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

Nathaniel Johnston<sup>1</sup>



Benjamin Lovitz<sup>2</sup> Aravindan Vijayaraghavan<sup>3</sup>

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

WACT 2023

March 30, 2023



Northeastern University





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



**Applications:** Quantum Information

- Range criterion: For a density operator  $\rho \in D(\mathbb{C}^n \otimes \mathbb{C}^n),$  $\operatorname{Im}(\rho)$  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  $U \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ , determine if U is entangled, i.e. if  $U \cap X_{Sep} = \{0\}$ .

X<sub>Sep</sub>

#### Outline:

- 1. Algorithm (Nullstellensatz Certificate)
- 2. Algorithm to recover elements of  $U \cap X_{Sep}$ , with applications to tensor decompositions
  - 3. Generalization to arbitrary conic variety *X*
  - 4. Robust generalization of Hilbert's Nullstellensatz for this problem

<u>Problem</u>: Given a basis for a linear subspace  $U \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ , 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  $2^{\tilde{O}(\sqrt{n})}$  time.

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

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

<u>Algorithm (deg. 2 N.C.)</u>: Takes poly(*n*)-time and outputs either: "Hay in a haystack problem" 1. Fail, or

2. A certificate that *U* is entangled

<u>Problem</u>: Given a basis for a linear subspace  $U \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ , 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.

Works-Extremely-Well Theorem [JLV 22]:

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

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

<u>Algorithm (deg. 2 N.C.)</u>: Takes poly(n)-time and outputs either: "Hay in a haystack problem"

- 1. Fail, or
- 2. A certificate that *U* is entangled

The Algorithm (Nullstellensatz Certificate)

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

Idea: Problem is difficult because it's non-linear

 $(X_{\text{Sep}} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n \text{ isn't a linear subspace}).$ 

<u>Make it linear</u>: Instead check if  $U \cap \text{Span}(X_{\text{Sep}}) = \{0\}$ .

Works extremely well already for d = 2!

**Doesn't work:** Span $(X_{Sep}) = \mathbb{C}^n \otimes \mathbb{C}^n$ .

Lift it up: Let 
$$I(X_{\text{Sep}})_d^{\perp} = \text{Span}\{(u \otimes v)^{\otimes d}: u, v \in \mathbb{C}^n\} = S^d(\mathbb{C}^n) \otimes S^d(\mathbb{C}^n)$$

Check if 
$$S^d(U) \cap I(X_{\text{Sep}})_d^{\perp} = \{0\}.$$

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

Hilbert's Nullstellensatz:

 $U \cap X = \{0\} \iff$  For some  $d \in \mathbb{N}$  it holds that  $I(U)_d + I(X)_d = \mathbb{C}[x_{1,1}, \dots, x_{n,n}]_d$ 

Works extremely well already for d = 2! $I(X_{\text{Sep}})_{d}^{\perp} = \{(u \otimes v)^{\otimes d} : u, v \in \mathbb{C}^{n}\} = S^{d}(\mathbb{C}^{n}) \otimes S^{d}(\mathbb{C}^{n})$ 

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

$$I(X_{\text{Sep}})_{2}^{\perp} := \text{Span}\{(u \otimes v)^{\otimes 2} : u, v \in \mathbb{C}^{n}\} = S^{2}(\mathbb{C}^{n}) \otimes S^{2}(\mathbb{C}^{n})$$

Takes poly(*n*) time to check

Algorithm (2<sup>nd</sup> level of Nullstellensatz certificate): If  $S^2(U) \cap I(X_{\text{Sep}})_2^{\perp} = \{0\}$ , output U is entangled Otherwise, output Fail

<u>Correctness:</u>  $u \otimes v \in U \Rightarrow (u \otimes v)^{\otimes 2} \in S^2(U) \cap I(X_{\text{Sep}})_2^{\perp}$  $\Rightarrow$  Algorithm outputs Fail.

Problem: Given a basis for a linear subspace  $U \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ , determine if II is entangled i.e. if  $II \cap X_{\alpha} = \{0\}$ Works-Extremely-Well Theorem [JLV 22]: U generic and  $\dim(U) \leq \frac{1}{4}(n-1)^2 \Rightarrow S^2(U) \cap I(X_{\text{Sep}})_2^\perp = \{0\}.$ Takes poly(n) time to check Algorithm (2<sup>nd</sup> level of Nullstellensatz certificate): If  $S^2(U) \cap I(X_{\text{Sep}})_2^{\perp} \stackrel{\checkmark}{=} \{0\}$ , output U is entangled Otherwise, output Fail

<u>Correctness:</u>  $u \otimes v \in U \Rightarrow (u \otimes v)^{\otimes 2} \in S^2(U) \cap I(X_{\text{Sep}})_2^{\perp}$  $\Rightarrow$  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

Analogous hierarchies for other notions of entanglement (any conic variety) Let  $X \subseteq \mathbb{C}^N$  be any conic variety (for example,  $X = X_{Sep} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ )

X

<u>Problem</u>: Given a basis for a linear subspace  $U \subseteq \mathbb{C}^N$ , determine if U avoids X, i.e. if  $U \cap X = \{0\}$ . Let  $X \subseteq \mathbb{C}^N$  be any conic variety (for example,  $X = X_{\text{Sep}} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ )

<u>Problem</u>: Given a basis for a linear subspace  $U \subseteq \mathbb{C}^N$ , determine if U avoids X, i.e. if  $U \cap X = \{0\}$ .

$$I(X)_d^{\perp} := \operatorname{Span}\{v^{\otimes d}: v \in X\}$$

Algorithm d: If  $S^{d}(U) \cap I(X)_{d}^{\perp} = \{0\}$ , output U avoids XOtherwise, output Fail

$$= \{0\}.$$
 U  
X

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

Examples <u>WEW Theorem [JLV 22]</u> : For generic U it holds that $S^d(U) \cap I$	of dimension dim $(U) \le \bigcirc$ $(X)_d^{\perp} = \{0\}$ , for $d = \bigstar$
Schmidt rank $\leq r$ tensors $X_r = \{v \in \mathbb{C}^n \otimes \mathbb{C}^n : \text{Schmidt}-\text{rank}(v) \leq r\}$	
<b>Product tensors</b> in- $X_{Sep}$ -arable $\leftrightarrow$ Completely entangled $X_{Sep} = \{v_1 \otimes \cdots \otimes v_m : v_i \in \mathbb{C}^n\}$	$ \widehat{\bigcirc} \sim (1/4)n^m $
<b>Biseparable tensors</b> $X_B = \{v \in (\mathbb{C}^n)^{\bigotimes m} : \text{ Some bipartition of } v \text{ has rank 1} \}$	$ \widehat{\bigotimes} \sim (1/4)n^m $ $ \underset{}{\overset{}{}} = 2 $
Slice rank 1 tensors $X_S = \{v \in (\mathbb{C}^n)^{\otimes m} : \text{Some 1 v.s. rest bipartition of } v \text{ has rank 1} \}$	$ \widehat{\mathbb{K}} \sim (1/4)n^m $
Matrix product tensors of bond dimension $\leq r$ $X_{MPS} = \{v \in (\mathbb{C}^n)^{\otimes m} : \text{Every left-right bipartition has rank} \leq r\}$	

<u>WEW Theorem [JLV 22]</u>: For generic U of dimension dim $(U) \leq Q_{Q}$ Examples it holds that  $S^d(U) \cap I(X)_d^{\perp} = \{0\}$ , for  $d = \overset{\leftrightarrow}{\mathbb{R}}$ Schmidt rank  $\leq r$  tensors  $\langle \Omega_{\mathcal{O}} \rangle = \Omega_r(n^2)$  $\frac{1}{2}$  = r + 1 $X_r = \{v \in \mathbb{C}^n \otimes \mathbb{C}^n : \text{Schmidt}-\text{rank}(v) \le r\}$ **Product tensors** in- $X_{Sep}$ -arable  $\leftrightarrow$  Completely entangled  $(2) \sim (1/4)n^m$ 案=2  $X_{\text{Sep}} = \{v_1 \otimes \cdots \otimes v_m : v_i \in \mathbb{C}^n\}$ Bisepara Takeaway: Algorithm certifies entanglement of subspaces  $X_B = \{v \text{ of dimension a constant multiple of the maximum possible in polynomial time.} \}$  $n^m$ Slice rank 1 tensors  $X_{S} = \{v \in (\mathbb{C}^{n})^{\otimes m}: \text{Some 1 v.s. rest bipartition of } v \text{ has rank 1} \}$ Matrix product tensors of bond dimension  $\leq r$  $\langle \Omega_{r} \rangle = \Omega_{r}(n^{m})$  $X_{MPS} = \{v \in (\mathbb{C}^n)^{\otimes m} : \text{Every left-right bipartition has rank} \leq r\}$ = r + 1

Derksen's proof (sketch)

\*A slightly weaker WEW Theorem appears in [JLV 22] with a different proof.

<u>WEW Theorem [Derksen]\*:</u> If  $I \subseteq \mathbb{C}[x_1, \dots, x_N]$  is a homogeneous ideal and R is a non-negative integer such that

$$\dim I_d^\perp < \binom{N-R+d}{d},$$

then there exists an *R*-dimensional subspace  $U \subseteq \mathbb{C}^D$  such that  $S^d(U) \cap I_d^{\perp} = \{0\}$ .

*Proof sketch:* By a theorem of Galligo, after a linear change of coordinates wma  $J \coloneqq lm(I)$  is Borel-fixed with respect to the reverse lexicographic monomial order.

If  $x_R^d \notin J_d$ , then  $J_d \subseteq \langle x_1, ..., x_{R-1} \rangle_d$ . But then  $\dim(I_d^{\perp}) = \dim(J_d^{\perp})$   $\geq \dim(\mathbb{C}[x_1, ..., x_N]_d / \langle x_1, ..., x_{R-1} \rangle_d)$   $= \binom{N-R+d}{d}$ , a contradiction. So  $x_R^d \in J_d$ . But this implies all monomials in  $x_1, ..., x_R$  of degree d lie in J. It follows that  $S^d(U) \cap I_d^{\perp} = \{0\}$  for  $U = \operatorname{span}\{e_1, ..., e_R\}$ . Lifted Jennrich's algorithm to recover elements of  $U \cap X$ (with applications to tensor decompositions) Suppose  $U \subseteq \mathbb{C}^N$  has a basis  $\{v_1, \dots, v_R\}$  such that each  $v_i \in X$ .

<u>Problem</u>: Given some other basis  $\{u_1, \dots, u_R\}$  of U, recover  $\{v_1, \dots, v_R\}$  (up to scale).

Example: Jennrich's Algorithm: If  $U' \subseteq S^d(\mathbb{C}^N)$  is spanned by  $\{v_1^{\otimes d}, \dots, v_R^{\otimes d}\}$  with  $\{v_1, \dots, v_R\}$  linearly independent, then  $\{v_1^{\otimes d}, \dots, v_R^{\otimes d}\}$  can be recovered from any basis of U' in  $n^{O(d)}$ - time.

Lifted Jennrich's Algorithm [JLV 2022]: Run Jennrich on  $U' = S^d(U) \cap I(X)_d^{\perp}$ .

$$v^{\bigotimes d} \in U' \iff v \in U \cap X$$

For this to work, need:

1. 
$$\{v_1^{\otimes d}, \dots, v_R^{\otimes d}\}$$
 spans  $U'$ .

Generalizes FOOBI algorithm [DLCC '07]

2.  $\{v_1, \dots, v_R\}$  is linearly independent.

Suppose  $U \subseteq \mathbb{C}^N$  has a basis  $\{v_1, \dots, v_R\}$  such that each  $v_i \in X$ .

Works-Extremely-Well Theorem [JLV 22]:

Pro If  $d \ge 2, X$  is irreducible, cut out in degree d, and has no equations in degree d - 1, le). then (1) and (2) hold for generic  $v_1, ..., v_R \in X$  as long as  $R \le \frac{\dim(I(X)_d)}{d! \binom{N+d-1}{d}} (N+d-1)$ 

Example: Jennrich's Algorithm: If  $U' \subseteq S^{\alpha}(\mathbb{C}^n)$  is spanned by  $\{v_1, \dots, v_R^{\otimes n}\}$  with  $\{v_1, \dots, v_R\}$  linearly independent, then  $\{v_1^{\otimes d}, \dots, v_R^{\otimes d}\}$  can be recovered from any basis of U' in  $n^{O(d)}$ - time.

Lifted Jennrich's Algorithm [JLV 2022]: Run Jennrich on  $U' = S^d(U) \cap I(X)_d^{\perp}$ .

$$v^{\bigotimes d} \in U' \iff v \in U \cap X$$

For this to work, need:

1. 
$$\{v_1^{\otimes d}, \dots, v_R^{\otimes d}\}$$
 spans  $U'$ .

Generalizes FOOBI algorithm [DLCC '07]

2.  $\{v_1, \dots, v_R\}$  is linearly independent.

Suppose  $U \subseteq \mathbb{C}^N$  has a basis  $\{v_1, \dots, v_R\}$  such that each  $v_i \in X$ .

Lifted Jennrich's Algorithm [JLV 2022]: Run Jennrich on  $U' = S^d(U) \cap I(X)_d^{\perp}$ .

For this to work, need:

$$\frac{Compare with Derksen's result:}{S^d(U) \cap I(X)_d^{\perp}} = \{0\} \text{ for generic } v_1, \dots, v_R \in \mathbb{C}^N$$

1. 
$$\{v_1^{\otimes d}, \dots, v_R^{\otimes d}\}$$
 spans  $U'$ .

2.  $\{v_1, \dots, v_R\}$  is linearly independent. Q: Clean algebraic proof? Similar WEW Theorems were claimed in [DL 06, DLCC 07] for the special case  $X = X_{Sep}$ , but their proofs are incorrect.

le).

Application: 
$$(X, \mathbb{C}^k)$$
-decompositions  
For  $T \in V \otimes \mathbb{C}^k$ , an  $(X, \mathbb{C}^k)$ -decomposition is an expression  $T = \sum_{i=1}^R v_i \otimes z_i \in V \otimes \mathbb{C}^k$ 

where  $v_1, \ldots, v_R \in X$ 

rank<sub>X</sub>(*T*): = min{*R*: there exists an  $(X, \mathbb{C}^k)$ -decomposition of T of length R}

<u>Example</u>: When  $X = X_{Sep} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ , an  $(X, \mathbb{C}^k)$ -decomposition is just a tensor decomposition.

Viewing 
$$T$$
 as a map  $\mathbb{C}^k \to V$ , each  $v_i \in T(\mathbb{C}^k) \cap X$ ,  
so computing  $T(\mathbb{C}^k) \cap X \leftrightarrow (X, \mathbb{C}^k)$ -decomposing  $T$   
(Assuming that  $\{z_1, \dots, z_R\}$  is linearly independent)

<u>Corollary to WEW Theorem [JLV 22]</u>: A generic tensor  $T \in \mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^k$  with  $\operatorname{rank}(T) \leq \min\{\frac{1}{4}(n-1)^2, k\}$ 

has a unique rank decomposition, which is recovered in POLY(n)-time by applying our algorithm to  $T(\mathbb{C}^k)$ .

In particular, a generic  $n \times n \times n^2$  tensor of rank  $\sim \frac{1}{4}n^2$  is recovered by algorithm.

<u>Corollary to WEW Theorem [JLV 22]</u>: A generic tensor  $T \in \mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^k$  of  $(X_r, \mathbb{C}^k)$ -rank  $\operatorname{rank}_{X_r}(T) \leq \min\{\Omega_r(n^2), k\}$ 

has a unique tensor rank decomposition, which is recovered in  $n^{O(r)}$ -time by applying our algorithm to  $T(\mathbb{C}^k)$ .

 $T = \sum_{i} v_i \otimes w_i$ , where  $v_i \in X_r$ 

 $(X_r, \mathbb{C}^k)$ -rank  $\Leftrightarrow$  r-aided rank  $\Leftrightarrow$  (r, r, 1)-multilinear rank

<u>Corollary to WEW Theorem [JLV 22]</u>: A generic tensor

$$\in (\mathbb{C}^n)^{\otimes m}$$
 of tensor rank  
rank $(T) = O(n^{\lfloor m/2 \rfloor})$ 

has a unique tensor rank decomposition, which is recovered in  $n^{O(m)}$ -time by applying our algorithm to  $T\left((\mathbb{C}^n)^{\otimes \lfloor m/2 \rfloor}\right)$ .

(This is new when m is even. When m is odd you can just use Jennrich directly.)

Robust generalization of the entanglement certification hierarchy

#### **Robust generalization:**

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

Robust generalization:

Instead of determining whether U avoids X, Compute  $h_X(U) \coloneqq \max_{v \in X} \langle v, P_U v \rangle$   $\|v\| = 1$  V = Proj(U)U avoids  $X \Leftrightarrow h_X(U) < 1$   $\begin{array}{l} \underline{\text{Theorem/Robust Hierarchy [JLV 23+]:}}\\ \text{Let } X \subseteq \mathbb{C}^N \text{ be nice}^*, \quad W \in \text{Herm}(\mathbb{C}^N) \text{ Hermitian.} \\ & \text{*Any conic variety} \\ \text{For each } d, \text{ let } \mu_d = \lambda_{\max} \left( P_X^d \left( W \otimes I^{\otimes d-1} \right) P_X^d \right) \\ & -P_X^d = \text{Proj}(I(X)_d^{\perp}) \\ \text{Then the } \mu_d \text{ form a non-increasing sequence converging to } h_X(W) \coloneqq \max_{\substack{v \in X \\ \|v\|=1}} \langle v, Wv \rangle. \\ & \|v\|=1 \end{array}$ 

Robust generalization: Instead of determining whether U avoids X, Compute  $h_X(U) \coloneqq \max_{\substack{v \in X \\ \|v\|=1}} \langle v, P_U v \rangle$   $\|v\|=1$   $P_U = \operatorname{Proj}(U)$ U avoids  $X \iff h_X(U) < 1$  Theorem/Robust Hierarchy not only holds for  $P_U$ , but for any Hermitian W!

### 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

**2.** 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. Robust version** of certification hierarchies to compute the distance between a variety and a linear subspace.

Title: TBD

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

Nathaniel Johnston<sup>1</sup>



Benjamin Lovitz<sup>2</sup> Aravindan Vijayaraghavan<sup>3</sup>

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

WACT 2023

March 30, 2023



Northeastern University



