Local transformations of bipartite entanglement are rigid

John Bostanci

Joint work with Tony Metger and Henry Yuen

Uhlmann transformations

Given two states $|C\rangle_{AB}$ and $|D\rangle_{AB}$, with reduced states on the A register ρ and σ, the following holds:

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

Uhlmann transformations

Given two states $|C\rangle_{\mathsf{AB}}$ and $|D\rangle_{\mathsf{AB}}$, with reduced states on the A register ρ and σ, the following holds:

$$\mathrm{F}(\rho, \sigma) = \max_{U} \langle D | \mathrm{id} \otimes U | C \rangle$$

In other words, the best you can map from $|C\rangle$ to $|D\rangle$, only touching the B register, is given by the fidelity of the reduced states on the A register.

Uhlmann transformations

Given two states $|C\rangle_{AB}$ and $|D\rangle_{AB}$, with reduced states on the A register ρ and σ, the following holds:

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

In other words, the best you can map from $|C\rangle$ to $|D\rangle$, only touching the B register, is given by the fidelity of the reduced states on the A register.

We call such a unitary U an Uhlmann transformation.

Why care about Uhlmann transformations?

They appear in many fields:

1. Optimal protocols for decoding quantum channels, compressing quantum information, entanglement distillation, state transfer, etc. all involve an Uhlmann transformation!

Why care about Uhlmann transformations?

They appear in many fields:

1. Optimal protocols for decoding quantum channels, compressing quantum information, entanglement distillation, state transfer, etc. all involve an Uhlmann transformation!

2. The hardness of Uhlmann transformations (for efficiently preparable states) is a necessary condition for cryptography to exist!

Why care about Uhlmann transformations?

They appear in many fields:

1. Optimal protocols for decoding quantum channels, compressing quantum information, entanglement distillation, state transfer, etc. all involve an Uhlmann transformation!

2. The hardness of Uhlmann transformations (for efficiently preparable states) is a necessary condition for cryptography to exist! [Yan22]

3. They characterize interesting complexity classes like the class of zero-knowledge provable unitaries, and the class of unitaries that can be implemented with the help of interaction with an all-powerful prover. [BEM+23]

Why care about Uhlmann transformations?

They appear in many fields:

1. Optimal protocols for decoding quantum channels, compressing quantum information, entanglement distillation, state transfer, etc. all involve an Uhlmann transformation!

2. The hardness of Uhlmann transformations (for efficiently preparable states) is a necessary condition for cryptography to exist! [Yan22]

3. They characterize interesting complexity classes like the class of zero-knowledge provable unitaries, and the class of unitaries that can be implemented with the help of interaction with an all-powerful prover. [BEM+23]

4. Studying them will have interesting connections to math too! (Foreshadowing)

The canonical Uhlmann transformation

In general, there could be many Uhlmann transformations for a pair of states (e.g., that differ off of the support of $|C\rangle$. But there is a way to define a canonical isometry:

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

The canonical Uhlmann transformation

In general, there could be many Uhlmann transformations for a pair of states (e.g., that differ off of the support of $|C\rangle$. But there is a way to define a canonical isometry:

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

It is known that two different Uhlmann transformations of the same pair of states must look the same on the support of W! [BEM+23]

Approximate Uhlmann transforms

Say you found a unitary U such that:

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

Approximate Uhlmann transforms

Say you found a unitary U such that:

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

Can you say that this U is "close" to an Uhlmann transformation in some sense?

Approximate Uhlmann transforms

Say you found a unitary U such that:

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

Can you say that this U is "close" to an Uhlmann transformation in some sense?

Our answer: Yes, up to some parameters!

Rigidity of Uhlmann transformations

Theorem: Let $|C\rangle_{\mathsf{AB}}, |D\rangle_{\mathsf{AB}}$ be two quantum states with reduced on A ρ, σ. Then for all unitaries U such that

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

There is a function $\delta(\,\cdot\,)$ such that

$$\left\| \, \mathrm{id} \otimes (W - U) W^* W | C \rangle \, \right\|^2 \leq \delta(\epsilon) \,.$$

Rigidity of Uhlmann transformations

Theorem: Let $|C\rangle_{\mathsf{AB}}, |D\rangle_{\mathsf{AB}}$ be two quantum states with reduced on A ρ, σ. Then for all unitaries U such that

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

There is a function $\delta(\,\cdot\,)$ such that

$$\left\| \, \mathrm{id} \otimes (W - U) W^* W | C \rangle \, \right\|^2 \leq \delta(\epsilon) \,.$$

Here, $\delta(\epsilon) = \left(\frac{2\kappa}{\eta}\right) \cdot \epsilon$, depends on the following properties of the states $|C\rangle, |D\rangle$:

$$\kappa = \left\| \rho^{-1/2} \cdot \mathrm{Image}(\rho^{1/2}\sigma\rho^{1/2}) \cdot \rho^{1/2} \right\|_{\mathrm{op}}^2 \quad \text{and} \quad \eta = \lambda_{\min}(\rho^{-1}\#\sigma) \,.$$

Rigidity of Uhlmann transformations

Theorem: Let $|C\rangle_{\mathsf{AB}}, |D\rangle_{\mathsf{AB}}$ be two quantum states with reduced on A ρ, σ. Then for all unitaries U such that

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

There is a function $\delta(\,\cdot\,)$ such that

$$\left\| \, \mathrm{id} \otimes (W - U) W^* W | C \rangle \, \right\|^2 \leq \delta(\epsilon) \,.$$

Here, $\delta(\epsilon) = \left(\frac{2\kappa}{\eta}\right) \cdot \epsilon$, depends on the following properties of the states $|C\rangle, |D\rangle$:

$$\kappa = \left\| \rho^{-1/2} \cdot \mathrm{Image}(\rho^{1/2} \sigma \rho^{1/2}) \cdot \rho^{1/2} \right\|_{\mathrm{op}}^2 \quad \text{and} \quad \eta = \lambda_{\min}(\rho^{-1} \# \sigma) \,.$$

Matrix geometric mean: $A \# B = A^{1/2} \cdot (A^{-1/2} B A^{-1/2})^{1/2} \cdot A^{1/2}$

Proof Sketch

Let's think about the theorem statement as a maximization problem:

$$\text{Maximize over U: } \left\| \text{id} \otimes (W - U)W^*W \,|\, C\rangle \right\|^2 .$$

$$\text{Subject to: } \langle D \,|\, \text{id} \otimes U \,|\, C\rangle = \mathrm{F}(\rho, \sigma) - \epsilon ,$$

$$U^*U = \text{id} .$$

Proof Sketch

Let's think about the theorem statement as a maximization problem:

$$\text{Maximize over U:} \ \left\| \operatorname{id} \otimes (W - U) W^* W | C \rangle \right\|^2 .$$

$$\text{Subject to:} \ \langle D | \operatorname{id} \otimes U | C \rangle = \mathrm{F}(\rho, \sigma) - \epsilon ,$$

$$U^* U = \operatorname{id} .$$

Very high level game plan: Use semi-definite programming duality to upper bound this!

Proof Sketch

Let's think about the theorem statement as a maximization problem:

$$\text{Maximize over U: } \left\| \, \text{id} \otimes (W - U) W^* W \, | \, C \rangle \, \right\|^2 .$$

$$\text{Subject to: } \langle D \, | \, \text{id} \otimes U \, | \, C \rangle = \mathrm{F}(\rho, \sigma) - \epsilon \, ,$$

$$U^* U \leq \text{id} \, .$$

Very high level game plan: Use semi-definite programming duality to upper bound this!

Proof Sketch

Let's think about the theorem statement as a maximization problem:

$$\text{Maximize over U:} \ \left\| \, \mathrm{id} \otimes (W - U) W^* W \,|\, C \rangle \, \right\|^2 .$$

$$\text{Subject to:} \ \langle D \,|\, \mathrm{id} \otimes U \,|\, C \rangle = \mathrm{F}(\rho, \sigma) - \epsilon \, ,$$

$$U^* U = \mathrm{id} \, .$$

Very high level game plan: Use semi-definite programming duality to upper bound this!

Proof Sketch

For our constraint, we can write it in a more standard form as:

$$A = \sqrt{\sigma}\sqrt{\rho}$$

$$\langle D \,|\, \mathrm{id} \otimes U \,|\, C \rangle = \mathrm{Tr}\left(\sqrt{\sigma}U\sqrt{\rho}\right) = \mathrm{Tr}\left(U\sqrt{\rho}\sqrt{\sigma}\right)$$

Since we want this to be a real number, we can write this constraint as:

$$\frac{1}{2}\left(\mathrm{Tr}\,(UA^*) + \mathrm{Tr}(U^*A)\right) \; .$$

Proof Sketch

Let's think about the theorem statement as a maximization problem:

$$\text{Maximize over U: } \left\| \mathrm{id} \otimes (W - U)W^*W \,|\, C\rangle \right\|^2 .$$

$$\text{Subject to: } \frac{1}{2}\left(\mathrm{Tr}\,(UA^*) + \mathrm{Tr}(U^*A)\right) = \mathrm{F}(\rho, \sigma) - \epsilon \,,$$

$$U^*U = \mathrm{id}\,.$$

Very high level game plan: Use semi-definite programming duality to upper bound this!

Proof Sketch

For the objective, we can expand it out as:

$$
\begin{aligned}
\left\| \mathrm{id} \otimes (W-U)W^*W|C\rangle \right\|^2 &= \langle C|\mathrm{id} \otimes W^*W|C\rangle \\
&\quad + \langle C|\mathrm{id} \otimes (W^*WU^*UW^*W)|C\rangle \\
&\quad + 2\mathrm{Re}\langle C|\mathrm{id} \otimes (W^*WW^*UW^*W)|C\rangle \\
&\leq 2\mathrm{Tr}(W^*W\rho) - \left(\mathrm{Tr}(UW^*W\rho W^*) + \mathrm{Tr}(W\rho W^*WU)\right) .
\end{aligned}
$$

Proof Sketch

For the objective, we can expand it out as:

$$
\begin{aligned}
\left\| \, \mathrm{id} \otimes (W - U) W^* W | C \rangle \, \right\|^2 &= \langle C | \mathrm{id} \otimes W^* W | C \rangle \\
&\quad + \langle C | \mathrm{id} \otimes (W^* W U^* U W^* W) | C \rangle \\
&\quad + 2\mathrm{Re} \langle C | \mathrm{id} \otimes (W^* W W^* U W^* W) | C \rangle \\
&\le 2\mathrm{Tr}(W^* W \rho) - \left(\mathrm{Tr}(U W^* W \rho W^*) + \mathrm{Tr}(W \rho W^* W U) \right) \; .
\end{aligned}
$$

We will use the second term as the new objective function (since the first term does not depend on U).

Proof Sketch

Let's think about the theorem statement as a maximization problem:

$$\text{Maximize over U: } -\Big(\mathrm{Tr}(UW^*W\rho W^*) + \mathrm{Tr}(W\rho W^*WU)\Big)\ .$$

$$\text{Subject to: } \frac{1}{2}\Big(\mathrm{Tr}\,(UA^*) + \mathrm{Tr}(U^*A)\Big) = \mathrm{F}(\rho,\sigma) - \epsilon\,,$$

$$\begin{pmatrix} \mathrm{id} & U \\ U^* & \mathrm{id} \end{pmatrix} \geq 0\,.$$

Now, this can be transformed into a standard form semidefinite program.

Proof Sketch

The dual of the SDP is:

$$\text{Minimize over } Y_1, Y_2, \alpha\text{: } \operatorname{Tr}(Y_1) + \operatorname{Tr}(Y_2) + \alpha \left(\mathrm{F}(\rho, \sigma) - \epsilon\right)$$

$$\text{Subject to: } \begin{pmatrix} Y_1 & \frac{1}{2}\alpha A \\ \frac{1}{2}\alpha A^* & Y_2 \end{pmatrix} \geq \frac{1}{2} \begin{pmatrix} & -W\rho W^* W \\ -W^* W\rho W & \end{pmatrix}$$

$$Y = \begin{pmatrix} Y_1 & & \\ & Y_2 & \\ & & \alpha \end{pmatrix} \quad \text{Hermitian}$$

Proof Sketch

The dual of the SDP is:

$$\text{Minimize over } Y_1, Y_2, \alpha\text{: } \mathrm{Tr}(Y_1) + \mathrm{Tr}(Y_2) + \alpha\left(\mathrm{F}(\rho, \sigma) - \epsilon\right)$$

$$\text{Subject to: } \begin{pmatrix} Y_1 & \frac{1}{2}\alpha A \\ \frac{1}{2}\alpha A^* & Y_2 \end{pmatrix} \geq \frac{1}{2}\begin{pmatrix} & -W\rho W^*W \\ -W^*W\rho W & \end{pmatrix}$$

$$Y = \begin{pmatrix} Y_1 & & \\ & Y_2 & \\ & & \alpha \end{pmatrix} \quad \text{Hermitian}$$

If we find any feasible solution to this, we get an upper bound on the rigidity.

Proof Sketch

We are going to identify a nice matrix/choice of α to plug in. Define the following:

$$\alpha = -\kappa/\eta$$

$$T = \frac{1}{2}\left(\alpha A^* + P\rho W^*\right)$$

Then we plug in the following for Y_1, Y_2 and we get the answer we want.

$$Y_1 = \sqrt{T^*T}$$

$$Y_2 = T\left(\sqrt{T^*T}\right)^{-1} T^*$$

Dependence on parameters κ, η

Is the dependence on these numbers κ and η necessary? Yes, to some extent

Dependence on parameters κ, η

Is the dependence on these numbers κ and η necessary? Yes, to some extent

Theorem: For every η, there is a pair of states whose matrix geometric mean has smallest eigenvalue η, and there is a transformation that saturates the bound, i.e.

$$\|\mathrm{id} \otimes (W - U)W^*W \,|\, C\rangle\|^2 \geq 2\epsilon/\eta$$

Dependence on parameters κ, η

Is the dependence on these numbers κ and η necessary? Yes, to some extent

Theorem: For every η, there is a pair of states whose matrix geometric mean has smallest eigenvalue η, and there is a transformation that saturates the bound, i.e.

$$\|\mathrm{id} \otimes (W - U)W^*W \,|\, C\rangle\|^2 \geq 2\epsilon/\eta$$

Theorem: For every $\kappa \geq 1$ and all ϵ, there is a pair of states with $\eta \geq 1$ and $\kappa = \left\| \rho^{-1/2} \cdot \mathrm{Image}(\rho^{1/2}\sigma\rho^{1/2}) \cdot \rho^{1/2} \right\|_{\mathrm{op}}^2$ such that

$$\|\mathrm{id} \otimes (W - U)W^*W \,|\, C\rangle\|^2 \geq \kappa\epsilon^2$$

Uhlmann transformations for math

Our rigidity theorem seems to be a very general form of rigidity, it implies other well known stability theorems. Let's consider one such example!

Uhlmann transformations for math

Our rigidity theorem seems to be a very general form of rigidity, it implies other well known stability theorems. Let's consider one such example!

A representation of a group is a mapping from a group G to unitaries on some vector space. The representation satisfies $U_g U_h = U_{gh}$.

Uhlmann transformations for math

Our rigidity theorem seems to be a very general form of rigidity, it implies other well known stability theorems. Let's consider one such example!

A representation of a group is a mapping from a group G to unitaries on some vector space. The representation satisfies $U_g U_h = U_{gh}$.

An approximate representation is a collection of unitaries such that

$$\frac{1}{d}\mathbb{E}_{g,h}\left[\|U_g U_h - U_{gh}\|_1^2\right] \leq \epsilon$$

Uhlmann transformations for math

Given an ϵ-approximate representation, how close is it to a real representation? Let's consider the following pair of states:

$$|C\rangle = \frac{1}{|G|} \sum_{g,h \in G} \left(\mathrm{id} \otimes U_g \right) |\mathrm{EPR}\rangle_{\mathsf{AB}_1} |g\rangle_{\mathsf{B}_2} |h\rangle_{\mathsf{B}_3} ,$$

$$|D\rangle = \frac{1}{|G|} \sum_{g,h \in G} \left(\mathrm{id} \otimes U_{hg} \right) |\mathrm{EPR}\rangle_{\mathsf{AB}_1} |g\rangle_{\mathsf{B}_2} |h\rangle_{\mathsf{B}_3} .$$

Let's consider the Uhlmann transformations that act on the B register.

Uhlmann transformations for math

$$|C\rangle = \frac{1}{|G|} \sum_{g,h \in G} \left(\mathrm{id} \otimes U_g\right) |\mathrm{EPR}\rangle\, |g\rangle\, |h\rangle\,,$$

$$|D\rangle = \frac{1}{|G|} \sum_{g,h \in G} \left(\mathrm{id} \otimes U_{hg}\right) |\mathrm{EPR}\rangle\, |g\rangle\, |h\rangle\,.$$

The canonical Uhlmann transformation is:

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

An approximate one is:

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

Uhlmann transformations for math

Applying the rigidity theorem to these two unitaries:

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

Gives us the following: There exists an isometry V and exact representation R

$$\frac{1}{d}\mathbb{E}_g \left[\| U_g - V^* R(g) V \|_1^2 \right] \leq \epsilon$$

Next steps?

We proved a rigidity theorem for Uhlmann transformations, but open questions still remain.

1. Can we relate other notions of stability to Uhlmann transformations? For example, is CHSH rigidity a consequence of the rigidity of the Uhlmann transformation for some pair of states? What about general algebra's and non-local games?

2. There is a way to round states to nearby states so that η (the minimum eigenvalue of the matrix geometric mean) is well behaved, does the same exist for κ?

Next steps?

We proved a rigidity theorem for Uhlmann transformations, but open questions still remain.

1. Can we relate other notions of stability to Uhlmann transformations? For example, is CHSH rigidity a consequence of the rigidity of the Uhlmann transformation for some pair of states? What about general algebra's and non-local games?

2. There is a way to round states to nearby states so that η (the minimum eigenvalue of the matrix geometric mean) is well behaved, does the same exist for κ?

Thanks for listening!