Nullstellensatz-inspired algorithms for certifying entanglement of subspaces

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

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

University of Western Ontario

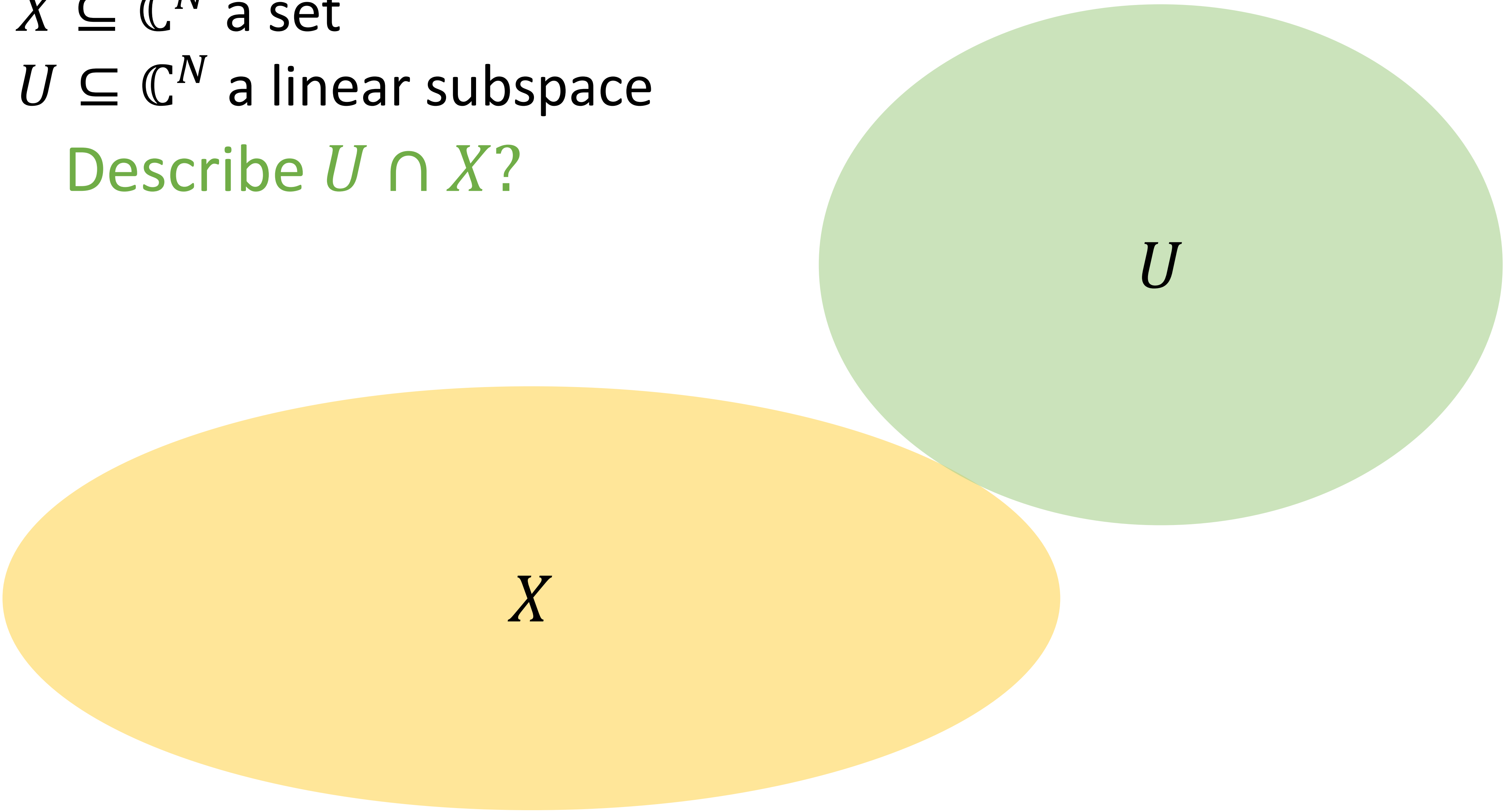
November 30, 2022

arXiv:2210.16389

$X \subseteq \mathbb{C}^N$ a set

$U \subseteq \mathbb{C}^N$ a linear subspace

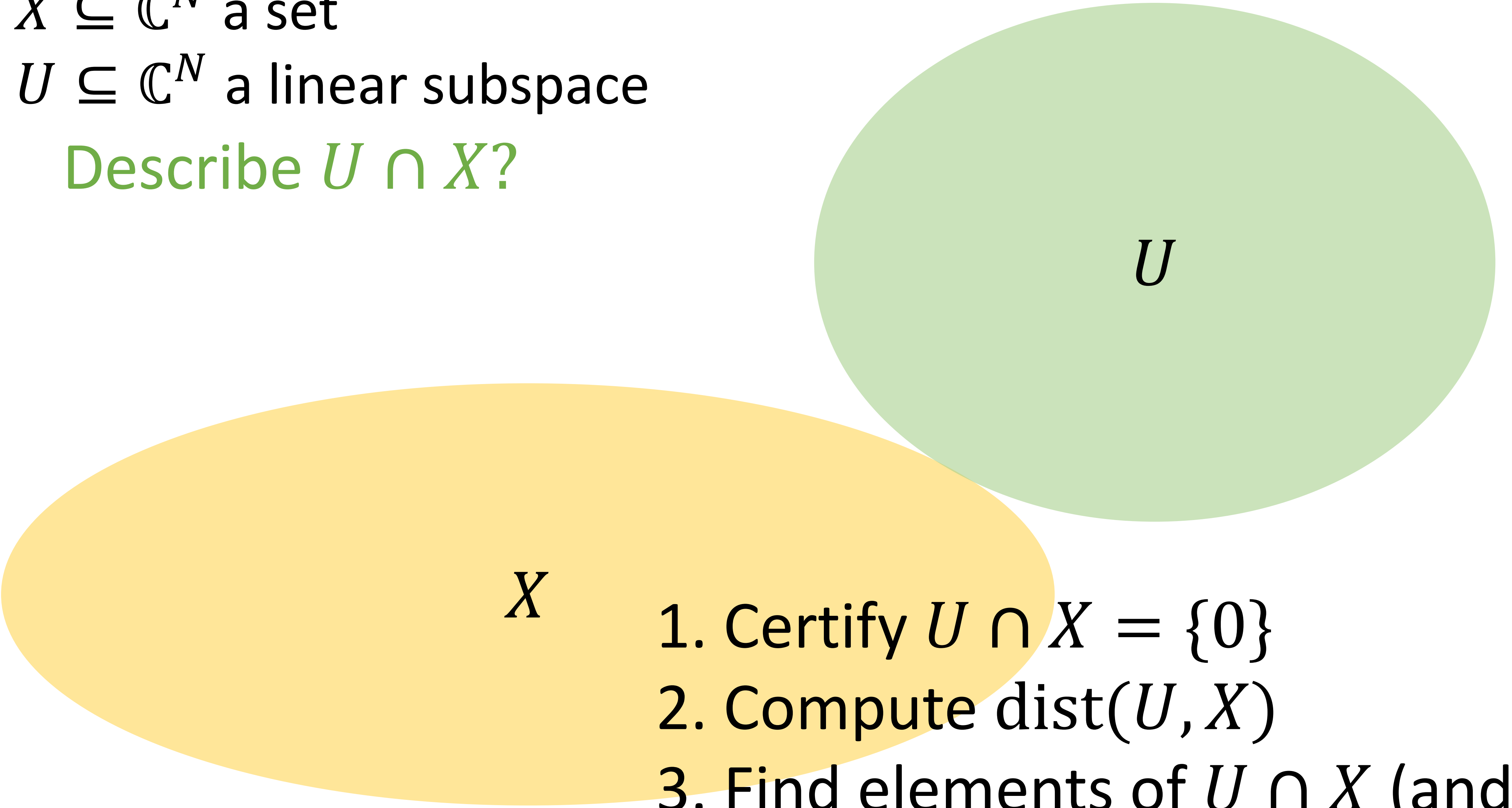
Describe $U \cap X$?



$X \subseteq \mathbb{C}^N$ a set

$U \subseteq \mathbb{C}^N$ a linear subspace

Describe $U \cap X$?

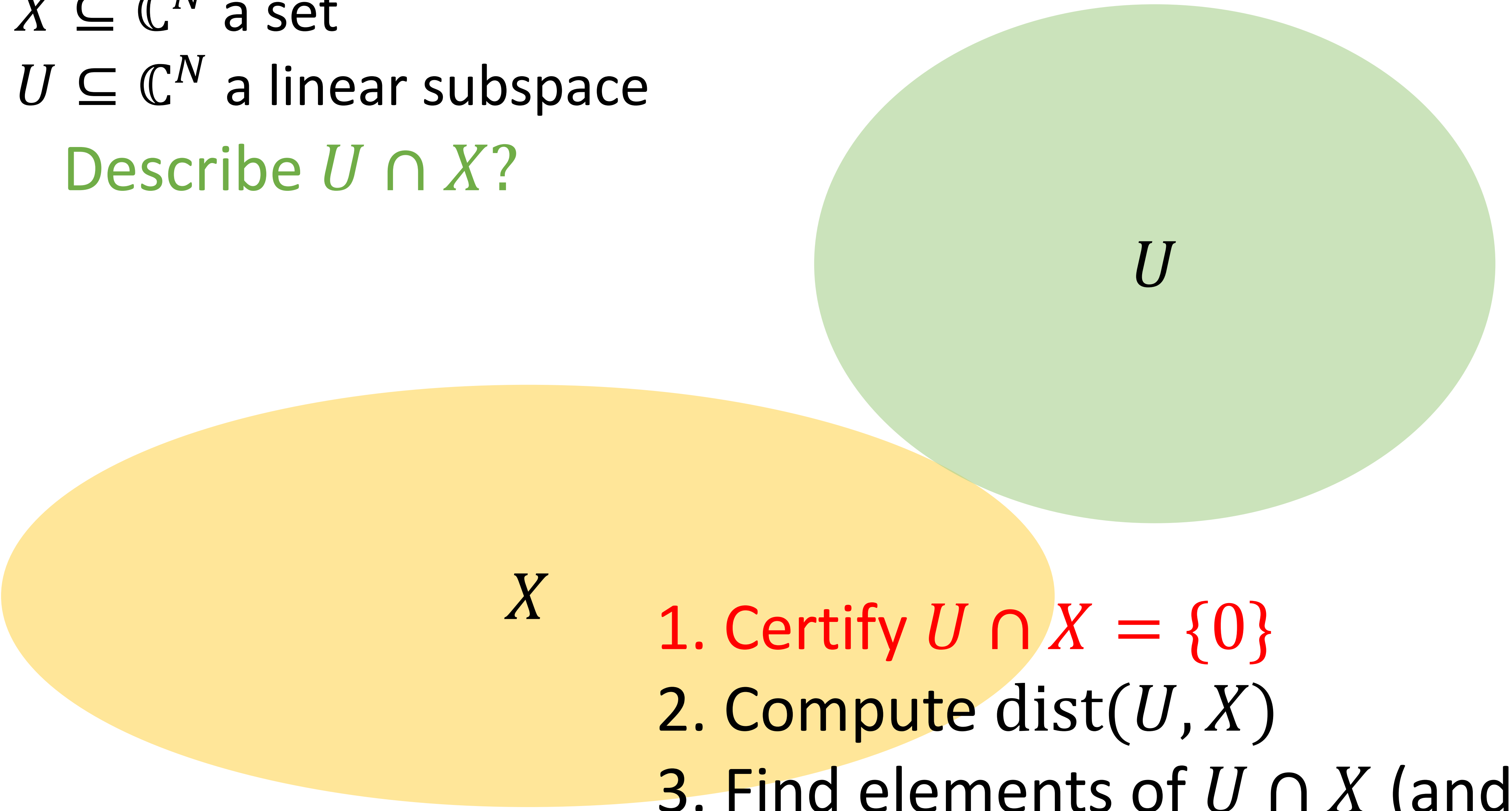


1. Certify $U \cap X = \{0\}$
2. Compute $\operatorname{dist}(U, X)$
3. Find elements of $U \cap X$ (and show that these are the only ones)

$X \subseteq \mathbb{C}^N$ a set

$U \subseteq \mathbb{C}^N$ a linear subspace

Describe $U \cap X$?



1. Certify $U \cap X = \{0\}$
2. Compute $\mathrm{dist}(U, X)$
3. Find elements of $U \cap X$ (and show that these are the only ones)

$X_1 = \{v \otimes w : v, w \in \mathbb{C}^n\} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$

Def: $U \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ is 1-entangled if $U \cap X_1 = \{0\}$.

Applications:

- A PVM $0 \le M \le I_{n^2}$ on $\mathbb{C}^n \otimes \mathbb{C}^n$ is an entanglement witness $\Leftrightarrow$ $\mathrm{Im}(M) \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ is 1-entangled

  $\mathrm{Tr}(M\rho) < 1$ for every separable state ρ

- For a density operator $\rho \in D(\mathbb{C}^n \otimes \mathbb{C}^n)$,

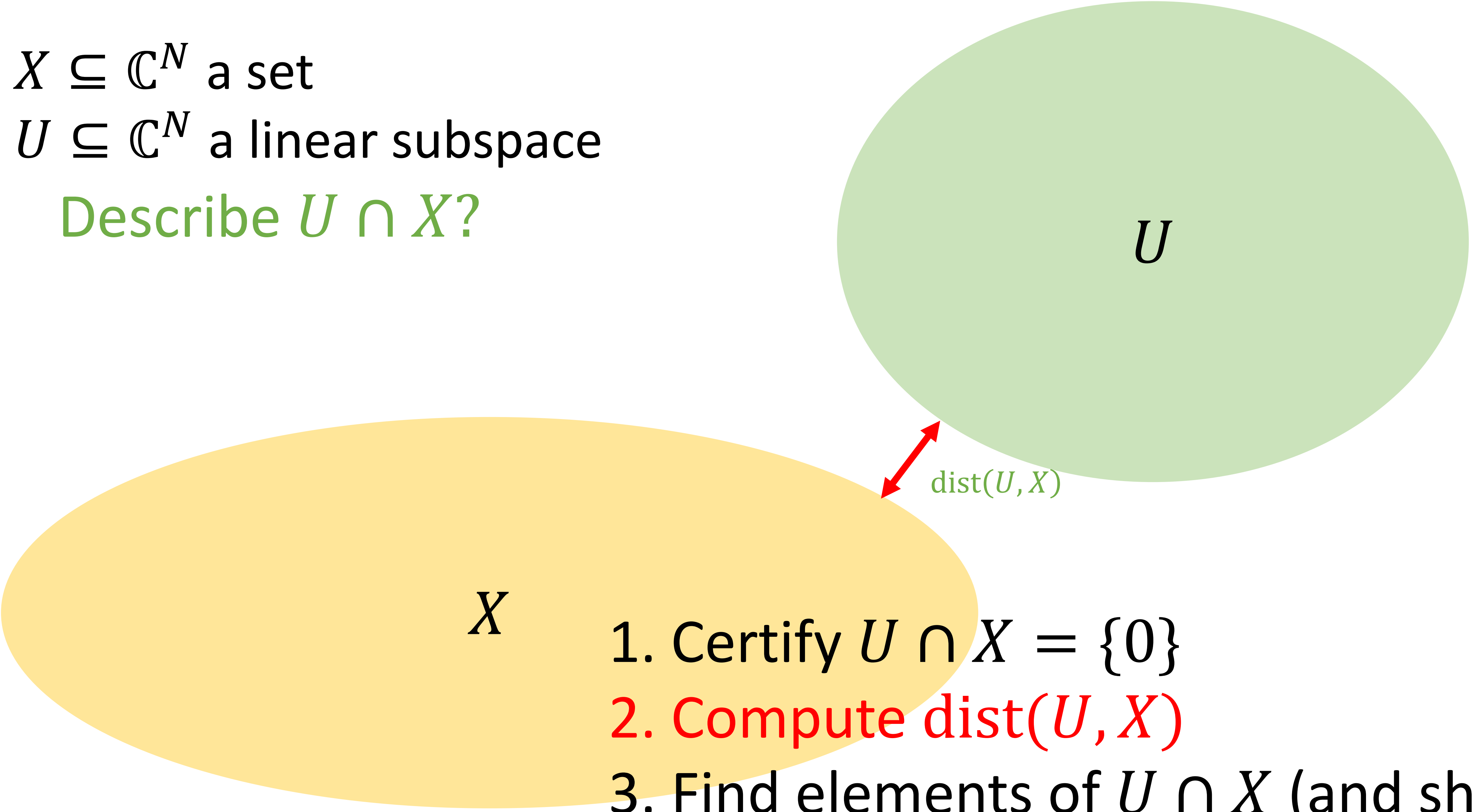
  $\mathrm{Im}(\rho)$ 1-entangled $\Rightarrow$ ρ is entangled   range criterion

- Quantum error correction

$X \subseteq \mathbb{C}^N$ a set

$U \subseteq \mathbb{C}^N$ a linear subspace

Describe $U \cap X$?



1. Certify $U \cap X = \{0\}$
2. Compute $\mathrm{dist}(U, X)$
3. Find elements of $U \cap X$ (and show that these are the only ones)

$X_1 = \{v \otimes w : v, w \in \mathbb{C}^n\} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$

Def: $U \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ is $(\epsilon, 1)$-entangled if $\mathrm{dist}(U, X_1) > \epsilon$

Applications:

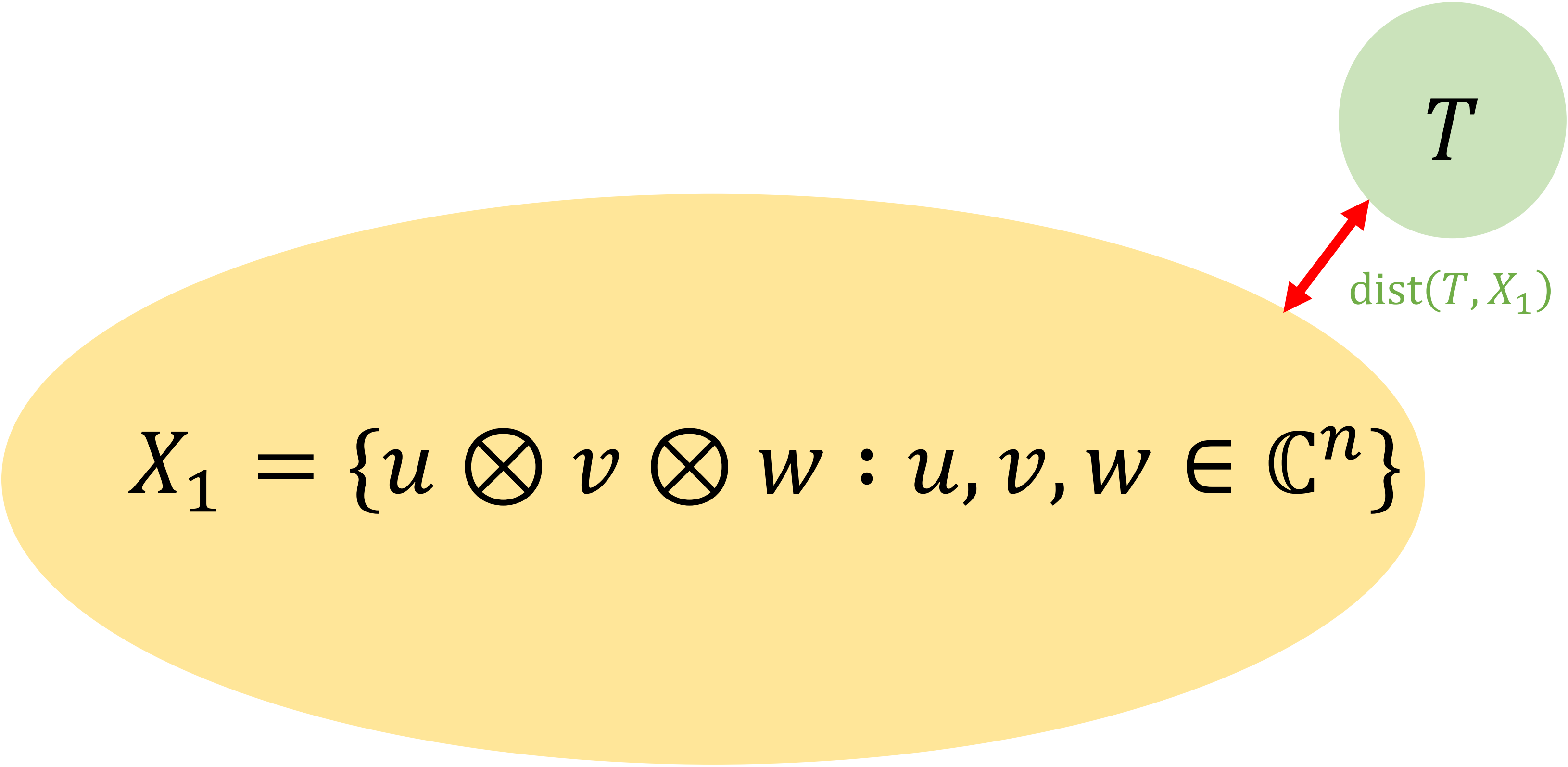
$\mathrm{Tr}(M\rho) < 1 - \epsilon$ for every separable state ρ

- A PVM $0 \leq M \leq I_{n^2}$ on $\mathbb{C}^n \otimes \mathbb{C}^n$ is an ϵ −entanglement witness $\Leftrightarrow$ $\mathrm{Im}(M) \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ is $(\epsilon, 1)$-entangled
- Computing geometric measure of entanglement

[Harrow and Montanaro, 2013]: 21 equivalent or closely related problems in quantum info and computer science, including:

- Determining acceptance probability of QMA(2) protocols
- Determining ground-state energy of mean-field Hamiltonians

Application: Computing the Geometric measure of entanglement/Injective tensor norm

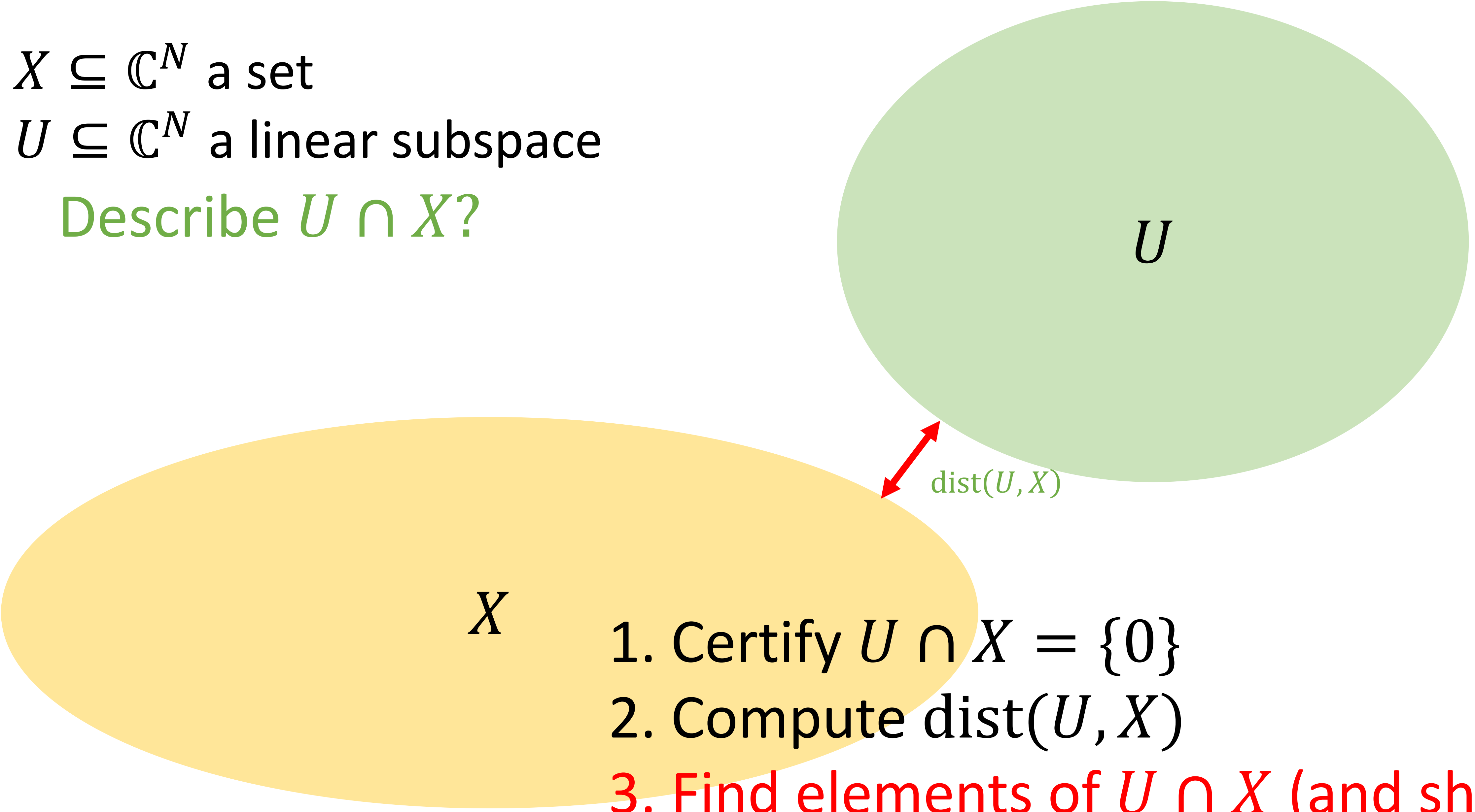


$T \in \mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^n$

$X \subseteq \mathbb{C}^N$ a set

$U \subseteq \mathbb{C}^N$ a linear subspace

Describe $U \cap X$?



1. Certify $U \cap X = \{0\}$
2. Compute $\mathrm{dist}(U, X)$
3. Find elements of $U \cap X$ (and show that these are the only ones)

Tensor decompositions

For $T \in \mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^n$, an expression $$T = \sum_{a=1}^{R} x_a \otimes y_a \otimes z_a \in \mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^n$$

is called a decomposition of T into product tensors

$$\mathrm{rank}(T) := \min\{ R : \text{there exists a decomposition of } T \text{ into R product tensors}\}$$

Uniqueness of tensor decompositions

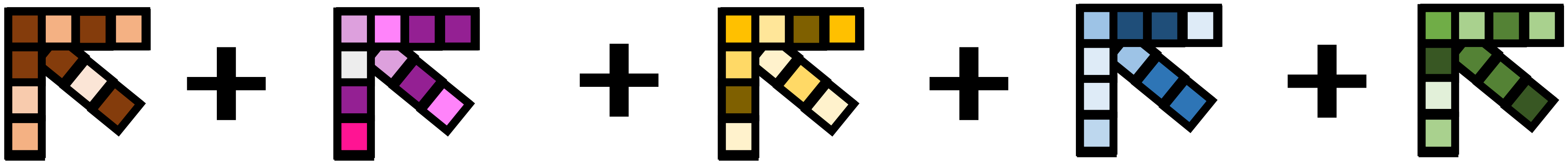
A rank decomposition

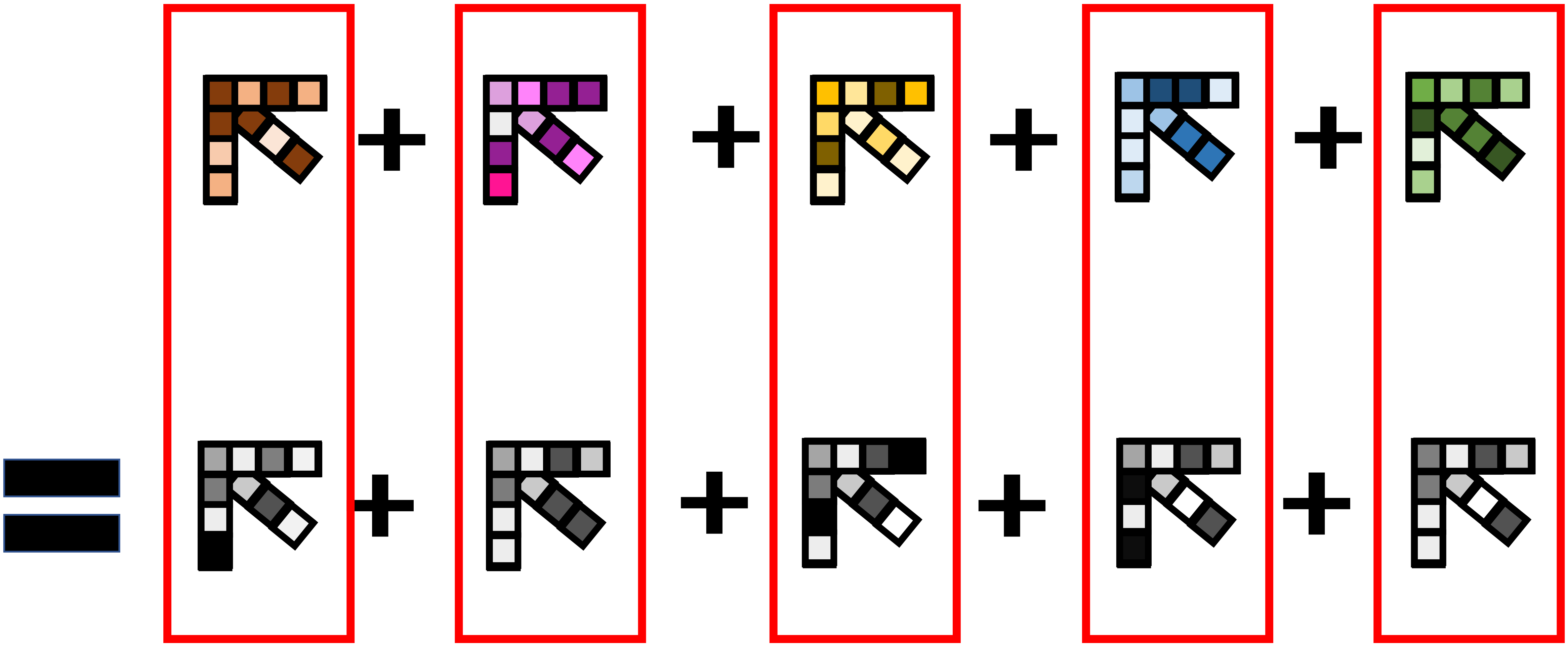
$$T = \sum_{a=1}^{R} x_a \otimes y_a \otimes z_a \in X \otimes Y \otimes Z$$

is called the unique (rank) decomposition of T if for any other decomposition

$$T = \sum_{a \in [R]} x'_a \otimes y'_a \otimes z'_a \in X \otimes Y \otimes Z$$

there is a permutation $\sigma \in S_R$ such that $x_a \otimes y_a \otimes z_a = x'_{\sigma(a)} \otimes y'_{\sigma(a)} \otimes z'_{\sigma(a)}$ for all $a \in [R]$.





Connection between finding elements of $U \cap X_1$ and decomposing tensors

Let $T \in \mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^m$ be a tensor.

If

$$T(\mathbb{C}^m) \text{ has a basis of the form } \{x_1 \otimes y_1, \dots, x_R \otimes y_R\} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n,$$

Then $T = \sum_{i=1}^R x_i \otimes y_i \otimes z_i$, where $z_i = T((x_i \otimes y_i)^*)$.

…So, algorithms for finding elements of $T(\mathbb{C}^m) \cap X_1$ lead to tensor decomposition algorithms

If $x_1 \otimes y_1, \dots, x_R \otimes y_R$ are the only elements of $T(\mathbb{C}^m) \cap X_1$ (up to scale), then $T = \sum_{i=1}^R x_i \otimes y_i \otimes z_i$ is the unique rank decomposition of T.

Application: Latent parameter learning

L is for latent

- Let A, B, C, L be finite random variables such that A, B, C are conditionally independent, i.e.

$$\Pr(a, b, c|l) = \Pr(a|l)\Pr(b|l)\Pr(c|l) \qquad \text{for all } a, b, c, l.$$

- <u>Goal:</u> Given the probability vector $\Pr(A, B, C)$, determine $\Pr(A, B, C, L)$.
- <u>Method:</u>

$$\Pr(A, B, C) = \sum_l \Pr(l)\Pr(A, B, C|l) = \sum_l \underbrace{\Pr(l)\Pr(A|l) \otimes \Pr(B|l) \otimes \Pr(C|l)}$$

... If $\Pr(A, B, C)$ has a unique decomposition, then we can recover $\Pr(A, B, C, l)$,

- <u>Applications:</u> Learning mixtures of spherical gaussians, phylogenetic tree reconstruction, hidden Markov models, orbit retrieval, blind signal separation, document topic models, …

$X \subseteq \mathbb{C}^N$ a conic variety

$U \subseteq \mathbb{C}^N$ a linear subspace

Describe $U \cap X$?

U

This talk: These problems are easy* if U is generic and $\dim(U)$ is not too large

X

1. Certify $U \cap X = \{0\}$
2. Compute $\operatorname{dist}(U, X)$
3. Find elements of $U \cap X$ (and show that these are the only ones)

Intersecting a subspace with a variety

- Let $V = \mathbb{C}^N$.
- $X \subseteq V$ is a variety if it is cut out by some $f_1, \ldots, f_p \in \mathbb{C}[x_1, \ldots, x_N]$, i.e.
$$X = \{v \in V : f_1(v) = \cdots = f_p(v) = 0\}$$
- X is a conic variety if $\mathbb{C}X = X$.

Question: Given a (linear) subspace $U \subseteq V$, describe $U \cap X$.

$X \subseteq V$ is a variety if it is cut out by some $f_1, \dots, f_p \in \mathbb{C}[x_1, \dots, x_N]$, i.e.

$$X = \{v \in V : f_1(v) = \cdots = f_p(v) = 0\}$$

<u>Example</u>: $X_1 = \{v \in \mathbb{C}^n \otimes \mathbb{C}^n : \operatorname{rank}(v) \leq 1\} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$

$$\operatorname{rank}\begin{bmatrix} a & b \\ b & c \end{bmatrix} \leq 1 \quad \Leftrightarrow \quad \det\begin{bmatrix} a & b \\ b & c \end{bmatrix} := ac - bd = 0$$

$n \times n$ matrix has rank ≤ 1 $\quad\Leftrightarrow\quad$ determinant of every 2×2 submatrix is zero

So X_1 is cut out by $p = \binom{n}{2}^2$ homogeneous polynomials of degree $d = 2$

Other examples…

- Schmidt rank $\leq r$ vectors:

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

- Product tensors: $X_1 = \{v_1 \otimes \cdots \otimes v_k : v_1, \dots, v_k \in \mathbb{C}^n\}$

- Biseparable tensors:

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

- Slice rank 1 tensors

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

- Matrix product states

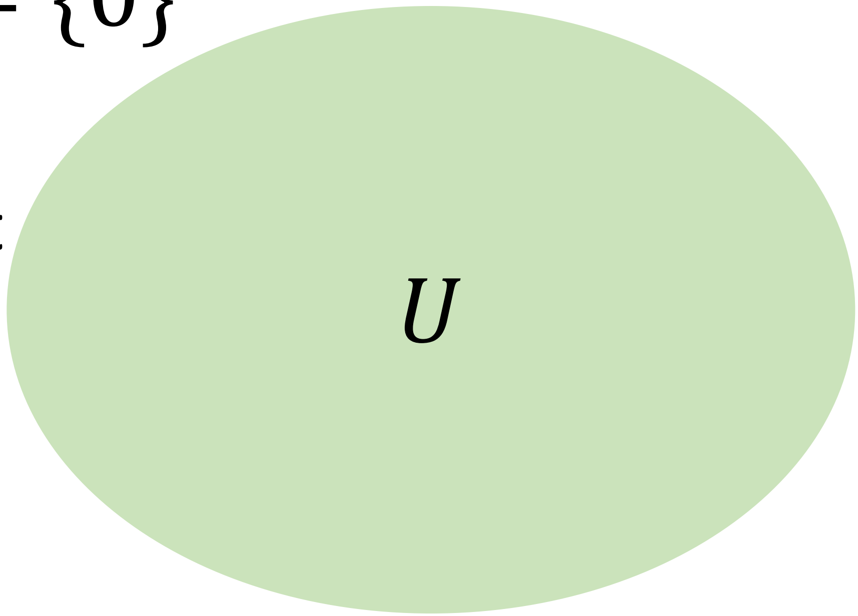
Outline

Given a conic variety $X \subseteq \mathbb{C}^N$ and a linear subspace $U \subseteq \mathbb{C}^N$, describe $U \cap X$.

<u>Algorithms to describe $U \cap X$</u>

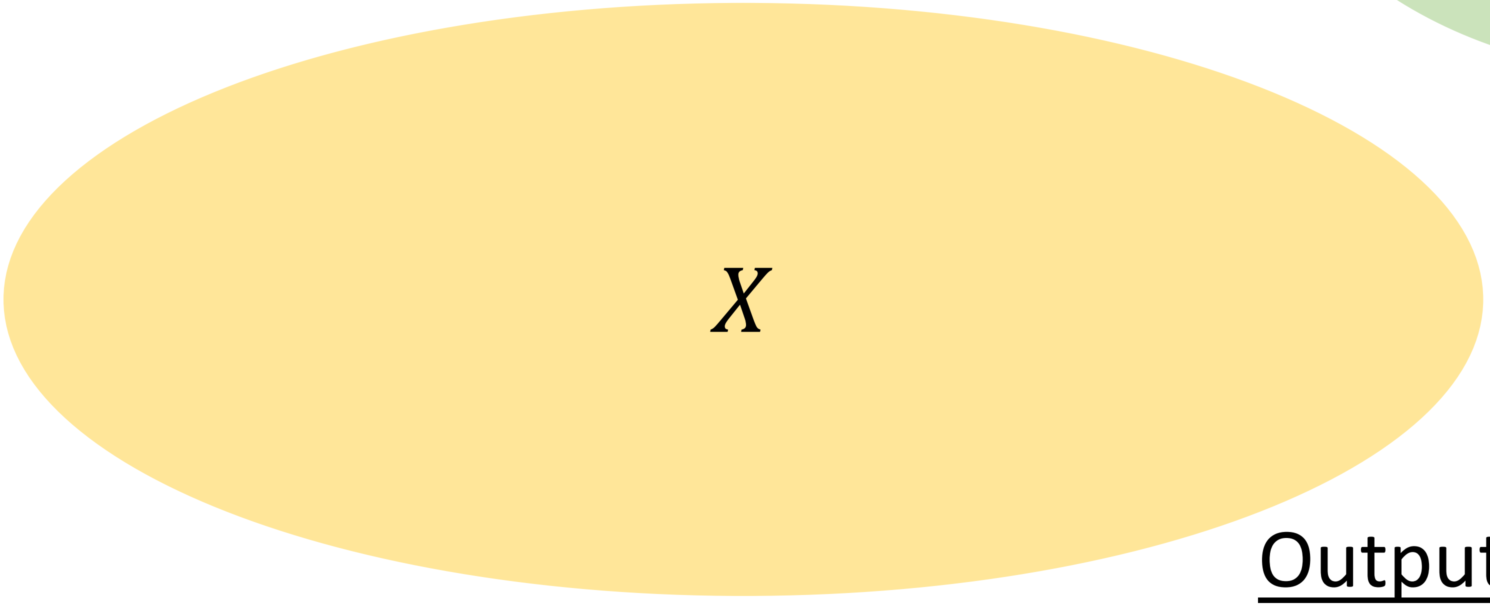
1. Algorithm to certify $U \cap X = \{0\}$.
2. Algorithm to determine $\mathrm{dist}(U, X)$.
3. Algorithm to recover elements of $U \cap X$.

Part 1: Algorithm to certify $U \cap X = \{0\}$



Input:

1. Polynomials $f_1, \dots, f_p \in \mathbb{C}[x_1, \dots, x_N]$ that cut out X.
2. A basis $\{u_1, \dots, u_R\}$ for U.



Output: Proof that $U \cap X = \{0\}$

Question: Given a (linear) subspace $U \subseteq V$, certify $U \cap X = \{0\}$.

Example: $X_1 = \{v \in \mathbb{C}^n \otimes \mathbb{C}^n : \mathrm{rank}(v) \leq 1\}$

Schmidt rank

We say $U \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ is 1-entangled if $U \cap X_1 = \{0\}$.

- [Buss et al 1999]: Determining whether U is 1-entangled is NP-Hard
- [Barak et al 2019]: Best known algorithm for determining 1-entanglement requires ϵ-promise and takes $2^{\tilde{O}(\sqrt{n}/\epsilon)}$ time.
- Theorem [JLV 2022]: Polynomial time algorithm if $\dim(U)$ is small enough and U is generic.

Theorem [JLV]: Case of $X_1 = \{v \in \mathbb{C}^n \otimes \mathbb{C}^n : \mathrm{rank}(v) \leq 1\}$

For a generic linear subspace $U \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ of dimension

$$\dim(U) \leq \frac{1}{4}(n-1)^2$$

Constant multiple of maximum possible $(n-1)^2$

it holds that $U \cap X_1 = \{0\}$, and our algorithm certifies this in time $n^{O(1)}$.

Analytic definition: If $\{u_1, \ldots, u_R\} \in \mathbb{C}^n \otimes \mathbb{C}^n$ are chosen independently at random according to e.g. the uniform spherical measure, then with probability 1…

Algebraic definition: There is a Zariski open dense subset $A \subseteq (\mathbb{C}^n \otimes \mathbb{C}^n)^{\times R}$ such that…

Theorem [JLV]: Case of $X_1 = \{v \in \mathbb{C}^n \otimes \mathbb{C}^n : \mathrm{rank}(v) \leq 1\}$

For a generic linear subspace $U \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ of dimension

$$\dim(U) \leq \frac{1}{4}(n-1)^2$$

Constant multiple of maximum possible $(n-1)^2$

it holds that $U \cap X_1 = \{0\}$, and our algorithm certifies this in time $n^{O(1)}$.

Furthermore, for a generic subspace $U \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ of this dimension containing a generic element of X_1, there is an algorithm that recovers this element in time $n^{O(1)}$.

Analytic def: "If you pick $v_1 \in X_1$ randomly, and $v_2, \ldots, v_R \in \mathbb{C}^n \otimes \mathbb{C}^n$ randomly…"

Algebraic def: There is a Zariski open dense subset $A \subseteq X_1 \times (\mathbb{C}^n \otimes \mathbb{C}^n)^{\times R-1}$ s.t…

Algorithm performance to certify $U \cap X_1 = \{0\}$

n	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

More general statement for arbitrary X

<u>Theorem [JLV]:</u> Suppose that $X \subseteq \mathbb{C}^N$ is a conic variety cut out by $p = \delta\binom{N+d-1}{d}$ linearly independent homogeneous degree-d polynomials $f_1, \ldots, f_p \in \mathbb{C}[x_1, \ldots, x_N]_d$ for some $\delta \in [0,1]$.

Then for a generic linear subspace $U \subseteq \mathbb{C}^N$ of dimension

$$\dim(U) \leq \frac{N+d-1}{d!}\delta,$$

it holds that $U \cap X = \{0\}$, and there is an algorithm that certifies this in time $N^{O(d)}$.

Theorem [JLV]: If $X \subseteq \mathbb{C}^N$ is cut out by $p = \delta\binom{N+d-1}{d}$ linearly independent homogeneous degree-d polynomials, then for a generic linear subspace $U \subseteq \mathbb{C}^N$ of dimension

$$\dim(U) \leq \frac{N+d-1}{d!}\delta,$$

it holds that $U \cap X = \{0\}$, and there is an algorithm that certifies this in time $N^{O(d)}$.

Not bad: Takes $\binom{N+d-1}{d}$ time just to read off degree-d polynomials

Example: If $d = 1$, then $X \subseteq \mathbb{C}^N$ is a linear subspace. Theorem says:

If $U \subseteq \mathbb{C}^N$ generic and $\dim(U) \leq \delta N = p = N - \dim(X)$,

Then $U \cap X = \{0\}$, and this can be verified in poly(N) time.

Theorem [JLV]: If $X \subseteq \mathbb{C}^N$ is cut out by $p = \delta\binom{N+d-1}{d}$ linearly independent homogeneous degree-d polynomials, then for a generic linear subspace $U \subseteq \mathbb{C}^N$ of dimension

$$\dim(U) \leq \frac{N+d-1}{d!}\delta,$$

it holds that $U \cap X = \{0\}$, and there is an algorithm that certifies this in time $N^{O(d)}$.

Fact: For a conic variety $X \subseteq \mathbb{C}^N$, if there exists $U \subseteq \mathbb{C}^N$ such that $U \cap X = \{0\}$, then $\dim(X) \leq N - \dim(U)$.

Hilbert function of X

Krull dimension of X

Maximize δ

Corollary: $\dim(X) \leq N - \frac{N+d-1}{d!}\delta = N - \frac{N+d-1}{d!}\left(1 - \frac{h_X(d)}{\binom{N+d-1}{d}}\right)$

Again: A curious upper bound on $\mathbf{dim}(\boldsymbol{X})$

Corollary:

For a conic variety $X \subseteq \mathbb{C}^N$,

$$\dim(X) \leq N - \frac{N+d-1}{d!}\left(1 - \frac{h_X(d)}{\binom{N+d-1}{d}}\right) \text{ for all } d \geq 1.$$

Theorem [JLV]: If $X \subseteq \mathbb{C}^N$ is cut out by $p = \delta\binom{N+d-1}{d}$ linearly independent homogeneous degree-d polynomials, then for a generic linear subspace $U \subseteq \mathbb{C}^N$ of dimension

$$\dim(U) \leq \frac{N+d-1}{d!}\delta,$$

it holds that $U \cap X = \{0\}$, and there is an algorithm that certifies this in time $N^{O(d)}$.

If $\delta = \Omega(1)$, then we certify $U \cap X = \{0\}$ for generic subspaces U with $\dim(U) = \Omega(N)$ (the largest possible).

If $\delta = \Omega(1)$, then we certify $U \cap X = \{0\}$ in time $N^{O(d)}$ for generic subspaces U with $\dim(U) = \Omega(N)$ (the largest possible).

<u>Example:</u> $X_1 = \{v \in \mathbb{C}^n \otimes \mathbb{C}^n : \mathrm{rank}(v) \leq 1\}$ cut out by 2×2 minors

$$\text{number of variables} = N = n^2$$

$$\text{number of polynomials} = p = \binom{n}{2}^2$$

$$\text{polynomial degree} = d = 2$$

$$\delta := \frac{p}{\binom{N+d-1}{d}} = \frac{\binom{n}{2}^2}{\binom{n^2+2-1}{2}} = \Omega(1)$$

So we certify $U \cap X_1 = \{0\}$ in time $n^{O(d)}$ for generic subspaces U with $\dim(U) = \Omega(n^2)$

Other examples…

All in poly(N) time

- Schmidt rank $\leq r$ vectors:

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

$\dim(U) = \Omega_r(n^2)$

- Product tensors: $X_1 = \{v_1 \otimes \cdots \otimes v_m : v_1, \ldots, v_m \in \mathbb{C}^n\}$

$\dim(U) \sim \frac{1}{4} n^m$

- Biseparable tensors:

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

$\dim(U) \sim \frac{1}{4} n^m$

- Slice rank 1 tensors

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

$\dim(U) \sim \frac{1}{4} n^m$

- Matrix product states:

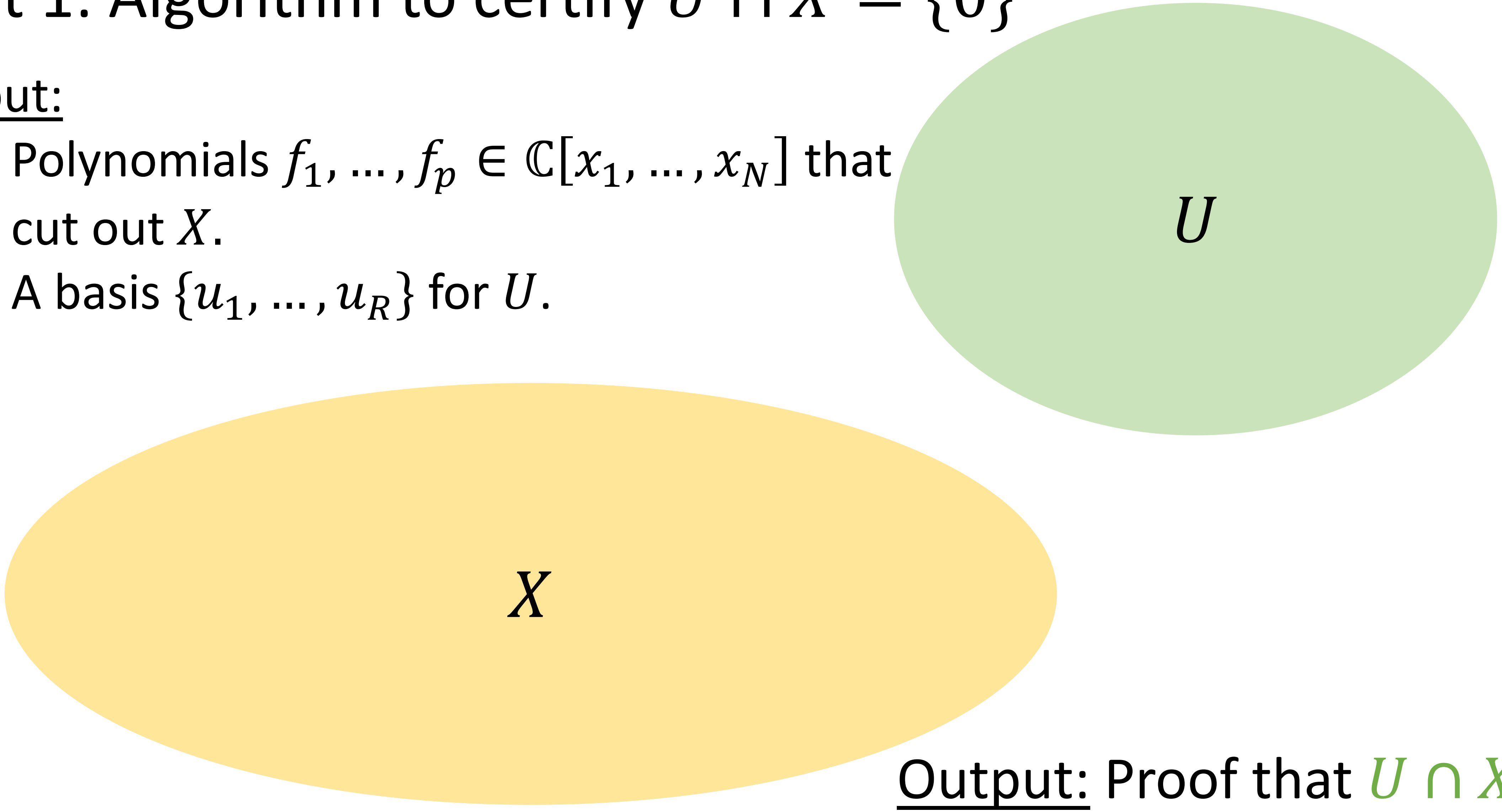
$\dim(U) \sim \frac{1}{4} n^m$

The Algorithm
(Nullstellensatz Certificate)

Part 1: Algorithm to certify $U \cap X = \{0\}$

<u>Input:</u>

1. Polynomials $f_1, \ldots, f_p \in \mathbb{C}[x_1, \ldots, x_N]$ that cut out X.
2. A basis $\{u_1, \ldots, u_R\}$ for U.



<u>Output:</u> Proof that $U \cap X = \{0\}$

The symmetric subspace

Let $S^d(V) \subseteq V^{\otimes d}$ be the symmetric subspace

$$S^d(V) = \left\{ T = \left(T_{i_1,\dots,i_d}\right)_{i_j \in [N]} \in V^{\otimes d} \colon \sigma(T) := \left(T_{i_{\sigma(1)},\dots,i_{\sigma(d)}}\right)_{i_j \in [N]} = T \quad \forall \sigma \in \mathfrak{S}_d \right\}$$

<u>Example:</u> $v^{\otimes d} \in S^d(V)$ for all $v \in V$

<u>Example:</u> $v_1 \otimes v_2 + v_2 \otimes v_1 \in S^2(V)$ for all $v_1, v_2 \in V$

<u>Non-example:</u> $v_1 \otimes v_2 - v_2 \otimes v_1 \notin S^2(V)$

The symmetric subspace

Let $S^d(V) \subseteq V^{\otimes d}$ be the symmetric subspace

$$S^d(V) = \left\{ T = \left(T_{i_1,\ldots,i_d}\right)_{i_j \in [N]} \in V^{\otimes d} : T = \left(T_{i_{\sigma(1)},\ldots,i_{\sigma(d)}}\right)_{i_j \in [N]} \quad \text{for all} \quad \sigma \in \mathfrak{S}_d \right\}$$

$P_{d,V}^{\vee} : V^{\otimes d} \to V^{\otimes d}$ orthogonal projection onto $S^d(V)$

The symmetric subspace

Let $S^d(V) \subseteq V^{\otimes d}$ be the symmetric subspace

$$S^d(V) = \left\{ T = \left(T_{i_1,\ldots,i_d}\right)_{i_j \in [N]} \in V^{\otimes d} : T = \left(T_{i_{\sigma(1)},\ldots,i_{\sigma(d)}}\right)_{i_j \in [N]} \quad \text{for all} \quad \sigma \in \mathfrak{S}_d \right\}$$

$P^{\vee}_{d,V} : V^{\otimes d} \to V^{\otimes d}$ orthogonal projection onto $S^d(V)$

Basis for $S^d(V)$: $B^{\vee}_{d,V} \coloneqq \{P^{\vee}_{d,V}(|i_1\rangle \otimes \cdots \otimes |i_d\rangle) : 1 \leq i_1 \leq \cdots \leq i_d \leq N\}$

A characterization of conic varieties

<u>Fact/Definition:</u> For a subset $X \subseteq V$, the following are equivalent:

1. X is a conic variety
2. There exists $d \in \mathbb{N}$ and an orthogonal projection $\Psi_X^d : V^{\otimes d} \to V^{\otimes d}$ such that:
   i. Ψ_X^d is symmetric: $\mathrm{Im}\left(\Psi_X^d\right) \subseteq S^d(V)$
   ii. $X = \{v \in V : v^{\otimes d} \in \mathrm{Im}\left(\Psi_X^d\right)\}$

$S^d(V^*) \cong \mathbb{F}[x_1, \ldots, x_N]_d$

<u>Why?</u> If X is cut out by $f_1, \ldots, f_p \in S^d(V^*)$, let $\Psi_X^d = \mathrm{Proj}\left(\bigcap_{i=1}^{p} \mathrm{Ker}(f_i)\right)$

$$v \in X \quad \Longleftrightarrow \quad f_1\left(v^{\otimes d}\right) = \cdots = f_p\left(v^{\otimes d}\right) = 0 \quad \Longleftrightarrow \quad v^{\otimes d} \in \mathrm{Im}\left(\Psi_X^d\right)$$

Fact/Definition: For a subset $X \subseteq V$, the following are equivalent:

1. X is a conic variety
2. There exists $d \in \mathbb{N}$ and an orthogonal projection $\Psi_X^d : V^{\otimes d} \to V^{\otimes d}$ such that:
   i. Ψ_X^d is symmetric: $\mathrm{Im}\left(\Psi_X^d\right) \subseteq S^d(V)$
   ii. $X = \{v \in V : v^{\otimes d} \in \mathrm{Im}\left(\Psi_X^d\right)\}$

Example: $X_1 = \{v \otimes w \;\; : \;\; v, w \in \mathbb{C}^n\} \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$

$d = 2$

$\Psi_X^2 = \mathrm{Proj}(\, S^2(\mathbb{C}^n) \otimes S^2(\mathbb{C}^n))$

$X_1 = \{v \in \mathbb{C}^n \otimes \mathbb{C}^n : v^{\otimes 2} \in S^2(\mathbb{C}^n) \otimes S^2(\mathbb{C}^n)\}$

Question: Given a conic variety $X = \{v \in V : v^{\otimes d} \in \mathrm{Im}(\Psi_X^d)\} \subseteq V$ and a basis $\{u_1, \ldots, u_R\}$ for a subspace $U \subseteq \mathbb{C}^N$, is $U \cap X = \{0\}$?

$$S^d(U) = U^{\otimes d} \cap S^d(V)$$
$$= \mathrm{span}\{P_{d,V}^{\vee}(u_{i_1} \otimes \cdots \otimes u_{i_d}) : 1 \leq i_1 \leq \cdots \leq i_d \leq R\}$$

Algorithm:

1. If $\mathrm{Im}(\Psi_X^d) \cap S^d(U) = \{0\}$, output YES
2. Otherwise, output I DON'T KNOW

Correctness: If $\mathrm{Im}(\Psi_X^d) \cap S^d(U) = \{0\}$, then $U \cap X = \{0\}$.

Proof: If $u \in U \cap X$, then $u^{\otimes d} \in \mathrm{Im}(\Psi_X^d) \cap S^d(U)$. $\blacksquare$

Theorem [JLV]: If $X \subseteq \mathbb{C}^N$ is cut out by $p = \delta\binom{N+d-1}{d}$ linearly independent homogeneous degree-d polynomials, then for a generic linear subspace $U \subseteq \mathbb{C}^N$ of dimension

$$\dim(U) \leq \frac{N+d-1}{d!}\delta, \qquad (1)$$

it holds that $\mathrm{Im}(\Psi_X^d) \cap S^d(U) = \{0\}$.

Proof idea: Given a subspace $W := \mathrm{Im}(\Psi_X^d) \subseteq S^d(\mathbb{C}^N)$, show that a (generic) subspace of the form $S^d(U)$, for $\dim(U)$ not too large, satisfies $W \cap S^d(U) = \{0\}$.

<u>Proof idea:</u> Given a subspace $W \subseteq S^d(\mathbb{C}^N)$, show that a (generic) subspace of the form $S^d(U)$, for $\dim(U)$ not too large, satisfies $W \cap S^d(U) = \{0\}$.

One might hope that you could take $R \coloneqq \dim(U)$ maximal for which

$$\dim(W) + \underbrace{\binom{N+R-1}{R}}_{\dim(S^d(U))} \leq \underbrace{\binom{N+d-1}{d}}_{\dim(S^d(\mathbb{C}^N))}$$

Proof idea: Given a subspace $W \subseteq S^d(\mathbb{C}^N)$, show that a (generic) subspace of the form $S^d(U)$, for $\dim(U)$ not too large, satisfies $W \cap S^d(U) = \{0\}$.

One might hope that you could take $R \coloneqq \dim(U)$ maximal for which

$$\dim(W) + \binom{N+R-1}{R} \leq \binom{N+d-1}{d}$$

3 3 6

Not true! Take $N = 3, d = 2,$ $W = S^2(\mathbb{C}^2) \subseteq S^2\,(\mathbb{C}^3)$.

Then for any $U \subseteq \mathbb{C}^3$ of dimension $\dim(U) = 2$, it holds that $S^2(\mathbb{C}^2)\ \cap S^2(U) \supseteq S^2(\mathbb{C}^2 \cap U) \neq \{0\}$

Question: Given a conic variety $X = \{v \in V : v^{\otimes d} \in \mathrm{Im}(\Psi_X^d)\} \subseteq V$ and a basis $\{u_1, \ldots, u_R\}$ for a subspace $U \subseteq \mathbb{C}^N$, is $U \cap X = \{0\}$?

Complete hierarchy:

1. For $c \geq d$, let $\Psi_X^c = (\Psi_X^d \otimes I_V^{\otimes c-d}) : V^{\otimes c} \to V^{\otimes c}$
2. If $\mathrm{Im}(\Psi_X^c) \cap S^c(U) = \{0\}$ for some $c \leq (d+1)^N$, output YES
3. Otherwise, output NO

Correctness:

$\mathrm{Im}(\Psi_X^c) \cap S^c(U) = \{0\}$ for some $c \leq (d+1)^N \iff U \cap X = \{0\}$

Proof: $\Rightarrow$: For any $u \in U \cap X$, it holds that $u^{\otimes c} \in \mathrm{Im}(\Psi_X^c) \cap S^c(U)$.

$\Leftarrow$: Hilbert's Nullstellensatz + degree bounds

Outline

Given a conic variety $X \subseteq \mathbb{C}^N$ and a linear subspace $U \subseteq \mathbb{C}^N$, describe $U \cap X$.

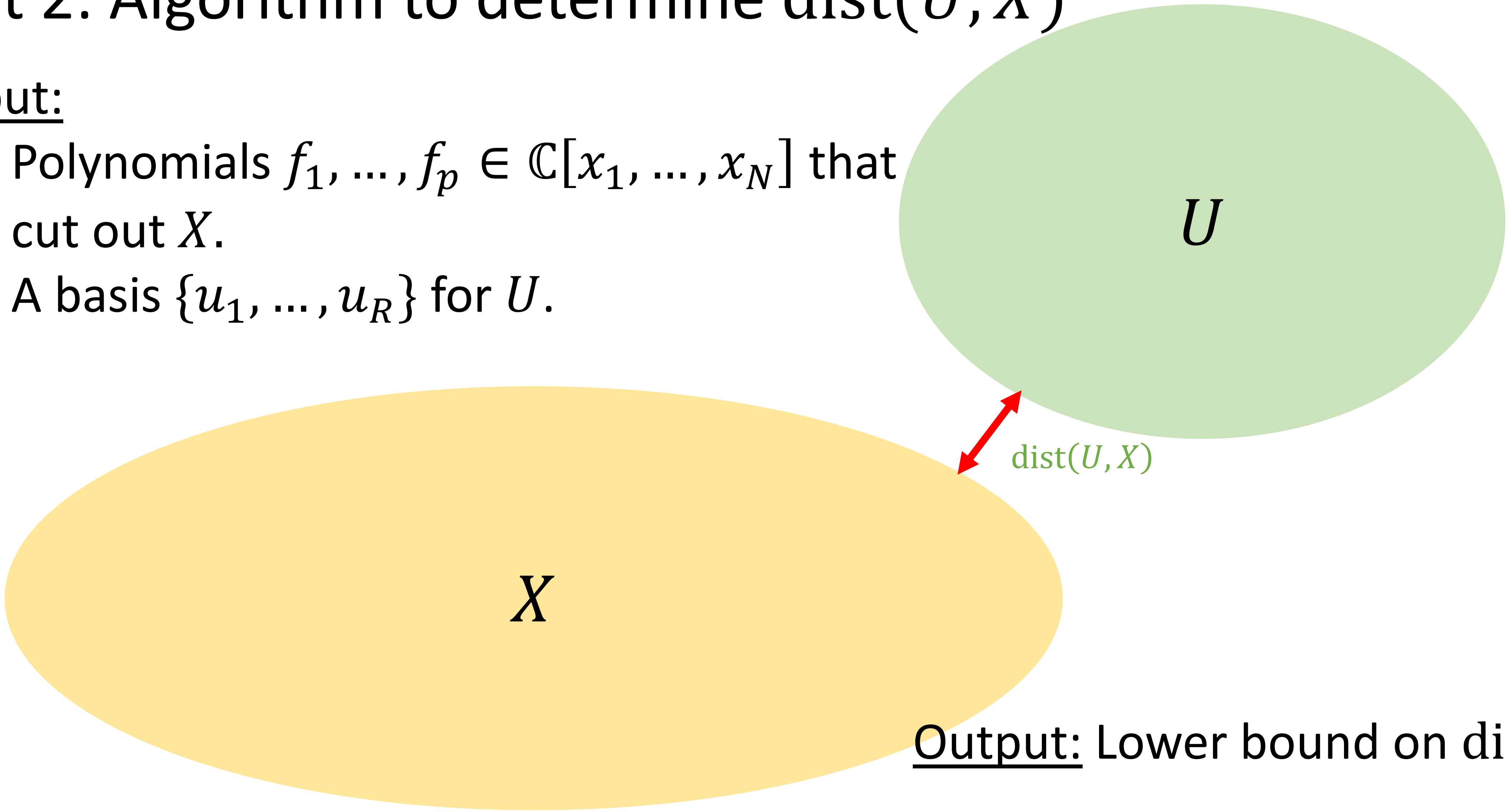
<u>Algorithms to describe $U \cap X$</u>

1. Algorithm to certify $U \cap X = \{0\}$.
2. Algorithm to determine $\mathrm{dist}(U, X)$.
3. Algorithm to recover elements of $U \cap X$.

Part 2: Algorithm to determine $\mathrm{dist}(U, X)$

Input:

1. Polynomials $f_1, \dots, f_p \in \mathbb{C}[x_1, \dots, x_N]$ that cut out X.
2. A basis $\{u_1, \dots, u_R\}$ for U.



Output: Lower bound on $\mathrm{dist}(U, X)$

We have a complete hierarchy of *lower bounds* on $\mathrm{dist}(U, X)$

Making the algorithm robust

<u>Observation:</u>

$$\mathrm{Im}(\Psi_X^c) \cap S^c(U) = \{0\} \quad \Leftrightarrow \quad \lambda_{max}\left(P_{d,V}^{\vee} \Psi_X^c (P_U \otimes I_V^{\otimes c-1})\right) < 1$$

<u>Proof:</u>

$$\lambda_{max}\left(P_{d,V}^{\vee} \Psi_X^c (P_U \otimes I_V^{\otimes c-1})\right) < 1$$

$$\Leftrightarrow S^d(V) \cap \mathrm{Im}(\Psi_X^c) \cap \left(U \otimes V^{\otimes c-1}\right) = \{0\}$$

$$\Leftrightarrow \mathrm{Im}(\Psi_X^c) \cap S^c(U) = \{0\} \qquad \blacksquare$$

Making the algorithm robust

<u>Observation:</u>

$$\mathrm{Im}(\Psi_X^c) \cap S^c(U) = \{0\} \quad \Leftrightarrow \quad \nu_c := \lambda_{max}\left(P_{d,V}^{\vee} \Psi_X^c (P_U \otimes I_V^{\otimes c-1}) \Psi_X^c P_{d,V}^{\vee}\right) < 1$$

<u>Proof:</u>

$$\nu_c < 1$$

$$\Leftrightarrow S^d(V) \cap \mathrm{Im}(\Psi_X^c) \cap \left(U \otimes V^{\otimes c-1}\right) = \{0\}$$

$$\Leftrightarrow \mathrm{Im}(\Psi_X^c) \cap S^c(U) = \{0\}$$

$\blacksquare$

Question: Given a conic variety $X = \{v \in V : v^{\otimes d} \in \mathrm{Im}\left(\Psi_X^d\right)\} \subseteq V$ and a basis $\{u_1, \dots, u_R\}$ for a subspace $U \subseteq \mathbb{C}^N$, is $U \cap X = \{0\}$?

$\nu_c \coloneqq \lambda_{max}\left(P_{d,V}^{\vee} \Psi_X^c (P_U \otimes I_V^{\otimes c-1}) \Psi_X^c P_{d,V}^{\vee}\right)$

Complete hierarchy:

1. If $\nu_c < 1$ for some $c \leq (d+1)^N$, output YES
2. Otherwise, output NO

Correctness:

$\nu_c < 1 \quad \Leftrightarrow \quad \mathrm{Im}(\Psi_X^c) \cap S^c(U) = \{0\}$ $\blacksquare$

Robust version

<u>Question:</u> Given a conic variety $X = \{v \in V : v^{\otimes d} \in \mathrm{Im}(\Psi_X^d)\} \subseteq V$ and a basis $\{u_1, \ldots, u_R\}$ for a subspace $U \subseteq \mathbb{F}^N$, what is $\mathrm{dist}(U, X)$?

$$\mathrm{dist}(U, X) = \frac{1}{4} \min_{\substack{x \in X \\ \|x\|=1}} \min_{\substack{u \in U \\ \|u\|=1}} \|xx^* - uu^*\|_1^2$$

Hausdorff distance

$$= 1 - \max_{\substack{x \in X \\ \|x\|=1}} \max_{\substack{u \in U \\ \|u\|=1}} |\langle x, u \rangle|^2$$

$$= 1 - \max_{\substack{x \in X \\ \|x\|=1}} \langle x, P_U x \rangle$$

Question: Given a conic variety $X = \{v \in V: v^{\otimes d} \in \mathrm{Im}(\Psi_X^d)\} \subseteq V$ and a basis $\{u_1, \dots, u_R\}$ for a subspace $U \subseteq \mathbb{C}^N$, what is $\mathrm{dist}(U, X)$?

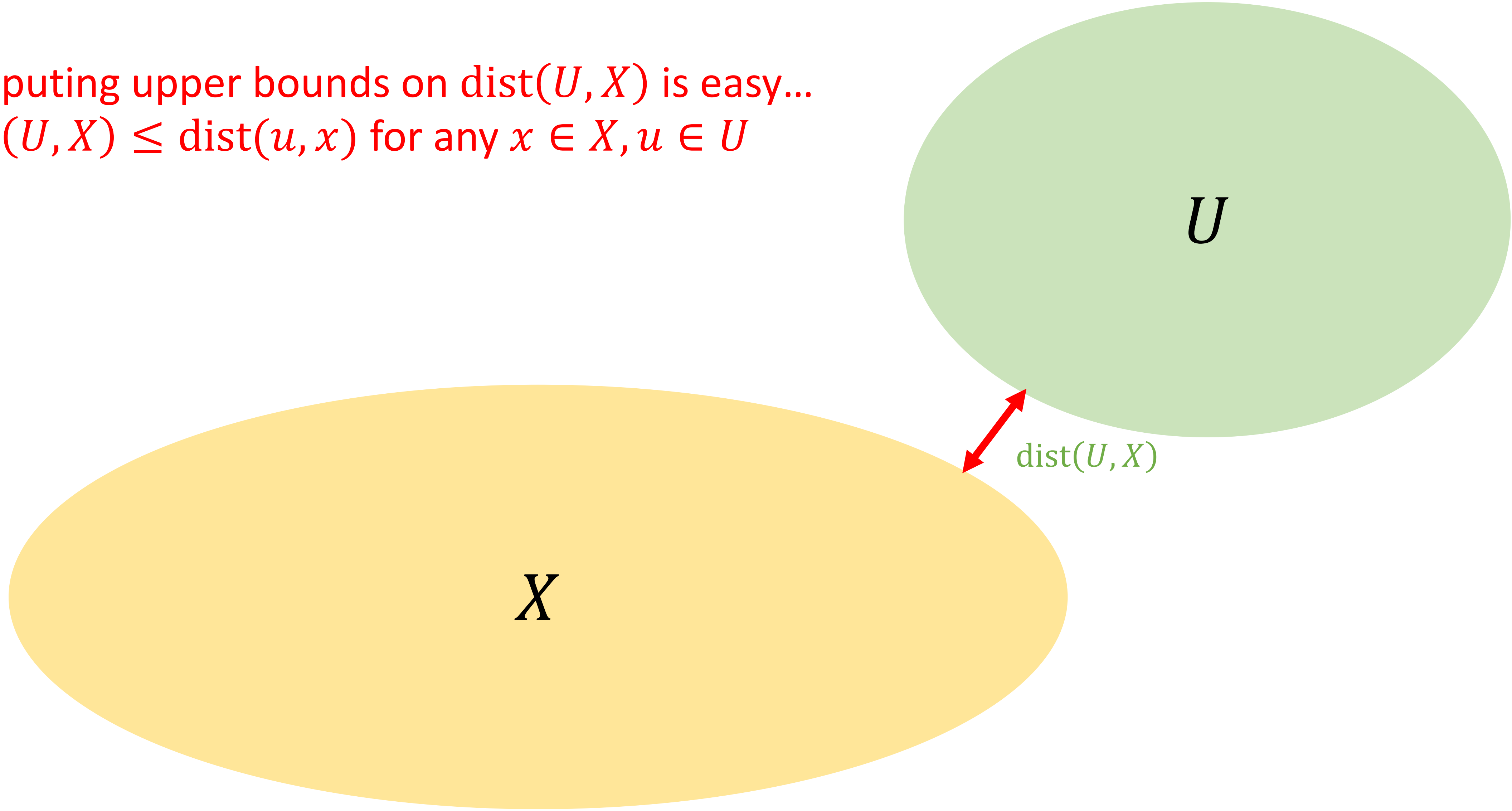
$\nu_c := \lambda_{max}\left(P_{d,V}^{\vee} \Psi_X^c (P_U \otimes I_V^{\otimes c-1}) \Psi_X^c P_{d,V}^{\vee}\right)$

Theorem [JLV]:

- $\nu_c = 1$ for all $c \leq (d+1)^N \iff \mathrm{dist}(U, X) = 0$
- $\nu_d \geq \nu_{d+1} \geq \nu_{d+2} \geq \cdots$
- $\mathrm{dist}(U, X) = 1 - \lim_{c \to \infty} \nu_c$

In particular, $\mathrm{dist}(U, X) \geq 1 - \nu_c$ for all c (inner approximation)

Computing upper bounds on $\mathrm{dist}(U, X)$ is easy…
$\mathrm{dist}(U, X) \le \mathrm{dist}(u, x)$ for any $x \in X, u \in U$



We have a complete hierarchy of *lower bounds* on $\mathrm{dist}(U, X)$

Theorem [JLV]:

$\nu_c := \lambda_{max}\left(P_{d,V}^{\vee}\Psi_X^c(P_U\otimes I_V^{\otimes c-1})\Psi_X^c P_{d,V}^{\vee}\right)$

- $\nu_c = 1$ for all $c \leq (d+1)^N \quad \Leftrightarrow \quad \mathrm{dist}(U,X) = 0$ ✓
- $\nu_d \geq \nu_{d+1} \geq \nu_{d+2} \geq \cdots$
- $1 - \mathrm{dist}(U,X) = \lim_{c\to\infty} \nu_c$

In particular, $1 - \mathrm{dist}(U,X) \leq \nu_c$ for all c (inner approximation)

Proof:

$\mathrm{Im}\left(P_{d,V}^{\vee}\Psi_X^c\right) \supseteq \mathrm{span}\{v^{\otimes c} : v \in X\}$, so for all $v \in X$,

$$\nu_c \geq \langle v^{\otimes c}, P_{d,V}^{\vee}\Psi_X^c(P_U\otimes I_V^{\otimes c-1})\Psi_X^c P_{d,V}^{\vee} v^{\otimes c}\rangle$$
$$= \langle v^{\otimes c}, \left(P_U \otimes I_V^{\otimes c-1}\right) v^{\otimes c}\rangle$$
$$= \langle v, P_U\, v\rangle$$

... So $\nu_c \geq \max_{v\in X}\langle v, P_U v\rangle = 1 - \mathrm{dist}(U,X)$ ∎

Outline

Given a conic variety $X \subseteq \mathbb{C}^N$ and a linear subspace $U \subseteq \mathbb{C}^N$, describe $U \cap X$.

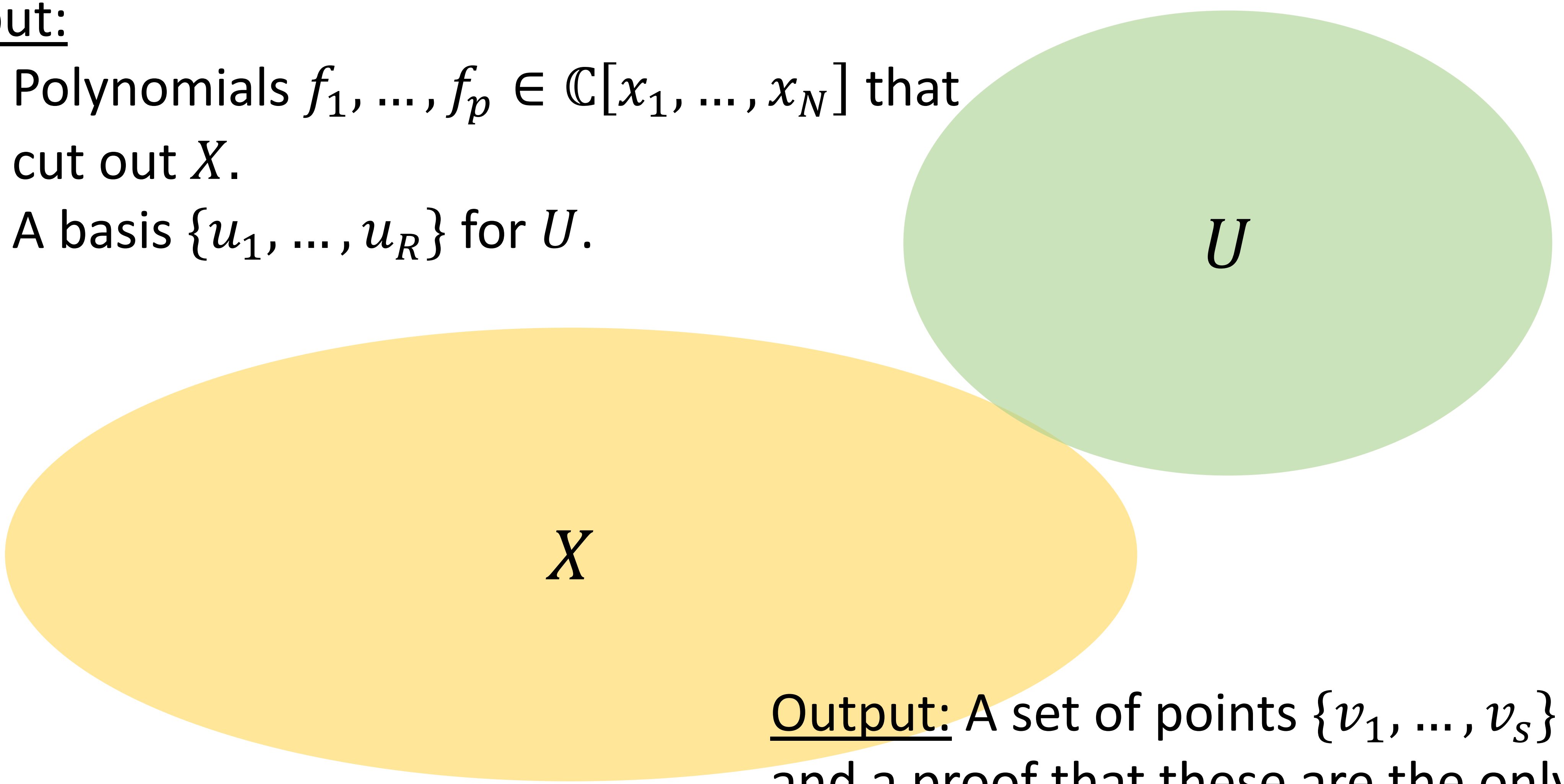
<u>Algorithms to describe $U \cap X$</u>

1. Algorithm to determine whether $U \cap X = \{0\}$.
2. Algorithm to determine $\operatorname{dist}(U, X)$.
3. Algorithm to recover elements of $U \cap X$.

Part 3: Algorithm to recover elements of $U \cap X$

<u>Input:</u>

1. Polynomials $f_1, \ldots, f_p \in \mathbb{C}[x_1, \ldots, x_N]$ that cut out X.
2. A basis $\{u_1, \ldots, u_R\}$ for U.



<u>Output:</u> A set of points $\{v_1, \ldots, v_s\} \in U \cap X$, and a proof that these are the only elements (up to scalar multiples).

Theorem [JLV]: Case of $X_1 = \{v \in \mathbb{C}^n \otimes \mathbb{C}^n : \mathrm{rank}(v) \leq 1\}$

For a generic linear subspace $U \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ of dimension

$$\dim(U) \leq \frac{1}{4}(n-1)^2$$

Constant multiple of maximum possible $(n-1)^2$

it holds that $U \cap X_1 = \{0\}$, and our algorithm certifies this in time $n^{O(1)}$.

More generally, for a generic subspace $U \subseteq \mathbb{C}^n \otimes \mathbb{C}^n$ of this dimension containing $s \leq \dim(U)$ generic elements of X_1, our algorithm recovers these elements in time $n^{O(1)}$, and certifies that these are the only elements of $U \cap X_1$.

Analytic def: "If I pick $v_1, \ldots, v_s \in X_1$ and $v_{s+1}, \ldots, v_R \in \mathbb{C}^n \otimes \mathbb{C}^n$ randomly…"
Algebraic def: There is a Zariski open dense subset $A \subseteq X_1^{\times s} \times (\mathbb{C}^n \otimes \mathbb{C}^n)^{\times R-s}$ s.t…

Corollary: A generic tensor $T \in \mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^m$ with

$$\mathrm{rank}(T) \leq \min\{\frac{1}{4}(n-1)^2, m\}$$

has a unique rank decomposition, which is recovered by applying our algorithm to $T(\mathbb{C}^m)$.

Analytic def: $T = \sum_{i=1}^{R} x_i \otimes y_i \otimes z_i$, where each $x_i \otimes y_i \otimes z_i$ is chosen randomly.

Algebraic def: There is a Zariski open dense subset $A \subseteq \{\mathrm{rank} \leq R \text{ tensors}\}$

Corollary: A generic tensor $T \in \mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathbb{C}^m$ with

$$\operatorname{rank}(T) \leq \min\{\frac{1}{4}(n-1)^2, m\}$$

has a unique rank decomposition, which is recovered by applying our algorithm to $T(\mathbb{C}^m)$.

Proof: Say $T = \sum_{i=1}^{R} x_i \otimes y_i \otimes z_i$.

T generic, $R \leq m \Rightarrow \{z_1, \dots, z_R\}$ is linearly independent

$$\Rightarrow T(\mathbb{C}^m) = \operatorname{span}\{x_1 \otimes y_1, \dots, x_R \otimes y_R\}$$

$T(\mathbb{C}^m)$ generic, $R \leq \frac{1}{4}(n-1)^2 \Rightarrow x_1 \otimes y_1, \dots, x_R \otimes y_R$ are the only elements of $T(\mathbb{C}^m) \cap X_1$ (up to scale), and they are recovered by our algorithm

$(X, \mathbb{C}^m)$-decompositions (aka simult. X-decomp)

Let $X \subseteq V$ be a non-degenerate conic variety.

For $T \in V \otimes \mathbb{C}^m$, an expression $$T = \sum_{i=1}^{R} v_i \otimes z_i \in V \otimes \mathbb{C}^m$$

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

is called an $(X, \mathbb{C}^m)$-decomposition of T

$\mathrm{rank}_{\mathrm{X}}(T) := \min\{ R: \text{there exists an } (X, \mathbb{C}^m)\text{–decomposition of T of length R}\}$

Uniqueness of $(X, \mathbb{C}^m)$-decompositions

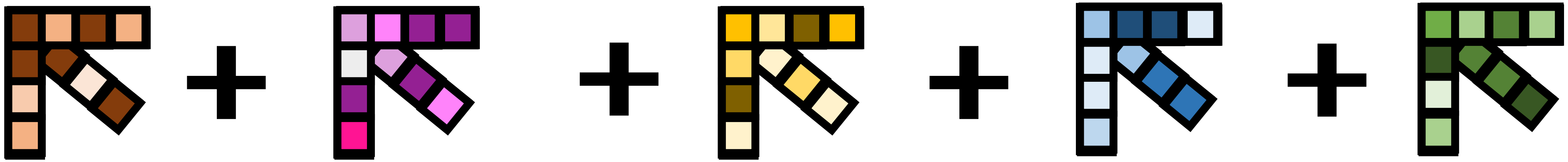
A rank decomposition

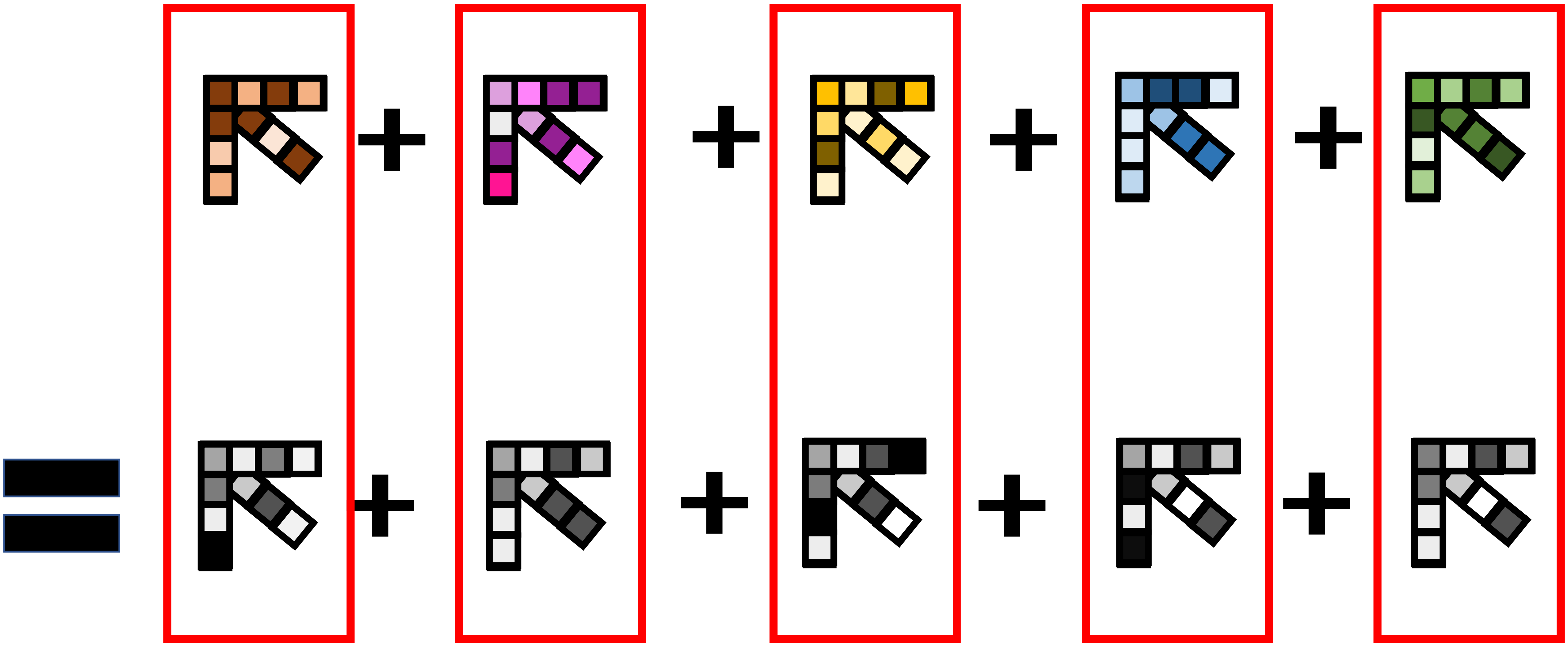
$$T = \sum_{i=1}^{R} v_i \otimes z_i \in V \otimes \mathbb{C}^m$$

is called the unique $(X, \mathbb{C}^m)$-(rank) decomposition of T if for any other decomposition

$$T = \sum_{i \in [R]} v_i' \otimes z_i' \in V \otimes \mathbb{C}^m$$

there is a permutation $\sigma \in S_R$ such that $v_i \otimes z_i = v'_{\sigma(i)} \otimes z'_{\sigma(i)}$ for all $i \in [R]$.





Application to $(\boldsymbol{X}, \mathbb{C}^m)$-decompositions (or simultaneous $\boldsymbol{X}$-decompositions)

Let $T \in V \otimes \mathbb{C}^m$ be a tensor.

If

$$T(\mathbb{C}^m) \text{ has a basis of the form } \{v_1, \dots, v_R\} \subseteq \mathrm{X},$$

Then $T = \sum_{i=1}^{R} v_i \otimes z_i$, where $z_i = T(v_i^*)$.

...So, algorithms for finding elements of $T(\mathbb{C}^m) \cap X$ lead to tensor decomposition algorithms

If $v_1, \dots, v_R$ are the only elements of $T(\mathbb{C}^m) \cap X$ (up to scale), then this is the unique rank decomposition of T.

Theorem [JLV]: If $X \subseteq \mathbb{C}^N$ is irreducible, cut out by $p = \delta\binom{N+d-1}{d}$ linearly independent homogeneous degree-d polynomials, and has no equations in degree $d-1$, then for a generic linear subspace $U \subseteq \mathbb{C}^N$ of dimension

$$\dim(U) \leq \frac{N+d-1}{d!}\delta,$$

containing $s \leq \dim(U)$ generic elements of X, our algorithm recovers these elements in time $N^{O(d)}$, and certifies that these are the only elements of $U \cap X$.

Algebraic def: There is a Zariski open dense subset $A \subseteq X^{\times s} \times (\mathbb{C}^n \otimes \mathbb{C}^n)^{\times R-s}$ s.t...

Corollary: A generic tensor $T \in V \otimes \mathbb{C}^m$ with

$$\mathrm{rank}_X(T) \leq \min\{\frac{N+d-1}{d!}\delta, m\}$$

has a unique $(X, \mathbb{C}^m)$-decomposition, which is recovered by applying our algorithm to $T(\mathbb{C}^m)$.

Proof: Say $T = \sum_{i=1}^{R} v_i \otimes z_i$

T generic, $R \leq m \quad \Rightarrow \quad \{z_1, \dots, z_R\}$ is linearly independent

$$\Rightarrow T(\mathbb{C}^m) = \mathrm{span}\{v_1, \dots, v_R\}$$

$T(\mathbb{C}^m)$ generic, $R \leq \frac{N+d-1}{d!}\delta \Rightarrow v_1, \dots, v_R$ are the only elements of $T(\mathbb{C}^m) \cap X$ (up to scale), and they are recovered by our algorithm

Other examples…

- Schmidt rank $\leq r$ vectors:

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

Recover $(X_r, \mathbb{C}^m)$ – decompositions of rank $\Omega_r(n^2)$

- Product tensors: $X_1 = \{v_1 \otimes \cdots \otimes v_{k/2} : v_1, \ldots, v_{k/2} \in \mathbb{C}^n\}$

Recover tensor decompositions in $(\mathbb{C}^n)^{\otimes k}$ of rank $\sim n^{k/2}$

- Biseparable tensors:

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

- Slice rank 1 tensors

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

Not irreducible!

Other examples…

- Schmidt rank $\leq r$ vectors:

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

Recover $(X_r, \mathbb{C}^m) - \text{decompositions of rank } \Omega_r(n^2)$

- Product tensors: $X_1 = \{v_1 \otimes \cdots \otimes v_k : v_1, \dots, v_m \in \mathbb{C}^n\}$

Recover tensor decompositions in $(\mathbb{C}^n)^{\otimes k}$ of rank $\sim n^{k/2}$

Related work:

[De Lathauwer, Castaing Cardoso 2007]: Algorithm to decompose symmetric fourth-order tensors

[De Lathauwer 2008]: Algorithm for $(X_r, \mathbb{C}^m)$-decompositions (also known as "block-term decompositions" and "r-aided ranks")

Our algorithm generalizes these to arbitrary varieties

The Algorithm (Inspired by Nullstellensatz Certificate)

Subroutine: Jennrich's Algorithm

<u>Input</u>: A basis $\{u_1, \dots, u_s\}$ for a subspace $U \subseteq \mathbb{C}^n \otimes \mathbb{C}^m$ of dimension $\dim(U) = s \leq n$

If U has a basis of the form $\{x_1 \otimes y_1, \dots, x_s \otimes y_s\}$,

where $\{x_1, \dots, x_s\}$ and $\{y_1, \dots, y_s\}$ are linearly independent

Then $x_1 \otimes y_1, \dots, x_s \otimes y_s$ are the only elements of $U \cap X_1$, and Jennrich's algorithm outputs these elements. Otherwise, it outputs FAIL.

Note: This version of Jennrich can only handle $\dim(U) \leq n$, whereas we can do $\dim(U) \leq \Omega(n^2)$

Recall the algorithm to determine if $U \cap X = \{0\}$...

$S^d(U) = U^{\otimes d} \cap S^d(V)$

Algorithm:

$= \mathrm{span}\{P_{d,V}^{\vee}(u_{i_1} \otimes \cdots \otimes u_{i_d}) : 1 \leq i_1 \leq \cdots \leq i_d \leq R\}$

1. If $\mathrm{Im}(\Psi_X^d) \cap S^d(U) = \{0\}$, output YES
2. Otherwise, output I DON'T KNOW

Idea: To find vectors in $U \cap X$, look at the vectors in $\mathrm{Im}(\Psi_X^d) \cap S^d(U)$.

If $v = \sum_{i=1}^R \alpha_i u_i \in U \cap X$, then

$$v^{\otimes d} = \sum_{i_1,\ldots,i_d} \alpha_{i_1} \cdots \alpha_{i_d} (u_{i_1} \otimes \cdots \otimes u_{i_d}) \in \mathrm{Im}(\Psi_X^d) \cap S^d(U) \qquad (1)$$

The tensor of coefficients $\alpha \in (\mathbb{C}^R)^{\otimes d}$ is a (symmetric) product tensor!

Take-home: vectors in $U \cap X$ $\leftrightarrow$ symmetric product tensors that solve (1)

Algorithm to find elements of $U \cap X$

1. Compute a basis $\{A_1, \dots, A_s\} \subseteq (\mathbb{C}^R)^{\otimes d}$ for the set of tensors $\alpha \in S^d(\mathbb{C}^R)$ s.t.

$$\sum_{i_1,\dots,i_d} \alpha_{i_1,\dots,i_d} \left(u_{i_1} \otimes \cdots \otimes u_{i_d}\right) \in \mathrm{Im}\left(\Psi_X^d\right) \cap S^d(U)$$

2. Find the symmetric product tensors in $\mathrm{span}\{A_1, \dots, A_s\} \subseteq (\mathbb{C}^R)^{\otimes d}$

New X!

New U!

Algorithm to find elements of $U \cap X$

1. Compute a basis $\{A_1, \dots, A_s\} \subseteq (\mathbb{C}^R)^{\otimes d}$ for the set of tensors $\alpha \in S^d(\mathbb{C}^R)$ s.t.

$$\sum_{i_1,\dots,i_d} \alpha_{i_1,\dots,i_d}(u_{i_1} \otimes \cdots \otimes u_{i_d}) \in \mathrm{Im}(\Psi_X^d) \cap S^d(U)$$

2. Find the symmetric product tensors in $\mathrm{span}\{A_1, \dots, A_s\} \subseteq (\mathbb{C}^R)^{\otimes d}$

1. Run Jennrich's algorithm on $\mathrm{span}\{A_1, \dots, A_s\} \subseteq \mathbb{C}^R \otimes ((\mathbb{C}^R)^{\otimes d-1})$

2. If Jennrich outputs a basis of the form $\{(\alpha^{(1)})^{\otimes d}, \dots, (\alpha^{(s)})^{\otimes d}\}$, then let $v_j := \sum_{i=1}^R \alpha_i^{(j)} u_i \in U \cap X$, and output the only elements of $U \cap X$ are $\{v_1, \dots, v_s\}$ (up to scale).

3. Otherwise, output FAIL.

Idea: Proving that this algorithm finds the elements of $U \cap X$ for generic U

- Recall: The algorithm takes a basis $\{u_1, \dots, u_R\}$ for U as input, and either outputs a basis $\{v_1, \dots, v_R\} \in X$ for U, or outputs FAIL.
- Our generic guarantee says that if $\{v_1, \dots, v_R\} \in X$ are chosen generically, then our algorithm recovers these elements from any basis $\{u_1, \dots, u_R\}$ of $U := \mathrm{span}\{v_1, \dots, v_R\}$.
- … It turns out that proving this is equivalent to proving that for generic $\{v_1, \dots, v_R\} \in X$, the intersection of $\mathrm{Im}\left(\Psi_X^d\right)$ with

$$\mathrm{span}\{P_{V,d}^{\vee}\left(v_{a_1} \otimes \cdots \otimes v_{a_d}\right) : 1 \leq a_1 \leq \cdots \leq a_d \leq R \text{ and not all } a_i \text{ are equal}\}$$

is zero.

- Compare with the genericity theorem in the $U \cap X = \{0\}$ algorithm: Reduces to proving that $\mathrm{Im}\left(\Psi_X^d\right) \cap S^d(U) = \{0\}$ for generic $\{u_1, \dots, u_R\} \in V$.

Conclusion

- Take home message 1: For an arbitrary variety $X \subseteq \mathbb{C}^N$, we can efficiently certify $U \cap X = \{0\}$ for a generic subspace $U \subseteq \mathbb{C}^N$ of dimension not too large. (First level of Nullstellensatz certificate)

- Take home message 2: This inspires a hierarchy of eigenvalue computations to compute the Hausdorff distance between U and X. (Robust version of Nullstellensatz certificate)

- Take home message 3*:* Also inspires an algorithm for finding elements of $U \cap X$, with similar genericity guarantees.

Open problems:

- Non-generic inputs U?
- Remove irreducibility/degree assumptions on the algorithm to find elements of $U \cap X$?

Nullstellensatz-inspired algorithms for certifying entanglement of subspaces

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

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

University of Western Ontario

November 30, 2022

arXiv:2210.16389