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

Nathaniel Johnston[1] Benjamin Lovitz[2] Aravindan Vijayaraghavan[3]

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

SIAM AG 2023

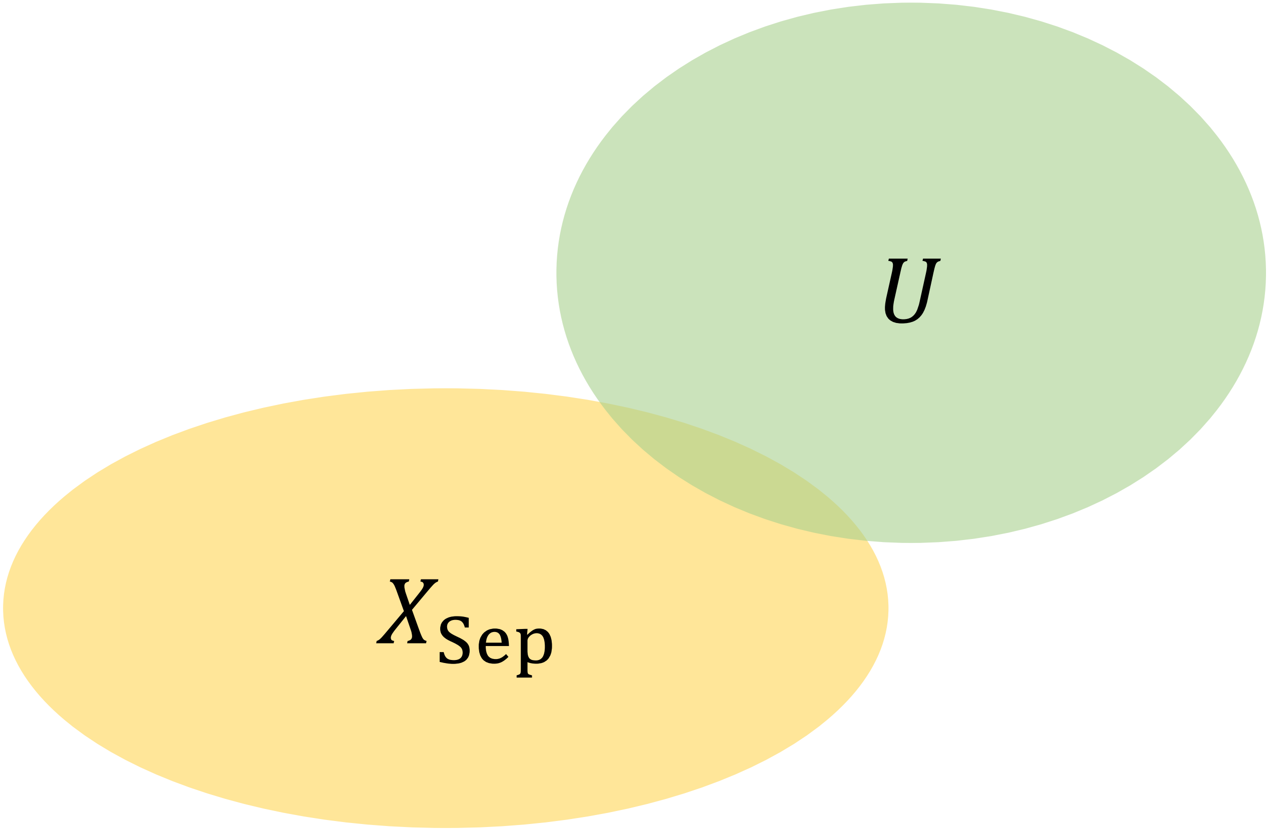
July 12, 2023

Northeastern University

Registration and travel support for this presentation was provided by the Society for Industrial and Applied Mathematics.

Product tensors: $X_{\text{Sep}} = \{u \otimes v : \; u, v \in \mathbb{C}^n\} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$

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

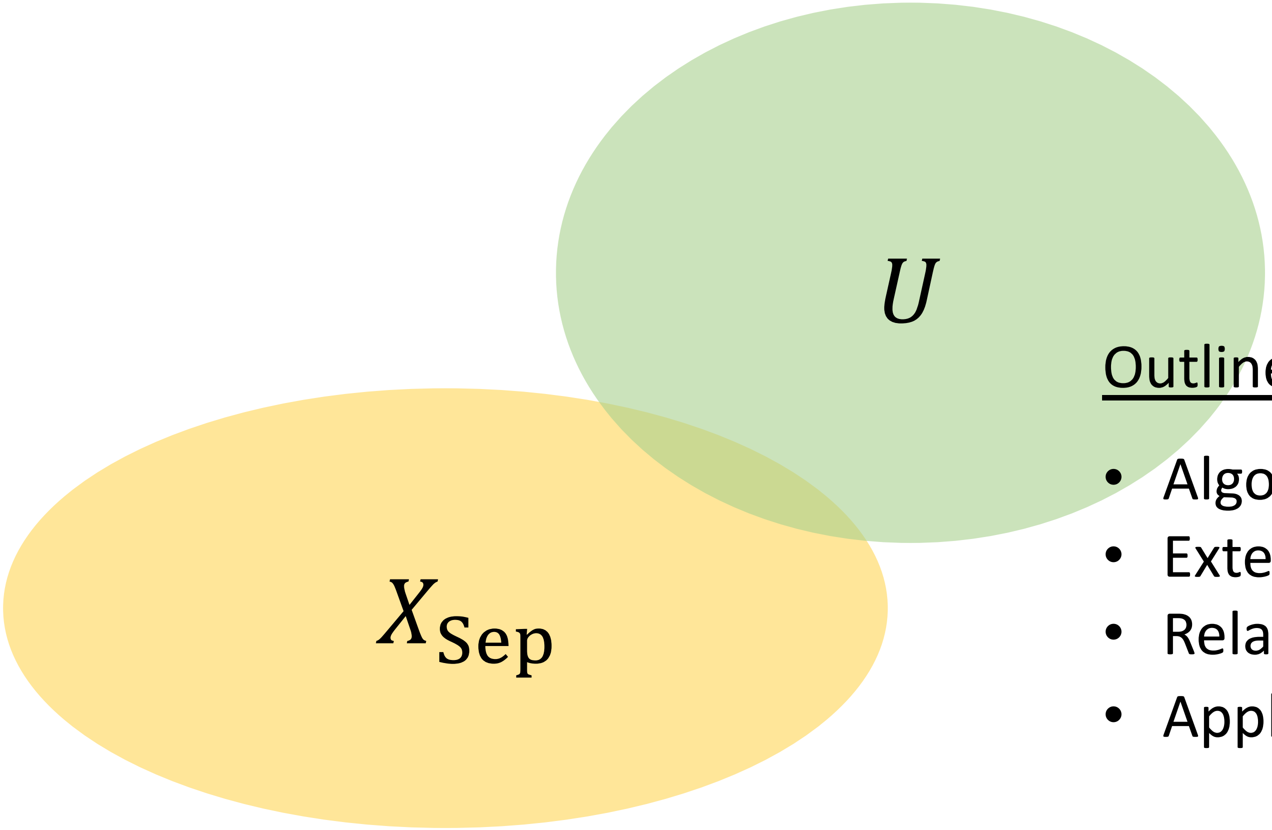


Applications: Quantum Information

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

Product tensors: $X_{\text{Sep}} = \{u \otimes v: \quad u, v \in \mathbb{C}^n\} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$

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



Outline:

- Algorithm + complete hierarchy (Nullstellensatz)
- Extension to other varieties X
- Related algorithm to recover elements of $U \cap X_{\text{Sep}}$
- Application to tensor decompositions

Product tensors: $X_{\mathrm{Sep}} = \{u \otimes v: \quad u, v \in \mathbb{C}^n\} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$

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

[Barak et al 2019]: 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]: $\dim(U) > (n-1)^2 \quad \Rightarrow \quad U$ is not entangled

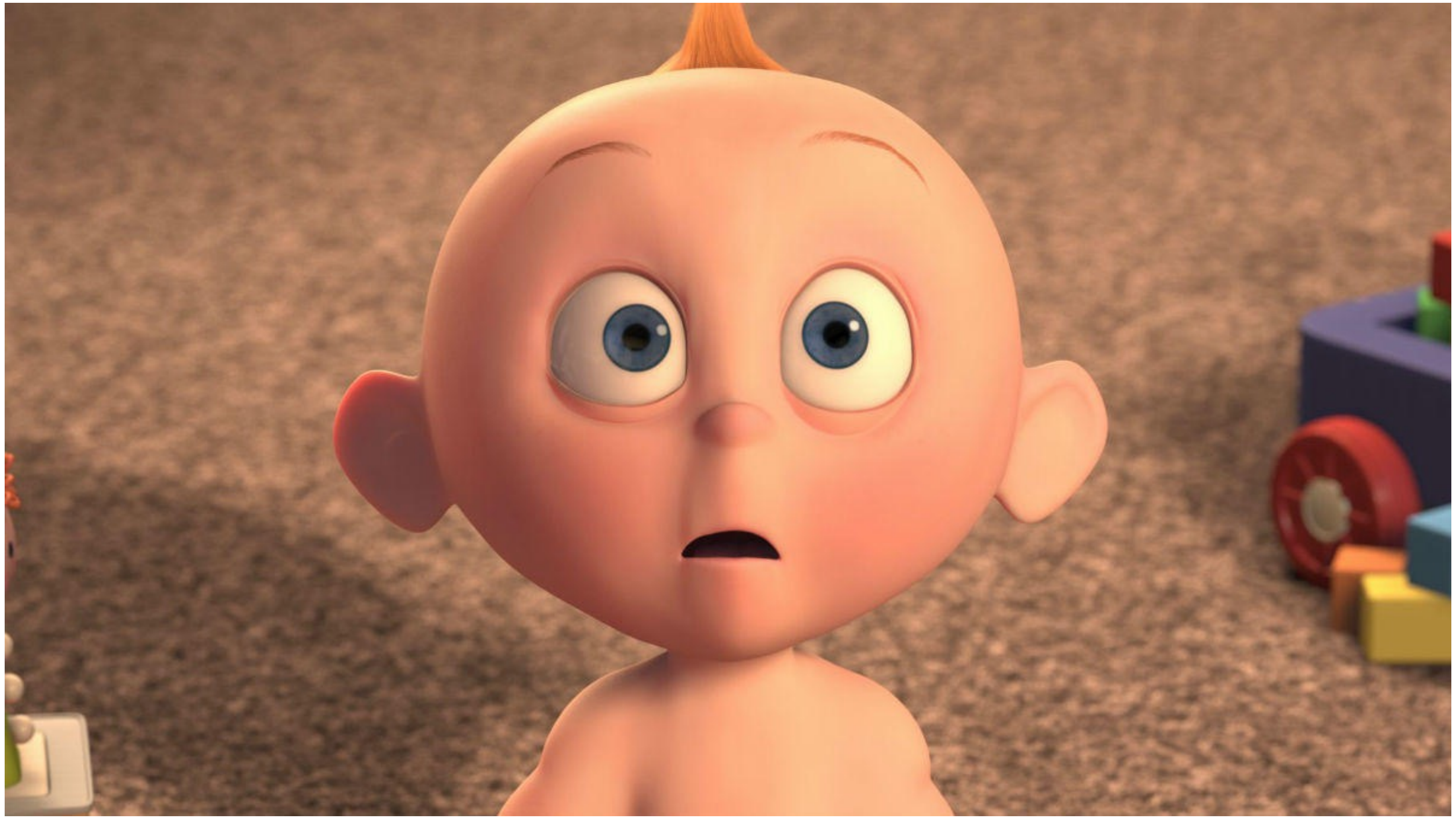
U generic and $\dim(U) \leq (n-1)^2 \quad \Rightarrow \quad U$ is entangled

"Hay in a haystack problem"

Outline:

- Algorithm + complete hierarchy (Nullstellensatz)
- Extension to other varieties X
- Related algorithm to recover elements of $U \cap X_{\mathrm{Sep}}$
- Applications to tensor decompositions

Algorithm for babies



Product tensors: $X_{\text{Sep}} = \{u \otimes v : \ u, v \in \mathbb{C}^n\} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$

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

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

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

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

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

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

Check if $U^{\otimes d} \cap X_{Sep}^d = \{0\}$.

Works extremely well already for $d = 2$!

Algorithm for adults

Product tensors: $X_{\text{Sep}} = \{u \otimes v: \quad u, v \in \mathbb{C}^n\} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$

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

Hilbert's Nullstellensatz:

$U \cap X = \{0\} \quad \Leftrightarrow \quad$ For some $d \in \mathbb{N}$ it holds that

$$I(U)_d + I(X_{Sep})_d = \mathbb{C}[x_{1,1}, \dots, x_{n,n}]_d$$

$$\Leftrightarrow$$

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

$I(X_{\text{Sep}})_d^{\perp} = X_{Sep}^d$

$$\Leftrightarrow$$

$$U^{\otimes d} \cap X_{Sep}^d = \{0\}$$

Works extremely well already for $d = 2$!

Product tensors: $X_{\text{Sep}} = \{u \otimes v: \quad u, v \in \mathbb{C}^n\} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$

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

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

Takes poly(n) time to check

Algorithm:

If $U^{\otimes 2} \cap X_{\text{Sep}}^2 = \{0\}$, output U is entangled

Otherwise, output Fail

Correctness: $u \otimes v \in U \ \Rightarrow (u \otimes v)^{\otimes 2} \in U^{\otimes 2} \cap X_{\text{Sep}}^2$

$\Rightarrow$ Algorithm outputs Fail.

Product tensors: $X_{\mathrm{Sep}} = \{u \otimes v: \quad u, v \in \mathbb{C}^n\} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$

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

Works-Extremely-Well Theorem [JLV 22]:
U generic and $\dim(U) \leq \frac{1}{4}(n-1)^2 \quad \Rightarrow \quad U^{\otimes 2} \cap X_{Sep}^2 = \{0\}$.

Takes poly(n) time to check

Algorithm:
If $U^{\otimes 2} \cap X_{\mathrm{Sep}}^2 = \{0\}$, output U is entangled
Otherwise, output Fail

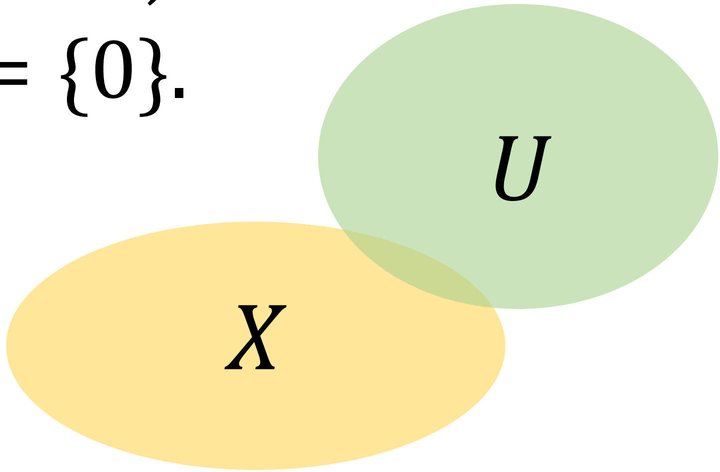
Correctness: $u \otimes v \in U \quad \Rightarrow (u \otimes v)^{\otimes 2} \in U^{\otimes 2} \cap X_{\mathrm{Sep}}^2$
$\Rightarrow$ Algorithm outputs Fail.

Outline:

- Algorithm + complete hierarchy (Nullstellensatz)
- Extension to other varieties X
- Related algorithm to recover elements of $U \cap X_{\mathrm{Sep}}$
- Applications to tensor decompositions

Let $X \subseteq \mathbb{C}^N$ be a conic variety (for example, $X = X_{\text{Sep}} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$)

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



$$X^d := \text{Span}\{v^{\otimes d} : \ v \in X\}$$

Algorithm d:

Takes $N^{O(d)}$ time to check

If $U^{\otimes d} \cap X^d = \{0\}$, output U avoids X

Otherwise, output Fail

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

Derksen's proof (sketch)

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

WEW Theorem [Derksen]*: 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 $U^{\otimes d} \cap I_d^\perp = \{0\}$.

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

If $x_R^d \notin J_d$, then $J_d \subseteq \langle x_1, \dots, x_{R-1} \rangle_d$. But then $\dim\left(I_d^\perp\right) = \dim\left(J_d^\perp\right)$

$$\geq \dim\left(\mathbb{C}[x_1, \dots, x_N]_d / \langle x_1, \dots, x_{R-1} \rangle_d\right)$$

$= \binom{N-R+d}{d}$, a contradiction.

So $x_R^d \in J_d$. But this implies all monomials in $x_1, \dots, x_R$ of degree d lie in J.

It follows that $S^d(U) \cap I_d^\perp = \{0\}$ for $U = \mathrm{span}\{e_1, \dots, e_R\}$. ∎

Examples

WEW Theorem [JLV 22]: For generic U of dimension $\dim(U) \leq$ 👽 it holds that $U^{\otimes d} \cap X^d = \{0\}$, for $d =$ 🐜

Schmidt rank $\leq r$ tensors

$X_r = \{v \in \mathbb{C}^n \otimes \mathbb{C}^n : \text{Schmidt−rank}(v) \leq r\}$

👽 $= \Omega_r(n^2)$
🐜 $= r + 1$

Product tensors in-X_{Sep}-arable ↔ Completely entangled

$X_{\text{Sep}} = \{v_1 \otimes \cdots \otimes v_m : v_i \in \mathbb{C}^n\}$

👽 $\sim(1/4)n^m$
🐜 $= 2$

Biseparable tensors in-X_B-arable ↔ Genuinely entangled

$X_B = \{v \in (\mathbb{C}^n)^{\otimes m}$: Some bipartition of v has rank 1$\}$

👽 $\sim(1/4)n^m$
🐜 $= 2$

Slice rank 1 tensors

$X_S = \{v \in (\mathbb{C}^n)^{\otimes m}$: Some 1 v.s. rest bipartition of v has rank 1$\}$

👽 $\sim(1/4)n^m$
🐜 $= 2$

Matrix product tensors of bond dimension $\leq r$

$X_{MPS} = \{v \in (\mathbb{C}^n)^{\otimes m}$: Every left-right bipartition has rank $\leq r\}$

👽 $= \Omega_r(n^m)$
🐜 $= r + 1$

Examples

WEW Theorem [JLV 22]: For generic U of dimension $\dim(U) \leq$ 👽 it holds that $U^{\otimes d} \cap X^d = \{0\}$, for $d =$ 🐜

Schmidt rank $\leq r$ tensors

$X_r = \{v \in \mathbb{C}^n \otimes \mathbb{C}^n : \text{Schmidt}-\text{rank}(v) \leq r\}$

👽 $= \Omega_r(n^2)$
🐜 $= r + 1$

Product tensors in-X_{Sep}-arable ↔ Completely entangled

$X_{\text{Sep}} = \{v_1 \otimes \cdots \otimes v_m : v_i \in \mathbb{C}^n\}$

👽 $\sim(1/4)n^m$
🐜 $= 2$

Bisepara

$X_B = \{v$

n^m

Takeaway: Algorithm certifies entanglement of subspaces of dimension a constant multiple of the maximum possible in polynomial time.

Slice rank 1 tensors

$X_S = \{v \in (\mathbb{C}^n)^{\otimes m}$: Some 1 v.s. rest bipartition of v has rank 1$\}$

👽 $\sim(1/4)n^m$
🐜 $= 2$

Matrix product tensors of bond dimension $\leq r$

$X_{MPS} = \{v \in (\mathbb{C}^n)^{\otimes m}$: Every left-right bipartition has rank $\leq r\}$

👽 $= \Omega_r(n^m)$
🐜 $= r + 1$

Outline:

- Algorithm + complete hierarchy (Nullstellensatz)
- Extension to other varieties X
- Related algorithm to recover elements of $U \cap X_{\mathrm{Sep}}$
- Applications to tensor decompositions

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

Problem: 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.

Jennrich's Algorithm:

Pick $T_j \in U'$, $j = 1,2$ at random, view these as maps $T_j : (\mathbb{C}^N)^{\otimes d-1} \to \mathbb{C}^N$

$$T_j = \sum_{i=1}^R \alpha_{j,i} v_i \left(v_i^t\right)^{\otimes d-1} \qquad T_j^{-1} = \sum_i \frac{1}{\alpha_{j,i}} (w_i)^{\otimes d-1} w_i^t \qquad \text{where } w_i^t v_{i'} = \delta_{i,i'}$$

So $T_1 T_2^{-1} = \sum_i \frac{\alpha_{1,i}}{\alpha_{2,i}} v_i w_i^t$. E-vectors / E-values of $T_1 T_2^{-1}$ are v_i , $\frac{\alpha_{1,i}}{\alpha_{2,i}}$ ← Distinct for different i

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

Pro ... le).

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 $U' = U^{\otimes d} \cap X^d$.

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

Generalizes FOOBI algorithm [DLCC '07]

For this to work, need:

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

Pro

le).

Exa

$\{v_1$

y

bas

Works-Extremely-Well Theorem [JLV 22]:

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

Proof technique: Show that

$$I(X)_d + I(U)_d = I(v_1, \dots, v_R)_d$$

for generic $v_1, \dots, v_R \in X$. This is equivalent to (1).

Lifted Jennrich's Algorithm [JLV 2022]: Run Jennrich on $U' = U^{\otimes d} \cap X^d$.

Compare with earlier result:

$I(X)_d + I(U)_d = S^d(\mathbb{C}^N)$ for generic $v_1, \dots, v_R \in \mathbb{C}^N$

For this to work, need:

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 $X = X_{\text{Sep}}$, but their proofs are incorrect.

Outline:

- Algorithm + complete hierarchy (Nullstellensatz)
- Extension to other varieties X
- Related algorithm to recover elements of $U \cap X_{\mathrm{Sep}}$
- Applications to tensor decompositions

Application: (X, k)-decompositions

For $T \in V \otimes \mathbb{C}^k$, an (X, k)-decomposition is an expression

$$T = \sum_{i=1}^{R} v_i \otimes z_i \in V \otimes \mathbb{C}^k$$

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

<u>Example:</u> When $X = X_{\text{Sep}} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$, an (X, 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 $T(\mathbb{C}^k) \cap X \leftrightarrow (X, k)$-decomposing T

(Assuming that $\{z_1, \ldots, z_R\}$ is linearly independent)

Corollary to WEW Theorem [JLV 22]: 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.

Corollary to WEW Theorem [JLV 22]: A generic tensor $T \in (\mathbb{C}^n)^{\otimes m}$ of tensor rank

$$\mathrm{rank}(T) = O(n^{\lfloor m/2 \rfloor})$$

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.)

Corollary to WEW Theorem [JLV 22]: A generic tensor $T \in \mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^k$ of r-aided rank

$$\mathrm{r-aided\ rank}(X) \leq \min\{\Omega_r(n^2), k\}$$

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 $v_i \in X_r$

r-aided rank $\iff$ $(r, r, 1)$-multilinear rank

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. **(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

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

Nathaniel Johnston[1] Benjamin Lovitz[2] Aravindan Vijayaraghavan[3]

1. Mount Allison University

2. NSF Postdoc, Northeastern University

3. Northwestern University

SIAM AG 2023

July 12, 2023