A complete hierarchy of linear systems for certifying quantum entanglement of subspaces

Nathaniel Johnston¹



Benjamin Lovitz² Aravindan Vijayaraghavan³

- 1. Mount Allison University
- 2. NSF Postdoc, Northeastern University
 - 3. Northwestern University

QIP 2023

February 6, 2023



Northeastern University





<u>Problem</u>: Given a basis for a linear subspace $U \subseteq \mathbb{C}^d \otimes \mathbb{C}^d$, determine if U is entangled, i.e. if $U \cap X_{Sep} = \{0\}$.



Applications:

- Range criterion: For a density operator $\rho \in D(\mathbb{C}^d \otimes \mathbb{C}^d),$ $\operatorname{Im}(\rho)$ entangled $\Rightarrow \rho$ entangled
- Entangled subspaces can be used to construct entanglement witnesses and quantum error-correcting codes

<u>Problem</u>: Given a basis for a linear subspace $U \subseteq \mathbb{C}^d \otimes \mathbb{C}^d$, determine if U is entangled, i.e. if $U \cap X_{Sep} = \{0\}$.

X_{Sep}

Outline:

- Algorithm
- Complete hierarchy
- Extension to other notions of entanglement
- Robust generalization of hierarchy
- Extending symmetric extensions [DPS 04] to other notions of separability

<u>Problem</u>: Given a basis for a linear subspace $U \subseteq \mathbb{C}^d \otimes \mathbb{C}^d$, determine if U is entangled, i.e. if $U \cap X_{Sep} = \{0\}$.

[Buss et al 1999]: This is NP-Hard in the worst case.

[Barak et al 2019]: Best known algorithm takes $2^{\tilde{O}(\sqrt{d})}$ time.

[Classical AG, Parthasarathy 01]: $\dim(U) > (d-1)^2 \Rightarrow U$ is not entangled

U generic and $\dim(U) \leq (d-1)^2 \Rightarrow U$ is entangled

<u>Algorithm [JLV 22]</u>: Takes poly(*d*)-time and outputs either: "Hay in a haystack problem" 1. Fail, or

2. A certificate that *U* is entangled

Works-Extremely-Well Theorem [JLV 22]:

U generic and $\dim(U) \leq \frac{1}{4}(d-1)^2 \Rightarrow$ Algorithm outputs a certificate that U is entangled

<u>Problem</u>: Given a basis for a linear subspace $U \subseteq \mathbb{C}^d \otimes \mathbb{C}^d$, determine if U is entangled, i.e. if $U \cap X_{Sep} = \{0\}$.

[Buss et al 1999]: This is NP-Hard in the worst case.

[Barak et al 2019]: Best known algorithm takes $2^{\tilde{O}(\sqrt{d})}$ time.

[Classical AG, Parthasarathy 01]: dim $(U) > (d-1)^2 \Rightarrow U$ is not entangled

U generic and $\dim(U) \le (d-1)^2 \Rightarrow U$ is entangled

<u>Algorithm [JLV 22]</u>: Takes poly(*d*)-time and outputs either: "Hay in a haystack problem"

1. Fail, or

- 2. A certificate that *U* is entangled, or
- 3. A separable state $|\psi\rangle \otimes |\phi\rangle \in U$.

Works-Extremely-Well Theorem [JLV 22]:

[JLV 22]: WEW Theorem when U contains a generic planted separable state

U generic and $\dim(U) \leq \frac{1}{4}(d-1)^2 \Rightarrow$ Algorithm outputs a certificate that *U* is entangled

<u>Problem</u>: Given a basis for a linear subspace $U \subseteq \mathbb{C}^d \otimes \mathbb{C}^d$, determine if U is entangled, i.e. if $U \cap X_{Sep} = \{0\}$.

[Buss et al 1999]: This is NP-Hard in the worst case.

[Barak et al 2019]: Best known algorithm takes $2^{\tilde{O}(\sqrt{d})}$ time.

[Classical AG, Parthasarathy 01]: $\dim(U) > (d-1)^2 \Rightarrow U$ is not entangled

U generic and $\dim(U) \le (d-1)^2 \Rightarrow U$ is entangled

<u>Algorithm [JLV 22]</u>: Takes poly(*d*)-time and outputs either: "Hay in a haystack problem"

- 1. Fail, or
- 2. A certificate that *U* is entangled, or
- 3. A separable state $|\psi\rangle \otimes |\phi\rangle \in U$.

<u>Works-Extremely-Well Theorem [JLV 22]:</u> U generic and $\dim(U) < \frac{1}{2}(d-1)^2$

This talk: Focus on certification part of algorithm

[JLV 22]: WEW Theorem when *U*-contains a generic planted separable state

U generic and $\dim(U) \leq \frac{1}{4}(d-1)^2 \Rightarrow$ Algorithm outputs a certificate that *U* is entangled

The Algorithm

<u>Problem</u>: Given a basis for a linear subspace $U \subseteq \mathbb{C}^d \otimes \mathbb{C}^d$, determine if U is entangled, i.e. if $U \cap X_{Sep} = \{0\}$.

Idea: Problem is difficult because it's non-linear $(X_{\text{Sep}} \subseteq \mathbb{C}^d \otimes \mathbb{C}^d \text{ isn't a linear subspace}).$ <u>Make it linear</u>: Instead check if $U \cap \text{Span}(X_{\text{Sep}}) = \{0\}$. **Doesn't work:** Span $(X_{\text{Sep}}) = \mathbb{C}^d \otimes \mathbb{C}^d$. <u>Lift it up</u>: Let $X_{\text{Sep}}^2 = \text{Span}\{(|\psi\rangle \otimes |\phi\rangle)^{\otimes 2} : |\psi\rangle, |\phi\rangle \in \mathbb{C}^d\} = S^2(\mathbb{C}^d) \otimes S^2(\mathbb{C}^d)$ Check if $U^{\otimes 2} \cap X^2_{\text{Sep}} = \{0\}$. Works extremely well!

<u>Problem</u>: Given a basis for a linear subspace $U \subseteq \mathbb{C}^d \otimes \mathbb{C}^d$, determine if U is entangled, i.e. if $U \cap X_{Sep} = \{0\}$.

Let $X_{\text{Sep}}^2 = \text{Span}\{(|\psi\rangle \otimes |\phi\rangle)^{\otimes 2} : |\psi\rangle, |\phi\rangle \in \mathbb{C}^d\} = S^2(\mathbb{C}^d) \otimes S^2(\mathbb{C}^d)$

Algorithm:Takes poly(d) time to checkIf $U^{\otimes 2} \cap X_{\operatorname{Sep}}^2 = \{0\}$, output U is entangled Otherwise, output Fail

<u>Correctness</u>: $|\psi\rangle \otimes |\phi\rangle \in U \Rightarrow (|\psi\rangle \otimes |\phi\rangle)^{\otimes 2} \in U^{\otimes 2} \cap X_{\text{Sep}}^2$ \Rightarrow Algorithm outputs Fail.

Algorithm runtime to certify $U \cap X_{Sep} = \{0\}$

d	$\dim(U)$	time
3	3	0.01 s
4	8	0.03 s
5	13	0.08 s
6	20	0.20 s
7	29	0.49 s
8	39	1.06 s
9	50	2.24 s
10	63	5.56 s

From algorithm to complete hierarchy (based on Hilbert's Nullstellensatz)

<u>Problem</u>: Given a basis for a linear subspace $U \subseteq \mathbb{C}^d \otimes \mathbb{C}^d$, determine if U is entangled, i.e. if $U \cap X_{Sep} = \{0\}$.

Let $X_{\text{Sep}}^{k} = \text{Span}\{(|\psi\rangle \otimes |\phi\rangle)^{\otimes k} : |\psi\rangle, |\phi\rangle \in \mathbb{C}^{d}\} = S^{k}(\mathbb{C}^{d}) \otimes S^{k}(\mathbb{C}^{d})$

<u>Algorithm k:</u> If $U^{\otimes k} \cap X_{\text{Sep}}^k = \{0\}$, output U is entangled Otherwise, output Fail

Completeness [Hilbert]: For
$$k = 3^{d^2}$$
, Fail \Leftrightarrow U not entangled

Analogous hierarchies for other notions of entanglement



Let $X \subseteq \mathbb{C}^D$ be nice* (for example, $X = X_{\text{Sep}} \subseteq \mathbb{C}^d \otimes \mathbb{C}^d$) Think: "Some set of low entanglement" * *Any conic variety Problem: Given a basis for a linear subspace $U \subseteq \mathbb{C}^D$, determine if U avoids X, i.e. if $U \cap X = \{0\}$. Let $X^k = \text{Span}\{|\psi\rangle^{\otimes k} : |\psi\rangle \in X\}$ X Algorithm k: If $U^{\otimes k} \cap X^k = \{0\}$, output U avoids X Otherwise, output Fail

<u>Completeness [Hilbert]</u>: For $k = 2^{O(D)}$, Fail \Leftrightarrow U intersects X

<u>WEW Theorem [JLV 22]</u>: For generic U of dimension dim $(U) \leq \bigcirc$ Examples it holds that $U^{\otimes k} \cap X^k = \{0\}$ for k =Schmidt rank $\leq r$ states $\langle \Omega_{\mathcal{O}} \rangle = \Omega_r(d^2)$ $\frac{1}{2}$ = r + 1 $X_r = \{|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d : \text{Schmidt}-\text{rank}(|\psi\rangle) \leq r\}$ in- X_{Sep} -arable \leftrightarrow Completely entangled **Product states** $(\mathfrak{Q}) \sim (1/4) d^m$ $X_{\text{Sep}} = \{ |\psi_1\rangle \otimes \cdots \otimes |\psi_m\rangle : |\psi_i\rangle \in \mathbb{C}^d \}$ **Biseparable states** in- X_{B} -arable \leftrightarrow Genuinely entangled $(\bigcirc \mathcal{O}) \sim (1/4)d^m$ $X_B = \{ |\psi \rangle \in (\mathbb{C}^d)^{\otimes m} : \text{Some bipartition of } |\psi \rangle \text{ has rank 1} \}$ 溪=2 Slice rank 1 states $(20) \sim (1/4)d^m$ $X_S = \{|\psi\rangle \in (\mathbb{C}^n)^{\otimes m}$: Some 1 v.s. rest bipartition of $|\psi\rangle$ has rank 1} $\not\cong 2$ $\langle \mathfrak{Q}_{\mathcal{Q}} \rangle = \Omega_r(d^m)$ Matrix product states of bond dimension $\leq r$

 $X_S = \{|\psi\rangle \in (\mathbb{C}^n)^{\otimes m}$: Every left-right bipartition has rank $\leq r\}$

$$\underbrace{\underbrace{}}_{\underbrace{K}} = r + 1$$

<u>WEW Theorem [JLV 22]</u>: For generic U of dimension dim $(U) \leq \bigcirc$ Examples it holds that $U^{\otimes k} \cap X^k = \{0\}$ for k =Schmidt rank $\leq r$ states $\langle \Omega_{\mathcal{O}} \rangle = \Omega_r(d^2)$ $\frac{1}{2}$ = r + 1 $X_r = \{|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d : \text{Schmidt}-\text{rank}(|\psi\rangle) \leq r\}$ **Product states** in- X_{Sep} -arable \leftrightarrow Completely entangled $(\mathfrak{Q}) \sim (1/4) d^m$ **※**=2 $X_{\text{Sep}} = \{ |\psi_1\rangle \otimes \cdots \otimes |\psi_m\rangle : |\psi_i\rangle \in \mathbb{C}^d \}$ **Biseparable states** in- X_{B} -arable \leftrightarrow Genuinely entangled $\bigcirc \mathcal{O} \sim (1/4)d^m$ $X_B = \{ |\psi \rangle \in (\mathbb{C}^d)^{\otimes m} : \text{Some bipartition of } |\psi \rangle \text{ has rank 1} \}$ 溪=2 Takeaway: Algorithm certifies entanglement of subspaces Slice rank of dimension a constant multiple of the maximum possible $X_S = \{|\psi\rangle\}$ in polynomial time. Matrix product states of bond dimension $\leq r$ $\langle 0 \rho \rangle = \Omega_m(d^m)$

 $X_S = \{|\psi\rangle \in (\mathbb{C}^n)^{\otimes m}$: Every left-right bipartition has rank $\leq r\}$

$$\bigotimes_{r=r+1}^{\infty} = r+1$$

Robust generalization of the hierarchy

Robust generalization: Instead of determining whether U avoids X, Compute $h_X(U) \coloneqq \max_{|\psi\rangle \in X} \langle \psi | P_U | \psi \rangle$ $P_U = \operatorname{Proj}(U)$ U avoids $X \Leftrightarrow h_X(U) < 1$ <u>Theorem/Robust Hierarchy [JLV 23+]:</u> Let $X \subseteq \mathbb{C}^D$ be nice*, $U \subseteq \mathbb{C}^D$ linear, and $P_U = \operatorname{Proj}(U)$. For each k, let $\mu_k = \lambda_{\max} (P_X^k (P_U \otimes I^{\otimes k-1}) P_X^k) - P_X^k = \operatorname{Proj}(X^k)$ Then the μ_k form a non-increasing sequence converging to $h_X(U) \coloneqq \max_{|\psi\rangle \in X} \langle \psi | P_U | \psi \rangle$.

Robust generalization: Instead of determining whether U avoids X, Compute $h_X(U) \coloneqq \max_{|\psi\rangle \in X} \langle \psi | P_U | \psi \rangle$ $P_U = \operatorname{Proj}(U)$ U avoids $X \Leftrightarrow h_X(U) < 1$ <u>Theorem/Robust Hierarchy [JLV 23+]:</u> Let $X \subseteq \mathbb{C}^{D}$ be nice*, $W \in \text{Herm}(\mathbb{C}^{D})$ Hermitian. *Any conic variety For each k, let $\mu_{k} = \lambda_{\max}(P_{X}^{k}(W \otimes I^{\otimes k-1})P_{X}^{k}) - P_{X}^{k} = \text{Proj}(X^{k})$ Then the μ_{k} form a non-increasing sequence converging to $h_{X}(W) \coloneqq \max_{|\psi\rangle \in X} \langle \psi | W | \psi \rangle$.

Theorem/Robust Hierarchy not only holds for P_U , but for any Hermitian W!

Robust generalization:

Instead of determining whether U avoids X, Compute $h_X(U) \coloneqq \max_{|\psi\rangle \in X} \langle \psi | P_U | \psi \rangle$ $P_U = \operatorname{Proj}(U)$ U avoids $X \iff h_X(U) < 1$ Extending symmetric extensions to other notions of separability <u>Theorem/Robust Hierarchy [JLV 23+]:</u> Let $X \subseteq \mathbb{C}^{D}$ be nice*, $W \in \text{Herm}(\mathbb{C}^{D})$ Hermitian. *Any conic variety For each k, let $\mu_{k} = \lambda_{\max} (P_{X}^{k} (W \otimes I^{\otimes k-1}) P_{X}^{k}) - P_{X}^{k} = \text{Proj}(X^{k})$ Then the μ_{k} form a non-increasing sequence converging to $h_{X}(W) \coloneqq \max_{|\psi\rangle \in X} \langle \psi | W | \psi \rangle$.

<u>Definition</u>: A density operator $\rho \in D(\mathbb{C}^D)$ is *X*-arable if there exist $|\psi_1\rangle, \dots, |\psi_\ell\rangle \in X$ such that $\rho = \sum_{i=1}^{\ell} p_i |\psi_i\rangle \langle \psi_i|.$

<u>Example</u>: $\rho \in D(\mathbb{C}^d \otimes \mathbb{C}^d)$ is X_{Sep} -arable $\Leftrightarrow \rho$ is separable.

<u>Theorem/Robust Hierarchy [JLV 23+]:</u> Let $X \subseteq \mathbb{C}^D$ be nice*, $W \in \text{Herm}(\mathbb{C}^D)$ Hermitian. For each k, let $\mu_k = \lambda_{\max} (P_X^k (W \otimes I^{\otimes k-1}) P_X^k) - P_X^k = \text{Proj}(X^k)$ Then the μ_k form a non-increasing sequence converging to $h_X(W) \coloneqq \max_{|\psi\rangle \in X} \langle \psi | W | \psi \rangle$.

<u>Definition</u>: A density operator $\rho \in D(\mathbb{C}^D)$ is *X*-arable if there exist $|\psi_1\rangle, \dots, |\psi_\ell\rangle \in X$ such that $\rho = \sum_{i=1}^{\ell} p_i |\psi_i\rangle \langle \psi_i|.$

<u>Corollary [JLV 23+]</u>: ρ is X-arable \Leftrightarrow for all k there exists $\sigma \in D\left((\mathbb{C}^D)^{\otimes k}\right)$ such that $\operatorname{Tr}_{2,3,\dots,k}(\sigma) = \rho$ and $\operatorname{Im}(\sigma) \subseteq X^k = \operatorname{Span}\{|\psi\rangle^{\otimes k} : |\psi\rangle \in X\}$ " σ is an extension of ρ "

<u>Example (Symmetric extensions)</u> [DPS 04]: ρ is separable \Leftrightarrow For all k there exists an extension σ of ρ such that $\operatorname{Im}(\sigma) \subseteq X_{\operatorname{Sep}}^k = S^k(\mathbb{C}^d) \otimes S^k(\mathbb{C}^d)^{4}$ Symmetric

<u>Theorem/Robust Hierarchy [JLV 23+]:</u> Let $X \subseteq \mathbb{C}^{D}$ be nice*, $W \in \text{Herm}(\mathbb{C}^{D})$ Hermitian. *Any conic variety For each k, let $\mu_{k} = \lambda_{\max} (P_{X}^{k} (W \otimes I^{\otimes k-1}) P_{X}^{k}) - P_{X}^{k} = \text{Proj}(X^{k})$ Then the μ_{k} form a non-increasing sequence converging to $h_{X}(W) \coloneqq \max_{|\psi\rangle \in X} \langle \psi | W | \psi \rangle$.

<u>Definition</u>: A density operator $\rho \in D(\mathbb{C}^D)$ is *X*-arable if there exist $|\psi_1\rangle, \dots, |\psi_\ell\rangle \in X$ such that $\rho = \sum_{i=1}^{\ell} p_i |\psi_i\rangle \langle \psi_i|.$

 Examples $\frac{\text{Theorem [JLV 23+]:}}{\text{Im}(\sigma) \subseteq X^k} \xrightarrow{\text{Theorem [JLV 23+]:}} \rho X \text{-arable} \Leftrightarrow \forall k \exists \text{ extension } \sigma \text{ of } \rho \text{ s.t.}$ $\text{Im}(\sigma) \subseteq X^k = \text{Span}\{|\psi\rangle^{\otimes k} : |\psi\rangle \in X\}$

Schmidt rank $\leq r$ states [TMG 15] ρX_r -able $\Leftrightarrow \forall k \exists$ extension σ of ρ s.t. $X_r = \{|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d : SR(|\psi\rangle) \leq r\}$ Im $(\sigma) \subseteq S^k(\mathbb{C}^d \otimes \mathbb{C}^d) \cap \left(\left(\wedge^{r+1} (\mathbb{C}^d)^{\otimes 2}\right)^{\perp} \otimes (\mathbb{C}^d \otimes \mathbb{C}^d)^{\otimes k-r-1}\right)$

Product states [DPS 04]	ho separable	\Leftrightarrow	$\forall k \exists extension \sigma of \rho s.t.$
$X_{\text{Sep}} = \{ \psi_1\rangle \otimes \cdots \otimes \psi_m\rangle$	$\rangle: \psi_i\rangle \in \mathbb{C}^d\}$		$\mathrm{Im}(\sigma) \subseteq S^k(\mathbb{C}^d) \otimes \cdots \otimes S^k(\mathbb{C}^d)$
Biseparable states	ρ biseparable	\Leftrightarrow	$\forall k \exists extension \sigma of \rho s.t$

 $X_B = \{ |\psi\rangle \in (\mathbb{C}^d)^{\bigotimes m} : \operatorname{SR}(|\psi\rangle) = 1 \text{ in some cut} \} \qquad \operatorname{Im}(\sigma) \subseteq \sum_{T \subseteq [m]} S^k \left((\mathbb{C}^d)^{\otimes T} \right) \otimes S^k \left((\mathbb{C}^d)^{\otimes [m] - T} \right)$

Slice rank 1 states ρX_S -arable $\Leftrightarrow \forall k \exists \text{ extension } \sigma \text{ of } \rho \text{ s.t}$ $X_S = \{|\psi\rangle \in (\mathbb{C}^n)^{\otimes m} : \text{SR}(|\psi\rangle) = 1 \text{ in some 1 vs. rest} \quad \text{Im}(\sigma) \subseteq \sum_{i=1}^m S^k(\mathbb{C}^d) \otimes S^k((\mathbb{C}^d)^{\otimes m-1})$

. . .

MPS of bond dimension $\leq r \quad \rho X_{\text{MPS, }r}$ -arable $\Leftrightarrow \quad \forall k \exists \text{ extension } \sigma \text{ of } \rho \text{ s.t}$ $X_{\text{MPS, }r} = \{ |\psi \rangle \in (\mathbb{C}^n)^{\otimes m} : \text{Every L-R cut has SR} \leq r \}$ **Examples** $\frac{\text{Theorem}\left[J \downarrow V 23+\right]:}{\text{Im}(\sigma) \subseteq X^{k}} \xrightarrow{\text{Theorem}\left[J \downarrow V 23+\right]:} \rho X \text{-arable} \Leftrightarrow \forall k \exists \text{ extension } \sigma \text{ of } \rho \text{ s.t.}$ $\text{Im}(\sigma) \subseteq X^{k} = \text{Span}\{|\psi\rangle^{\otimes k}: |\psi\rangle \in X\}$

Schmidt rank $\leq r$ states [TMG 15] ρX_r -able $\Leftrightarrow \forall k \exists$ extension σ of ρ s.t. $X_r = \{|\psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d : SR(|\psi\rangle) \leq r\}$ Im $(\sigma) \subseteq S^k(\mathbb{C}^d \otimes \mathbb{C}^d) \cap \left(\left(\wedge^{r+1} (\mathbb{C}^d)^{\otimes 2}\right)^{\perp} \otimes (\mathbb{C}^d \otimes \mathbb{C}^d)^{\otimes k-r-1}\right)$



 $X_{\text{MPS}, r} = \{ |\psi\rangle \in (\mathbb{C}^n)^{\otimes m} : \text{Every L-R cut has SR} \leq r \}$

Conclusion



1. Complete hierarchies of linear systems to certify entanglement of a subspace. These work extremely well already at early levels.

Title: Complete hierarchy of linear systems for certifying quantum entanglement of subspaces

 (Briefly mentioned) poly-time algorithms to find low-entanglement elements of a subspace. These also work extremely well.

Title: Computing linear sections of varieties: quantum entanglement, tensor decompositions and beyond

3. Extending symmetric extensions: Separability testing hierarchy of [DPS 04] extended to hierarchies for Schmidt number, biseparability, and *X*-arability.

Title: TBD

A complete hierarchy of linear systems for certifying quantum entanglement of subspaces

Nathaniel Johnston¹



Benjamin Lovitz² Aravindan Vijayaraghavan³

- 1. Mount Allison University
- 2. NSF Postdoc, Northeastern University
 - 3. Northwestern University

QIP 2023

February 6, 2023



Northeastern University



