\right\rangle|^2} \cdot \sqrt{\frac{\left\langle \sigma\right| \rho^2 \left|\sigma\right\rangle}{\left\langle \sigma\right| \rho \left|\sigma\right\rangle^2}} \cdot \sqrt{\left\langle \sigma\right| \rho \left|\sigma\right\rangle} \\
&\geq \mathrm{F}(\rho, \sigma) \cdot |\left\langle \tau|v\right\rangle| \cdot \sqrt{\frac{\left\langle \sigma\right| \rho^2 \left|\sigma\right\rangle}{\left\langle \sigma\right| \rho \left|\sigma\right\rangle^2}} = \sqrt{\kappa} \cdot \epsilon \ .
\end{aligned}$$

□

The reader may notice that the construction of $(\left|C\right\rangle, \left|D\right\rangle)$ in Lemma 4.4 has Uhlmann fidelity $\mathrm{F}(\rho, \sigma)$ that vanishes as the parameter κ increases:

$$\frac{\left\langle \sigma\right| \rho^2 \left|\sigma\right\rangle}{\left\langle \sigma\right| \rho \left|\sigma\right\rangle^2} \leq \frac{\left\langle \sigma\right| \rho \left|\sigma\right\rangle}{\left\langle \sigma\right| \rho \left|\sigma\right\rangle^2} = \frac{1}{\left\langle \sigma\right| \rho \left|\sigma\right\rangle} = \frac{1}{\mathrm{F}(\rho, \sigma)^2} \ .$$

This is not inherent: the following simple modification of the construction yields a pair of states $(\left|C\right\rangle, \left|D\right\rangle)$ whose Uhlmann fidelity $\mathrm{F}(\rho, \sigma)$ is at least $1/2$, but the spectral norm parameter κ can be arbitrarily large, and furthermore the canonical Uhlmann transformation has rigidity that necessarily depends on κ.

Let $\left|\tilde{C}\right\rangle$ and $\left|\tilde{D}\right\rangle$ denote the states constructed in Lemma 4.4. Define new states

$$\left|C\right\rangle = \frac{1}{\sqrt{2}} \left|\perp\right\rangle + \frac{1}{\sqrt{2}} \left|\tilde{C}\right\rangle \ , \qquad \left|D\right\rangle = \frac{1}{\sqrt{2}} \left|\perp\right\rangle + \frac{1}{\sqrt{2}} \left|\tilde{D}\right\rangle$$

where $\left|\perp\right\rangle$ denotes an arbitary vector that is orthogonal to both $\left|\tilde{C}\right\rangle, \left|\tilde{D}\right\rangle$. Clearly the Uhlmann fidelity $\mathrm{F}(\rho, \sigma)$ of $\left|C\right\rangle, \left|D\right\rangle$ is at least $1/2$. On the other hand, one can calculate that the smallest nonzero eigenvalue of $\rho^{-1} \# \sigma$ is at least 1, and the spectral norm parameter $\|\rho^{-1/2} P \rho^{1/2}\|_{\infty}^2$ is at least $1/\mathrm{F}(\tilde{\rho}, \tilde{\sigma})^2$ where $\mathrm{F}(\tilde{\rho}, \tilde{\sigma})$ is the Uhlmann fidelity of $\left|\tilde{C}\right\rangle, \left|\tilde{D}\right\rangle$, which can be made arbitrarily large. Finally, the robustness of the canonical Uhlmann transformation for $\left|C\right\rangle, \left|D\right\rangle$ obeys a similar dependence on κ as in Lemma 4.4.

A rounding lemma for the obliqueness? A natural question is whether there is a rounding lemma for the obliqueness, similar to the rounding lemma for the spectral gap (Lemma 4.2). That is, could every pair of states be close to another pair with a controlled obliqueness? One could even ask for a stronger statement: is every pair of states close to a pair where *both* the spectral gap and obliqueness are controlled? We leave these as interesting open questions.

5 Applications

5.1 The complexity of the Uhlmann Transformation Problem

Recently, Bostanci, Efron, Metger, Poremba, Qian, and Yuen [BEM+23] proposed a framework for studying the computational complexity of unitary transformations. A major focus of their study was on the Uhlmann Transformation Problem, which is the computational task of implementing canonical Uhlmann transformations corresponding to a specified pair of states. In particular, instances of the Uhlmann Transformation problem are pairs (C, D) of circuit descriptions that act on two registers AB, and the corresponding unitary transformation is the canonical Uhlmann transformation between $|C\rangle = C|0\rangle$ and $|D\rangle = D|0\rangle$.

Bostanci, et al. [BEM+23] showed that the Uhlmann Transformation Problem, when restricted to instances whose reduced states on A have fidelity 1, is complete for the unitary complexity class $\mathsf{avgUnitaryHVPZK}$, the unitary complexity analogue of the decision class PZK (perfect zero knowledge, i.e., problems with zero-knowledge protocols with a simulator that exactly reproduces the verifier's view) with an honest verifier. For our discussion here, we need to recall the proof idea for the *containment* of the Uhlmann transformation problem in $\mathsf{avgUnitaryHVPZK}$.

The setup is as follows: a verifier is given classical descriptions of two circuits, C and D, and wants to implement the Uhlmann transformation between the states $|C\rangle$ and $|D\rangle$ with the help of an all-powerful but untrusted prover. The verifier and prover can exchange quantum messages. To check that the untrusted prover applies the canonical Uhlmann transformation, the verifier prepares $|C\rangle$, sends B of $|C\rangle$ to the prover, and checks that the resulting state has high overlap with $|D\rangle$ (e.g. using a SWAP test). If the verifier repeats this experiment many times and all of the experiments pass, by [BEM+23, Proposition 6.3] the verifier knows that the prover has implemented (a channel completion of) the canonical Uhlmann transformation. Furthermore, if the verifier wants to implement the canonical Uhlmann transformation on an arbitrary input state (instead of the B-register of the state $C|0\rangle$ prepared by the verifier itself), they can replace the copy of $|C\rangle$ in a random run of the experiment with a given input state. Provided that the input state has the same distribution as the reduced state of $|C\rangle$ on the B register, [BEM+23] shows that, up to an error that scales as the inverse of the number of experiments the verifier performs, the verifier will have implemented the canonical Uhlmann transformation on their input. For their proof, [BEM+23] used the weak Uhlmann rigidity mentioned in Theorem 1.8 to argue that the prover correctly mapping $|C\rangle$ to $|D\rangle$ with high fidelity must be approximately applying the canonical Uhlmann transformation.

When the fidelity of the reduced states on A is a constant $\gamma < 1$, however, the verifier only expects a γ fraction of the trials to pass, even if the prover is honest and implements the canonical Uhlmann transformation. By repeatedly sending copies of $|C\rangle$ and measuring $|D\rangle\langle D|$, the verifier can estimate how well the prover is mapping $|C\rangle$ to $|D\rangle$, but it was not previously clear that the condition $\langle D|\, \mathbb{1} \otimes R\, |C\rangle \geq \gamma - \epsilon$ implies that R was close, in some notion, to the canonical Uhlmann transformation. Using Theorem 1.6, we can show that such a verifier does indeed implement a transformation close to the canonical Uhlmann transformation on their input state. This yields a 2-round quantum interactive protocol for synthesizing Uhlmann transformations with fidelity γ (formally, solving the unitary synthesis problem $\textsc{DistUhlmann}_\gamma$), similar to the $\mathsf{avgUnitaryHVPZK}$ protocol presented in [BEM+23]. Previously, the only way to synthesize $\textsc{DistUhlmann}_\gamma$ without assuming a polarization conjecture was to go through that fact that the Uhlmann transformation is in $\mathsf{avgUnitaryPSPACE} = \mathsf{avgUnitaryQIP}$, yielding a 8-round protocol.

We note that while we are able to show that (roughly) the same algorithm works to synthesize $\textsc{DistUhlmann}_\gamma$ instances, we are not able to show that $\textsc{DistUhlmann}_\gamma$ is contained in $\mathsf{avgUnitaryHVSZK}$. In fact, the task of the $\mathsf{avgUnitaryHVSZK}$ simulator for $\textsc{DistUhlmann}_\kappa$ is QSZK-hard in general, as it allows one to estimate the fidelity between the input states $|C\rangle$ and $|D\rangle$. Thus, without a major complexity theoretic breakthrough, $\textsc{DistUhlmann}_\gamma$ (for constant γ) is unlikely to be shown to be in $\mathsf{avgUnitaryHVSZK}$. We also note that our algorithm is only efficient for so-called "well-conditioned" instances of $\textsc{DistUhlmann}_\gamma$, namely those whose spectral gap and obliqueness are polynomial in n and r. While we do not formalize the notion of "well-conditioned" Uhlmann instances, it is not hard to see how it could be formalized from the protocol below.

Protocol 1. 2-round quantum interactive protocol for DistUhlmann$_\gamma$

Instance: A valid $\textsc{DistUhlmann}_\gamma$ instance $x = (1^n, C, D)$, and precision $r \in \mathbb{N}$, with spectral gap η and obliqueness κ
Input: An n qubit quantum register B_0.

1. Let $m = 8n(\kappa r/\eta)^2$. Sample $i^* \in [m]$ uniformly at random. Initialize $j \leftarrow 0$.
2. For $i = 1$ through m:
   (a) If $i \neq i^*$:
      i. Prepare the state $|C\rangle_{\mathsf{A'B'}}$ and send $\mathsf{B'}$ to the prover.
      ii. After receiving $\mathsf{B'}$ from the prover, apply D^* to $\mathsf{A'B'}$ and measure all of the qubits in the computational basis.
      iii. If the measurement outcome is 0^n, increment j by 1.
   (b) If $i = i^*$:
      i. Send B_0 to the prover and receive B_0 back.
3. If $j \geq m \cdot \left(\gamma - \frac{\eta}{4\kappa r}\right)$, accept and output B_0, otherwise reject.

We prove that the protocol satisfies both the completeness and soundness conditions in Definition 4.9 of [BEM+23]. Here we will make use of the terminology and notation from [BEM+23].

Lemma 5.1 (Completeness)**.** *For all valid* $\textsc{DistUhlmann}_\gamma$ *instances* $(1^n, C, D)$ *and error parameter* $r \in \mathbb{N}$*, for sufficiently large* n *and* r*, the honest prover that applies the canonical Uhlmann transformation between* $|C\rangle$ *and* $|D\rangle$ *is accepted with probability at least* $1 - 2^{-n}$*.*

Proof. Since the honest prover applies the canonical Uhlmann transformation, every measurement in Step 2(a)ii accepts with probability κ independently. Let X_i be the event that the i'th measurement accepts, the probability that the verifier rejects the honest prover is upper bounded by

Hoeffding's inequality as

$$\begin{aligned}\Pr\left[\sum_i X_i \le m\cdot\left(\gamma-\frac{\eta}{4\kappa r}\right)\right] &\le \Pr\left[\left|\sum_i X_i - \mathbb{E}\left[\sum_i X_i\right]\right| \ge \frac{m}{(2\kappa r/\eta)}\right]\\ &\le \exp\left(-2m/(4\kappa r/\eta)^2\right)\\ &= 2\exp(-n)\\ &\le 2^{-n}\,.\end{aligned}$$

□

Lemma 5.2 (Soundness)**.** *For all valid* $\textsc{DistUhlmann}_\kappa$ *instances* $(1^n, C, D)$*, and error parameters* $r \in \mathbb{N}$*, for sufficiently large* n *and* r*, for all quantum provers* P*, there exists a channel completion* Φ_x *of the canonical Uhlmann transformation* U_x *such that*

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

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

Proof. Similar to [BEM+23], we can write the state of the verifiers register, before they do the measurements in Step 2(a)ii as

$$\rho = (\Lambda\otimes\mathbb{1})(|C\rangle\langle C|^{\otimes m})\,,$$

where Λ denotes the channel that the prover applies to registers $\mathsf{B}_1\ldots\mathsf{B}_m$, and importantly the state ρ is permutation-invariant. We can imagine the process of sampling a m-bit string X by measuring each register $\mathsf{A}_i\mathsf{B}_i$ using the POVM $\{|D\rangle\langle D|, \mathbb{1}-|D\rangle\langle D|\}$ and writing down the answer as X_i. For a subset $S\subseteq[m]$ of size $\left(\kappa-\frac{1}{r}\right)m$, let the event E_S be the event that all of the bits X_i with $i\in S$ are 1, then we have the following

$$\begin{aligned}&\Pr\left[X_{i^*}=0 \;\middle|\; \sum_{i\neq i^*} X_i \ge \left(\gamma-\frac{\eta}{4\kappa r}\right)m\right]\\ &\quad= \frac{1}{m}\sum_{i^*}\mathop{\mathbb{E}}_{|S|=\left(\gamma-\frac{1}{r}\right)m}\left[\Pr\left[X_{i^*}=0|X_i=1\ \forall i\in S\right]\right]\\ &\quad= \left(1-\gamma+\frac{\eta}{4\kappa r}\right)+\frac{1}{m}\sum_{i^*}\mathop{\mathbb{E}}_{\substack{|S|=\left(\gamma-\frac{1}{r}\right)m\\ i^*\notin S}}\left[\Pr\left[X_{i^*}=0|X_i=1\ \forall i\in S\right]\right]\\ &\quad\le \left(1-\gamma+\frac{\eta}{4\kappa r}\right)+\frac{2}{m}\sum_{i^*}\mathop{\mathbb{E}}_{\substack{|S|=\left(\gamma-\frac{\eta}{4\kappa r}\right)m\\ i^*\notin S}}\left[\Pr\left[X_{i^*}=0\wedge X_i=1\ \forall i\in S\right]\right]\\ &\quad= \left(1-\gamma+\frac{\eta}{4\kappa r}\right)+\frac{2}{m}\mathop{\mathbb{E}}_{|S|=\left(\gamma-\frac{1}{r}\right)m}\left[\sum_{i^*\notin S}\Pr\left[X_{i^*}=0\wedge X_i=1\ \forall i\neq i^*\right]\right]\\ &\quad\le 1-\gamma+\frac{\eta}{4\kappa r}+\frac{2}{m}\\ &\quad\le 1-\gamma+\frac{\eta}{2\kappa r}\,.\end{aligned}$$

Here we use the fact that ρ is permutation-invariant to average over all permutations of the registers $\mathsf{A}_i\mathsf{B}_i$, then we use the fact that the probability of the verifier measuring a greater than $\gamma-\frac{\eta}{4\kappa r}$

fraction of accepts is at least 1/2, and finally we use the fact that when restricting to the variables in a fixed S, all of the events $X_{i^*} = 0 \wedge X_i = 1 \; \forall i \neq i^*$ are mutually exclusive, so their probabilities sum to 1. Finally we use the definition of m to upper bound $2/m$.

Thus, we have a bound on the probability of measuring the i^*'th register in the state $|D\rangle\langle D|$. Put another way, there exist a purification of the provers channel, R, and states $|\psi\rangle$ and $|\phi\rangle$ such that

$$|\langle D| \langle \phi| (\mathbb{1} \otimes R) |C\rangle |\psi\rangle|^2 \geq \gamma - \frac{\eta}{2\kappa r} .$$

Thus, by Theorem 1.6, we have that

$$\|\mathbb{1} \otimes (W - R) (W^* W \otimes |\psi\rangle\langle\psi|) |C\rangle |\psi\rangle \| \leq \frac{1}{r} .$$

Tracing out the registers used to purify the prover, we see that the verifier satisfies the soundness condition of a quantum interactive protocol for a distributional unitary synthesis problem. □

Theorem 5.3 (2-round quantum interactive protocol for DistUhlmann)**.** *For all γ, $\eta = 1/\mathrm{poly}(n)$ and $\kappa = \mathrm{poly}(r)$, there is a 2-round* avgUnitaryQIP *protocol with completeness error 2^{-n} and soundness $\frac{1}{2}$ for synthesizing instances of* $\textsc{DistUhlmann}_\gamma$ *with spectral gap η and obliqueness κ.*

Proof. Follows immediately from Lemma 5.1, Lemma 5.2, and the definition of Protocol 1. □

5.2 Stability of approximate representations

To demonstrate the flexibility and power of the robust rigidity theorem for Uhlmann transformations, we show how a stability theorem for approximate representations of groups arises from the robust rigidity of Uhlmann transformations. The proof draws inspiration from the proof of Gowers-Hatami theorem with non-uniform measures from [MNZ24], and similarly achieves a worse dimension blowup than the result of [GH15]. However, we believe that presenting the proof this way gives a framework for proving similar stability theorems, and highlights how the robust rigidity of Uhlmann transformations is a very general kind of stability theorem.

As a matter of notation, for a probability measure μ over a finite set S, we use the notation $g \sim \mu$ to describe sampling g from the distribution μ, and $h \sim S$ to denote h sampled uniformly at random from S.

Definition 5.4 (ϵ-approximate representation)**.** *Let G be a finite group, μ be a measure over G, and ρ be a quantum state on register* B*. A collection of unitaries $\{U_g\}_{g \in G}$ acting on* B *is an ϵ-approximate representation of G on $|\psi\rangle$ with measure μ if*

$$\mathop{\mathbb{E}}_{\substack{g \sim \mu \\ h \sim G}} \left[\|U_h U_g - U_{hg}\|_\rho^2 \right] \leq \epsilon ,$$

where $\|A\|_\rho = \sqrt{\mathrm{Tr}(A^* A \rho)}$.

Remark 5.5. The condition that $\{U_g\}_{g \in G}$ is an ϵ-approximate representation on the state ρ implies that for all purifications $|\psi\rangle$ of ρ, the following holds:

$$\mathop{\mathbb{E}}_{\substack{g \sim \mu \\ h \sim G}} \left[\mathrm{Re} \left(\langle\psi| \left(\mathbb{1} \otimes U_{hg}^* U_h U_g \right) |\psi\rangle \right) \right] \geq 1 - \epsilon/2 .$$

Our goal will be to prove that ϵ-approximate representations (in the sense of Definition 5.4) are close to exact representations, up to an isometry. Formally, we will prove the following theorem.

Theorem 5.6 (Stability of approximate representations)**.** *Let G be a finite group, μ be a measure over G, and ρ be a bipartite state on registers B. Let $\{U_g\}_{g\in G}$ be an ϵ-approximate representation of G on ρ over μ. Then there exists an exact representation of G, $\mathcal{R}$, and isometry V such that*

$$\mathop{\mathbb{E}}_{g\sim\mu}\left[\|U_g - V^*\mathcal{R}(g)V\|_\rho^2\right] \leq \epsilon\,.$$

To prove the theorem, we will exhibit a pair of states $|C\rangle$ and $|D\rangle$ such that the rigidity of the Uhlmann transformation between them implies the stability theorem. Let $\{U_g\}_{g\in G}$ be an approximate representation of a group G in the sense of Definition 5.4, and let $|\psi\rangle$ be a purification of ρ (for example $\mathbb{1}\otimes\sqrt{\rho}\,|\Omega\rangle$, although any purification will suffice). Then consider the following pair of states:

$$|C\rangle = \frac{1}{\sqrt{|G|}}\sum_{g,h\in G}\sqrt{\mu(g)}\,(\mathbb{1}\otimes U_g)\,|\psi\rangle_{\mathsf{AB}_1}\,|g\rangle_{\mathsf{B}_2}\,|h\rangle_{\mathsf{B}_3}\ ,$$
$$|D\rangle = \frac{1}{\sqrt{|G|}}\sum_{g,h\in G}\sqrt{\mu(g)}\,(\mathbb{1}\otimes U_{hg})\,|\psi\rangle_{\mathsf{AB}_1}\,|g\rangle_{\mathsf{B}_2}\,|h\rangle_{\mathsf{B}_3}\ .$$

To prove the stability theorem, we prove the following lemmas.

Lemma 5.7 (Uhlmann transformation for $|C\rangle$ and $|D\rangle$)**.** *The following transformation between $|C\rangle$ and $|D\rangle$ achieves the Uhlmann fidelity.*

$$\widetilde{W} = \sum_{g,h}\left(U_{hg}U_g^*\right)_{\mathsf{B}_1}\otimes|g,h\rangle\langle g,h|_{\mathsf{B}_2\mathsf{B}_3}\ .$$

Note that from Uhlmann's theorem, the reduced states on register A of $|C\rangle$ and $|D\rangle$ are identical. Furthermore, since the reduced states are the same, they commute with each other, and $\rho^{-1}\#\sigma$ is the projector onto their positive eigenspace, and all of its non-zero eigenvalues are 1. Therefore, both η and κ from Theorem 1.6 are 1. Further, if we let W be the *canonical* Uhlmann transformation[5], it is clear that $W^*W\,|C\rangle = |C\rangle$, because W^*W is a projector and W maps $|C\rangle$ to $|D\rangle$, implying $|C\rangle$ is in the image if W.

Next, we show that the approximate representation corresponds to an approximate Uhlmann transformation between $|C\rangle$ and $|D\rangle$.

Lemma 5.8. *Let $\{U_g\}$ is an ϵ-approximate representation of G under $|\psi\rangle$. Consider the following unitary*

$$U = \sum_h (U_h)_{\mathsf{B}_1}\otimes|h\rangle\langle h|_{\mathsf{B}_3}\ .$$

Then U achieves the following.

$$|\,\langle D|\,\mathbb{1}\otimes U\,|C\rangle\,| \geq 1-\frac{\epsilon}{2}\,.$$

[5]In general, $\widetilde{W}$ will not be the canonical Uhlmann transformation, since μ might not assign non-zero probability to all g. However in the case when μ is the uniform distribution, $\widetilde{W}$ is the canonical Uhlmann transformation between $|C\rangle$ and $|D\rangle$.

Finally, we show that the implication of the rigid robustness theorem corresponds exactly to being close to a specific exact representation of G.

Lemma 5.9. *Define the following representation $\mathcal{R}$ of G and an isometry V:*

$$\mathcal{R}(g) = \sum_h |h\rangle\langle hg| \quad \textit{and} \quad V = \frac{1}{\sqrt{|G|}} \sum_h (U_h)_{\mathsf{B}_1} \otimes |h\rangle_{\mathsf{B}_3} \ .$$

Then the following holds:

$$\|\mathbb{1} \otimes (U - \widetilde{W}) |C\rangle\|^2 = \mathop{\mathbb{E}}_{g\sim\mu} \left[\|U_g - V^*\mathcal{R}(g)V\|_\rho^2\right] \ .$$

Combining all of these, we have the following simple proof of Theorem 5.6.

Proof of Theorem 5.6. From Lemma 5.8, Lemma 5.7, and Theorem 1.6, together with the fact that $\eta = \kappa = 1$ in Theorem 1.6 for the states $|C\rangle$ and $|D\rangle$, we have that

$$\|\mathbb{1} \otimes (U - \widetilde{W}) |C\rangle\|^2 = \|\mathbb{1} \otimes (U - W)W^*W |C\rangle\|^2 \leq \epsilon \, .$$

Here, W is the canonical Uhlmann transformation, and we use the fact that, from the rigidity theorem, $\widetilde{W}$ is equal to W when restricted to the image of W. Then from Lemma 5.9, we have that

$$\mathop{\mathbb{E}}_{g\sim\mu} \left[\|U_g - V^*\mathcal{R}(g)V\|_\rho^2\right] \leq \epsilon \, ,$$

as desired. □

We now fill in the missing proofs.

Proof of Lemma 5.7. To prove the lemma, we apply the definition of $\widetilde{W}$.

$$\begin{aligned}
\widetilde{W} |C\rangle &= \widetilde{W} \left(\frac{1}{\sqrt{|G|}} \sum_{g,h\in G} \sqrt{\mu(g)} (\mathbb{1} \otimes U_g) |\psi\rangle_{\mathsf{AB}_1} |g\rangle_{\mathsf{B}_2} |h\rangle_{\mathsf{B}_3} \right) \\
&= \frac{1}{\sqrt{|G|}} \sum_{g,h\in G} \sqrt{\mu(g)} (\mathbb{1} \otimes U_{hg} U_g^* U_g) |\psi\rangle_{\mathsf{AB}_1} |g\rangle_{\mathsf{B}_2} |h\rangle_{\mathsf{B}_3} \\
&= \frac{1}{\sqrt{|G|}} \sum_{g,h\in G} \sqrt{\mu(g)} (\mathbb{1} \otimes U_{hg}) |\psi\rangle_{\mathsf{AB}_1} |g\rangle_{\mathsf{B}_2} |h\rangle_{\mathsf{B}_3} \\
&= |D\rangle \ .
\end{aligned}$$

□

Proof of Lemma 5.8. We can expand out the real component of the inner product between $|D\rangle$ and U applied to $|C\rangle$ as follows.

$$\begin{aligned}
\mathrm{Re}\left(\langle D| \mathbb{1} \otimes U |C\rangle\right) &= \frac{1}{|G|} \sum_{g,h\in G} \mu(g) \mathrm{Re}\left(\langle\psi| (\mathbb{1} \otimes U_{hg}^* U_h U_g) |\psi\rangle\right) \\
&= \mathop{\mathbb{E}}_{\substack{g\sim\mu \\ h\in G}} \left[\mathrm{Re}\left(\langle\psi| (\mathbb{1} \otimes U_{hg}^* U_h U_g) |\psi\rangle\right)\right] \\
&\geq 1 - \frac{\epsilon}{2} \, .
\end{aligned}$$

Here in the final line we use Remark 5.5 and the fact that $\{U_g\}_{g\in G}$ is an ϵ-approximate representation under $|\psi\rangle$. Since $|\langle D| \mathbb{1} \otimes U |C\rangle| \geq \mathrm{Re}(\langle D| \mathbb{1} \otimes U |C\rangle)$, this completes the proof. □

Proof of Lemma 5.9. We first note that

$$\begin{aligned} V^*\mathcal{R}(g)V &= \frac{1}{|G|}\sum_{h,h'} \left(U_h^* \otimes \langle h|\right) \mathcal{R}(g) \left(U_{h'} \otimes |h'\rangle\right) \\ &= \frac{1}{|G|}\sum_{h,h'} \left(U_h^* \otimes \langle hg|\right) \left(U_{h'} \otimes |h'\rangle\right) \\ &= \frac{1}{|G|}\sum_{h} U_h^* \cdot U_{hg}\,. \end{aligned}$$

We can interpret this as the convolution of the function $f(g) = U_g$ with itself. Here in the second to last line, we re-index the sum over h' by shifting every element by g. Note that if U_g was an exact representation of G, then we would have $U_h^* U_{hg} = U_h^* U_h U_g = U_g$.

Now to prove the lemma, we expand the definition of the 2-norm to get the following

$$\begin{aligned} &\|\mathbb{1} \otimes (U - \widetilde{W})\,|C\rangle\,\|^2 \\ &\quad= \langle C| \left(\mathbb{1} \otimes \left((U - \widetilde{W})^*(U - \widetilde{W})\right)\right) |C\rangle \\ &\quad= 2 - 2\mathrm{Re}\left(\langle C| \left(\mathbb{1} \otimes U^*\widetilde{W}\right) |C\rangle\right) \\ &\quad= 2 - \frac{2}{|G|}\sum_{g,g',h,h'} \sqrt{\mu(g)\mu(g')}\mathrm{Re}\left(\langle\psi|\,\langle g,h|\left(U_g^* \cdot U^* \cdot \widetilde{W} \cdot U_{g'}\right)|\psi\rangle\,|g',h'\rangle\right) \\ &\quad= 2 - \frac{2}{|G|}\sum_{g,g',h,h'} \sqrt{\mu(g)\mu(g')}\mathrm{Re}\left(\langle\psi|\,\langle g,h|\left(U_g^* \cdot U_h^* \cdot U_{h'g'}\right)|\psi\rangle\,|g',h'\rangle\right) \\ &\quad= 2 - \frac{2}{|G|}\sum_{g,h} \mu(g)\mathrm{Re}\left(\langle\psi|\,U_g^* \cdot U_h^* \cdot U_{hg}\,|\psi\rangle\right) \\ &\quad= 2 - 2\sum_{g} \mu(g)\mathrm{Re}\left(\langle\psi|\,U_g^* \cdot \left(\frac{1}{|G|}\sum_h U_h^* \cdot U_{hg}\right)|\psi\rangle\right) \\ &\quad= 2 - 2\sum_{g} \mu(g)\mathrm{Re}\left(\langle\psi|\,U_g^* \cdot (V^*\mathcal{R}(g)V)\,|\psi\rangle\right) \\ &\quad= \mathbb{E}_{g\sim\mu}\left[\|U_g - V^*\mathcal{R}(g)V\|_\rho^2\right]\,. \end{aligned}$$

Here we apply the definition on $\widetilde{W}$ and using the fact that Re is linear to move the sum over h inside, and using the definition to replacing $\sum_h U_h^* U_{hg}$ with $V^*\mathcal{R}(g)V$. □

Acknowledgments

JB and HY are supported by AFOSR award FA9550-23-1-0363, NSF CAREER award CCF-2144219, and the Sloan Foundation. TM acknowledges support from SNSF Grant No. 20QU-1_225171 and NCCR SwissMAP.

References

[BEM+23] John Bostanci, Yuval Efron, Tony Metger, Alexander Poremba, Luowen Qian, and Henry Yuen. "Unitary complexity and the Uhlmann transformation problem". In: *arXiv preprint arXiv:2306.13073* (2023) (cit. on pp. 1, 2, 5, 23–25).

[Bha09] Rajendra Bhatia. *Positive definite matrices*. Princeton University Press, 2009 (cit. on pp. 4, 8).

[BV04] Stephen Boyd and Lieven Vandenberghe. *Convex optimization*. Cambridge university press, 2004 (cit. on p. 8).

[CS20] Sam Cree and Jamie Sikora. "A fidelity measure for quantum states based on the matrix geometric mean". In: *arXiv preprint arXiv:2006.06918* (2020) (cit. on p. 4).

[FF21] Hamza Fawzi and Omar Fawzi. "Defining quantum divergences via convex optimization". In: *Quantum* 5 (2021), p. 387 (cit. on p. 4).

[GH15] William Timothy Gowers and Omid Hatami. "Inverse and stability theorems for approximate representations of finite groups". In: *arXiv preprint arXiv:1510.04085* (2015) (cit. on pp. 5, 26).

[Hig86] Nicholas J Higham. "Computing the polar decomposition – with applications". In: *SIAM Journal on Scientific and Statistical Computing* 7.4 (1986), pp. 1160–1174 (cit. on p. 6).

[JNV+21] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. "$\mathsf{MIP}^* = \mathsf{RE}$". In: *Communications of the ACM* 64.11 (2021), pp. 131–138 (cit. on p. 6).

[LWWZ24] Nana Liu, Qisheng Wang, Mark M Wilde, and Zhicheng Zhang. "Quantum algorithms for matrix geometric means". In: *arXiv preprint arXiv:2405.00673* (2024) (cit. on p. 4).

[MNZ24] Tony Metger, Anand Natarajan, and Tina Zhang. "Succinct arguments for QMA from standard assumptions via compiled nonlocal games". In: *2024 IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE. 2024, pp. 1193–1201 (cit. on pp. 5, 26).

[MS12] Carl A Miller and Yaoyun Shi. "Optimal robust quantum self-testing by binary nonlocal XOR games". In: *arXiv preprint arXiv:1207.1819* (2012) (cit. on p. 6).

[MY03] Dominic Mayers and Andrew Yao. "Self testing quantum apparatus". In: *arXiv preprint quant-ph/0307205* (2003) (cit. on pp. 2, 6).

[MY23] Tony Metger and Henry Yuen. "$\mathsf{stateQIP} = \mathsf{statePSPACE}$". In: *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE. 2023, pp. 1349–1356 (cit. on pp. 1, 2, 7).

[MYS12] Matthew McKague, Tzyh Haur Yang, and Valerio Scarani. "Robust self-testing of the singlet". In: *Journal of Physics A: Mathematical and Theoretical* 45.45 (2012), p. 455304 (cit. on pp. 2, 6).

[NY23] Ashwin Nayak and Henry Yuen. "Rigidity of superdense coding". In: *ACM Transactions on Quantum Computing* 4.4 (2023), pp. 1–39 (cit. on p. 2).

[RUV13] Ben W Reichardt, Falk Unger, and Umesh Vazirani. "Classical command of quantum systems". In: *Nature* 496.7446 (2013), pp. 456–460 (cit. on p. 6).

[ŠB20] Ivan Šupić and Joseph Bowles. "Self-testing of quantum systems: a review". In: *Quantum* 4 (2020), p. 337 (cit. on pp. 2, 6).

[Uhl76] Armin Uhlmann. "The "transition probability" in the state space of a $*$-algebra". In: *Reports on Mathematical Physics* 9.2 (1976), pp. 273–279 (cit. on p. 1).

[Ula60] Stanislaw M. Ulam. *A Collection of Mathematical Problems*. New York: Interscience Publishers, 1960, p. 150 (cit. on p. 5).

[Wat18] John Watrous. *The theory of quantum information*. Cambridge University Press, 2018 (cit. on pp. 8, 19).