

How to solve?

Linear Algebra

system of linear
equations



Nonlinear Algebra

system of polynomial
equations

How to solve?

Linear Algebra

system of linear
equations



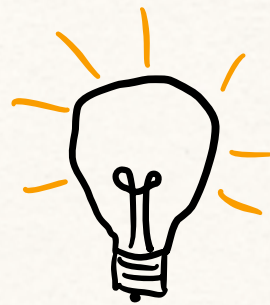
Gaussian
elimination

Nonlinear Algebra

system of polynomial
equations



Gröbner
bases

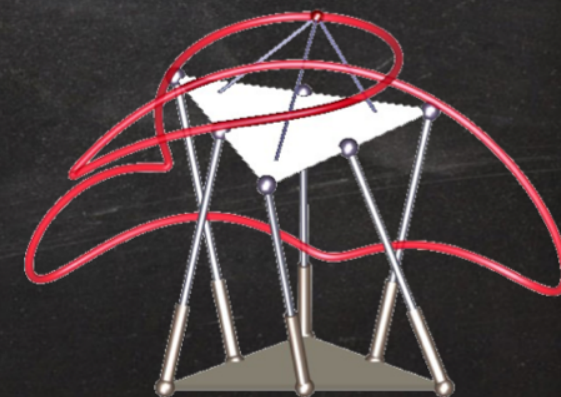
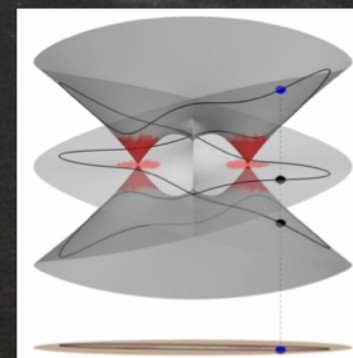
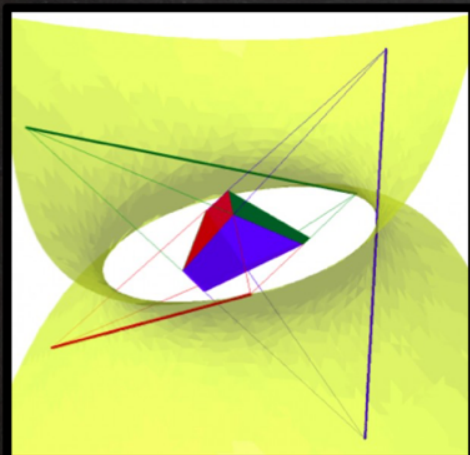
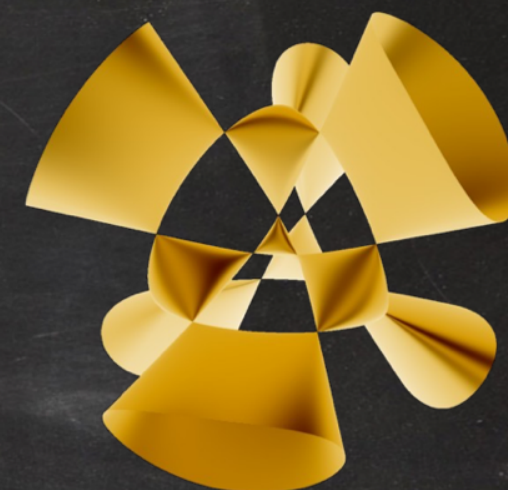


Nonlinear Algebra & Computer Vision



Kathlén Kohn

WASP | WALLENBERG
AUTONOMOUS SYSTEMS
AND SOFTWARE PROGRAM



Linear algebra

All undergraduate students learn about **Gaussian elimination**, a general method for solving linear systems of algebraic equations:

Input:

$$\begin{aligned}x + 2y + 3z &= 5 \\7x + 11y + 13z &= 17 \\19x + 23y + 29z &= 31\end{aligned}$$

Output:

$$\begin{aligned}x &= -35/18 \\y &= 2/9 \\z &= 13/6\end{aligned}$$

Solving very large linear systems is central to applied mathematics.

Nonlinear algebra

Lucky students also learn about **Gröbner bases**, a general method for non-linear systems of algebraic equations:

Input:

$$\begin{aligned}x^2 + y^2 + z^2 &= 2 \\x^3 + y^3 + z^3 &= 3 \\x^4 + y^4 + z^4 &= 4\end{aligned}$$

Output:

$$3z^{12} - 12z^{10} - 12z^9 + 12z^8 + 72z^7 - 66z^6 - 12z^4 + 12z^3 - 1 = 0$$

$$\begin{aligned}4y^2 + (36z^{11} + 54z^{10} - 69z^9 - 252z^8 - 216z^7 + 573z^6 + 72z^5 \\- 12z^4 - 99z^3 + 10z + 3)y + 36z^{11} + 48z^{10} - 72z^9 \\- 234z^8 - 192z^7 + 564z^6 - 48z^5 + 96z^4 - 96z^3 + 10z^2 + 8 = 0\end{aligned}$$

$$\begin{aligned}4x + 4y + 36z^{11} + 54z^{10} - 69z^9 - 252z^8 - 216z^7 \\+ 573z^6 + 72z^5 - 12z^4 - 99z^3 + 10z + 3 = 0\end{aligned}$$

This is very hard for large systems, but . . .

The world is non-linear!

Many models in the sciences and engineering are characterized by polynomial equations. Such a set is an **algebraic variety**.

- ♦ Algebraic statistics
- ♦ Machine learning
- ♦ Optimization
- ♦ **Computer vision**
- ♦ Robotics
- ♦ Complexity theory
- ♦ Cryptography
- ♦ Biology
- ♦ Economics
- ♦ ...



Nonlinear Algebra

Algebraic Geometry

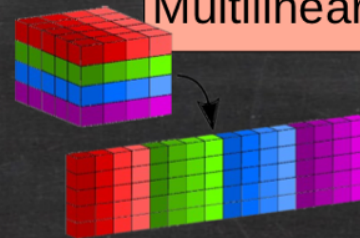


Combinatorics

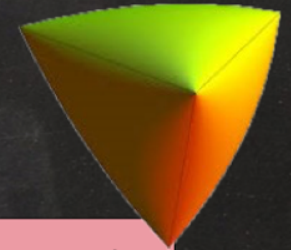
Discrete Geometry

Tropical Geometry

Multilinear Algebra



Convex Geometry



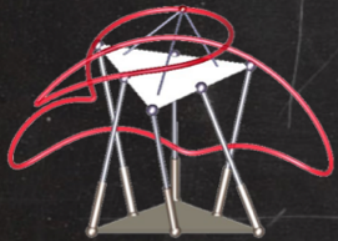
Algebraic Topology

Representation Theory

Numerics

Number Theory

...



Applications



Example: Solve the system $\begin{bmatrix} x^2 + y^2 + z^2 = 1 \\ x^2 + z^2 = y \\ x = z \end{bmatrix} !$

Example: Solve the system $\begin{bmatrix} x^2 + y^2 + z^2 = 1 \\ x^2 + z^2 = y \\ x = z \end{bmatrix} !$

2 Gröbner bases:

$$4z^4 + 2z^2 - 1 = 0$$

$$y - 2z^2 = 0$$

$$x - z = 0$$

$$y^2 + y - 1 = 0$$

$$2x^2 - y = 0$$

$$z - x = 0$$

Example: Solve the system $\begin{bmatrix} x^2 + y^2 + z^2 = 1 \\ x^2 + z^2 = y \\ x = z \end{bmatrix} !$

2 Gröbner bases:
analog to triangular form

$$4z^4 + 2z^2 - 1 = 0$$

$$y - 2z^2 = 0$$

$$x - z = 0$$

$$x > y > z$$

monomials ordered lexicographically

$$y^2 + y - 1 = 0$$

$$2x^2 - y = 0$$

$$z - x = 0$$

$$z > x > y$$

Example: Solve the system $\begin{bmatrix} x^2 + y^2 + z^2 = 1 \\ x^2 + z^2 = y \\ x = z \end{bmatrix} !$

2 Gröbner bases:

$$4z^4 + 2z^2 - 1 = 0$$

$$y - 2z^2 = 0$$

$$x - z = 0$$

$$y^2 + y - 1 = 0$$

$$2x^2 - y = 0$$

$$z - x = 0$$

$$x > y > z$$

monomials ordered lexicographically

$$z > x > y$$

$$\{(a, 2a^2, a) \mid 4a^4 + 2a^2 = 1\}$$

solutions



Example: Solve the system $\begin{bmatrix} x^2 + y^2 + z^2 = 1 \\ x^2 + z^2 = y \\ x = z \end{bmatrix} !$

2 Gröbner bases:

$$4z^4 + 2z^2 - 1 = 0$$

$$y - 2z^2 = 0$$

$$x - z = 0$$

$$y^2 + y - 1 = 0$$

$$2x^2 - y = 0$$

$$z - x = 0$$

$$x > y > z$$

monomials ordered lexicographically

$$z > x > y$$

$$\{(a, 2a^2, a) \mid 4a^4 + 2a^2 = 1\}$$

4 solutions

$$\left\{ \left(\pm \sqrt{\frac{b}{2}}, b, \pm \sqrt{\frac{b}{2}} \right) \mid b = -\frac{1}{2} \pm \frac{\sqrt{5}}{2} \right\}$$

Computing a Gröbner basis rewrites your polynomial system so that you can "read off" the solutions (e.g. by solving for one variable after another)

$\underbrace{z > x > y}$

```

1 QQ[z, x, y, MonomialOrder => Lex]
2 G = gb ideal {x^2 + y^2 + z^2 - 1, x^2 + z^2 - y, x - z}
3 gens G
  
```

Macaulay2 code

+

Symbolic (i.e., non-numeric)
methods

→ exact representation of solutions
→ provides proof

-

requires a lot of
computation time
and memory

Gröbner bases more formal

For $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$, we write $x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$

4
we need to
decide how
our monomials
are ordered

Definition: A monomial order $>$ on $\mathbb{C}[x]$ is defined by a total order $>$ on $\mathbb{Z}_{\geq 0}^n$ such that:

- (1) $\forall \alpha, \beta \in \mathbb{Z}_{\geq 0}^n: [\alpha > \beta \Rightarrow \forall \gamma \in \mathbb{Z}_{\geq 0}^n: \alpha + \gamma > \beta + \gamma]$ &
(2) every non-empty subset of $\mathbb{Z}_{\geq 0}^n$ has a smallest element under $>$.

- ↑
- | |
|--|
| <ul style="list-style-type: none">• $a \neq a$• $a > b \Rightarrow b \neq a$• $a > b, b > c \Rightarrow a > c$• $\forall a \neq b: a > b \text{ or } b > a$ |
|--|

Gröbner bases more formal

For $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$, we write $x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$

4
we need to
decide how
our monomials
are ordered

Definition: A monomial order $>$ on $\mathbb{C}[x]$ is defined by a total order $>$ on $\mathbb{Z}_{\geq 0}^n$ such that:

- (1) $\forall \alpha, \beta \in \mathbb{Z}_{\geq 0}^n: [\alpha > \beta \Rightarrow \forall \gamma \in \mathbb{Z}_{\geq 0}^n: \alpha + \gamma > \beta + \gamma]$ &
- (2) every non-empty subset of $\mathbb{Z}_{\geq 0}^n$ has a smallest element under $>$.

- ↑
- $a \neq a$
 - $a > b \Rightarrow b \neq a$
 - $a > b, b > c \Rightarrow a > c$
 - $\forall a \neq b: a > b \text{ or } b > a$

Example: lexicographic (lex) order:

For $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$, define $\alpha > \beta : \Leftrightarrow \alpha_j > \beta_j$, where $j := \min \{i \mid \alpha_i \neq \beta_i\}$.

$\hookrightarrow$ e.g., $x_1^2 x_2$? $x_1 x_2 x_3$

$x_1 x_3^7$? $x_1 x_2 x_3$

Gröbner bases more formal

For $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}_{\geq 0}^n$, we write $x^\alpha := x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$

4

we need to
decide how
our monomials
are ordered

Definition: A monomial order $>$ on $\mathbb{C}[x]$ is defined by a total order $>$ on $\mathbb{Z}_{\geq 0}^n$ such that:

- (1) $\forall \alpha, \beta \in \mathbb{Z}_{\geq 0}^n: [\alpha > \beta \Rightarrow \forall \gamma \in \mathbb{Z}_{\geq 0}^n: \alpha + \gamma > \beta + \gamma]$ &
- (2) every non-empty subset of $\mathbb{Z}_{\geq 0}^n$ has a smallest element under $>$.

- ↑
- $a \neq a$
 - $a > b \Rightarrow b \neq a$
 - $a > b, b > c \Rightarrow a > c$
 - $\forall a \neq b: a > b \text{ or } b > a$

Example: lexicographic (lex) order:

For $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$, define $\alpha > \beta : \Leftrightarrow \alpha_j > \beta_j$, where $j := \min \{i \mid \alpha_i \neq \beta_i\}$.

$\hookrightarrow$ e.g., $x_1^2 x_2 > x_1 x_2 x_3$
 $(2, 1, 0) > (1, 1, 1)$

$x_1 x_3^7 < x_1 x_2 x_3$
 $(1, 0, 7) < (1, 1, 1)$

Gröbner bases more formal

Fix a monomial order $>$ on $\mathbb{C}[x]$.⁵

Definition: Let $f \in \mathbb{C}[x]$, $f \neq 0$, and write $f = c_\alpha x^\alpha + c_\beta x^\beta + \dots$,
where $\alpha > \beta > \dots$ and $c_\alpha, c_\beta, \dots \in \mathbb{C} \setminus \{0\}$.
The **leading term** of f is $LT(f) := c_\alpha x^\alpha$.

Remark: Property (1) $\leftarrow [\alpha > \beta \Rightarrow \forall \gamma \in \mathbb{Z}_{\geq 0}^n: \alpha + \gamma > \beta + \gamma]$

in Def. of monomial order implies: $LT(f \cdot x^\delta) = LT(f) \cdot x^\delta$

Gröbner bases more formal

Fix a monomial order $>$ on $\mathbb{C}[x]$.⁵

Definition: Let $f \in \mathbb{C}[x]$, $f \neq 0$, and write $f = c_\alpha x^\alpha + c_\beta x^\beta + \dots$,
where $\alpha > \beta > \dots$ and $c_\alpha, c_\beta, \dots \in \mathbb{C} \setminus \{0\}$.
The **leading term** of f is $\text{LT}(f) := c_\alpha x^\alpha$.

Remark: Property (1) $\leftarrow [\alpha > \beta \Rightarrow \forall \gamma \in \mathbb{Z}_{\geq 0}^n: \alpha + \gamma > \beta + \gamma]$

in Def. of monomial order implies: $\text{LT}(f \cdot x^\delta) = \text{LT}(f) \cdot x^\delta$

Definition: Let $\mathcal{I} \subseteq \mathbb{C}[x]$ be an ideal.

- The **leading term ideal** of $\mathcal{I}$ is $\text{LT}(\mathcal{I}) := \langle \{\text{LT}(f) \mid f \in \mathcal{I}, f \neq 0\} \rangle$.
-

Gröbner bases more formal

Fix a monomial order $>$ on $\mathbb{C}[x]$.⁵

Definition: Let $f \in \mathbb{C}[x]$, $f \neq 0$, and write $f = c_\alpha x^\alpha + c_\beta x^\beta + \dots$,
where $\alpha > \beta > \dots$ and $c_\alpha, c_\beta, \dots \in \mathbb{C} \setminus \{0\}$.
The **leading term** of f is $\text{LT}(f) := c_\alpha x^\alpha$.

Remark: Property (1) $\leftarrow [\alpha > \beta \Rightarrow \forall \gamma \in \mathbb{Z}_{\geq 0}^n: \alpha + \gamma > \beta + \gamma]$

in Def. of monomial order implies: $\text{LT}(f \cdot x^\delta) = \text{LT}(f) \cdot x^\delta$

Definition: Let $\mathcal{I} \subseteq \mathbb{C}[x]$ be an ideal.

- The **leading term ideal** of $\mathcal{I}$ is $\text{LT}(\mathcal{I}) := \langle \{\text{LT}(f) \mid f \in \mathcal{I}, f \neq 0\} \rangle$.
- A **Gröbner basis** for $\mathcal{I}$ with respect to $>$ is a finite subset $G \subseteq \mathcal{I}$ s.t. $\langle \{\text{LT}(g) \mid g \in G\} \rangle = \text{LT}(\mathcal{I})$.

Gröbner bases more formal

Fix a monomial order $>$ on $\mathbb{C}[x]$.

Definition: Let $f \in \mathbb{C}[x]$, $f \neq 0$, and write $f = c_\alpha x^\alpha + c_\beta x^\beta + \dots$,
where $\alpha > \beta > \dots$ and $c_\alpha, c_\beta, \dots \in \mathbb{C} \setminus \{0\}$.
The **leading term** of f is $\text{LT}(f) := c_\alpha x^\alpha$.

Remark: Property (1) $\leftarrow [\alpha > \beta \Rightarrow \forall \gamma \in \mathbb{Z}_{\geq 0}^n: \alpha + \gamma > \beta + \gamma]$

in Def. of monomial order implies: $\text{LT}(f \cdot x^\delta) = \text{LT}(f) \cdot x^\delta$

Definition: Let $\mathcal{I} \subseteq \mathbb{C}[x]$ be an ideal.

- The **leading term ideal** of $\mathcal{I}$ is $\text{LT}(\mathcal{I}) := \langle \{ \text{LT}(f) \mid f \in \mathcal{I}, f \neq 0 \} \rangle$.
- A **Gröbner basis** for $\mathcal{I}$ with respect to $>$ is a finite subset $G \subseteq \mathcal{I}$ s.t. $\langle \{ \text{LT}(g) \mid g \in G \} \rangle = \text{LT}(\mathcal{I})$.

Exercise: $\langle G \rangle = \mathcal{I}$ $\leftarrow$ this justifies the name "basis"

Example: $I = \langle x^2 + y^2 + z^2 - 1, \\ x^2 + z^2 - y, \\ x - z \rangle$

$$\langle LT(g) \mid g \in G \rangle \\ = \langle LT(f) \mid f \in I \setminus \{0\} \rangle$$

2 Gröbner bases:

Lex order $x > y > z$:

$$G = \{ 4z^4 + 2z^2 - 1, \\$$

$$\begin{array}{l} \text{leading} \nearrow \\ \text{terms} \longrightarrow \end{array} \left\{ \begin{array}{l} y - 2z^2, \\ x - z \end{array} \right\}$$

Lex order $z > x > y$:

$$G = \{ y^2 + y - 1, \\$$

$$\begin{array}{l} \text{leading} \nearrow \\ \text{terms} \longrightarrow \end{array} \left\{ \begin{array}{l} 2x^2 - y, \\ z - x \end{array} \right\}$$

Example: $I = \langle x^2 + y^2 + z^2 - 1, \\ x^2 + z^2 - y, \\ x - z \rangle$

$$\langle LT(g) \mid g \in G \rangle \\ = \langle LT(f) \mid f \in I \setminus \{0\} \rangle$$

2 Gröbner bases:

Lex order $x > y > z$:

$$G = \{ 4z^4 + 2z^2 - 1, \\ y - 2z^2, \\ x - z \}$$

leading terms $\nearrow$

$$x^2 + y^2 + z^2 - 1, \\ x^2 + z^2 - y, \\ x - z$$

Lex order $z > x > y$:

$$G = \{ y^2 + y - 1, \\ 2x^2 - y, \\ z - x \}$$

leading terms $\nearrow$

leading terms
of original equations

$$x^2 + y^2 + z^2 - 1, \\ x^2 + z^2 - y, \\ x - z$$

Example: $I = \langle x^2 + y^2 + z^2 - 1, \\ x^2 + z^2 - y, \\ x - z \rangle$

$$\langle LT(g) \mid g \in G \rangle \\ = \langle LT(f) \mid f \in I \setminus \{0\} \rangle$$

2 Gröbner bases:

Lex order $x > y > z$:

$$G = \{ 4z^4 + 2z^2 - 1, \\ y - 2z^2, \\ x - z \}$$

leading terms $\nearrow$

Lex order $z > x > y$:

$$G = \{ y^2 + y - 1, \\ 2x^2 - y, \\ z - x \}$$

leading terms $\nearrow$

$$x^2 + y^2 + z^2 - 1, \\ x^2 + z^2 - y, \\ x - z$$

leading terms
of original equations
do NOT generate $LT(I)$

$$x^2 + y^2 + z^2 - 1, \\ x^2 + z^2 - y, \\ x - z$$

Example: $\mathcal{I} = \langle x^2 + y^2 + z^2 - 1, \\ x^2 + z^2 - y, \\ x - z \rangle$

allow to solve $\mathcal{I}$ by sequentially solving univariate polynomials!

$$\langle \text{LT}(g) \mid g \in G \rangle \\ = \langle \text{LT}(f) \mid f \in \mathcal{I} \setminus \{0\} \rangle$$

2 Gröbner bases:

Lex order $x > y > z$:

$$G = \{ 4z^4 + 2z^2 - 1, \\ y - 2z^2, \\ x - z \}$$

leading terms $\nearrow$

Lex order $z > x > y$:

$$G = \{ y^2 + y - 1, \\ 2x^2 - y, \\ z - x \}$$

leading terms $\nearrow$

$$x^2 + y^2 + z^2 - 1, \\ x^2 + z^2 - y, \\ x - z$$

leading terms
of original equations
do NOT generate $\text{LT}(\mathcal{I})$

$$x^2 + y^2 + z^2 - 1, \\ x^2 + z^2 - y, \\ x - z$$

Gröbner bases w.r.t. Lex orders enable to solve ideals with finitely many solution by sequentially solving univariate polynomials

Gröbner bases w.r.t. Lex orders enable to solve ideals with finitely many solution by sequentially solving univariate polynomials

Let $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ be an ideal with finitely many solutions.

For $0 \leq j < n$, define $I_j := I \cap \mathbb{C}[x_{j+1}, \dots, x_n]$.

Proposition: I_j is a non-zero ideal in $\mathbb{C}[x_{j+1}, \dots, x_n]$.

Gröbner bases w.r.t. Lex orders enable to solve ideals with finitely many solutions by sequentially solving univariate polynomials

Let $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ be an ideal with finitely many solutions.

For $0 \leq j < n$, define $I_j := I \cap \mathbb{C}[x_{j+1}, \dots, x_n]$.
 known as j -th elimination ideal

Proposition: I_j is a non-zero ideal in $\mathbb{C}[x_{j+1}, \dots, x_n]$.

Elimination Theorem:

If $G \in I$ is a Gröbner basis for I w.r.t. the Lex order with $x_1 > \dots > x_n$, then $G_j := G \cap \mathbb{C}[x_{j+1}, \dots, x_n]$ is a Gröbner basis for I_j .

Gröbner bases w.r.t. Lex orders enable to solve ideals with finitely many solutions by sequentially solving univariate polynomials

Let $I \subseteq \mathbb{C}[x_1, \dots, x_n]$ be an ideal with finitely many solutions.

For $0 \leq j < n$, define $I_j := I \cap \mathbb{C}[x_{j+1}, \dots, x_n]$.
known as j -th elimination ideal

Proposition: I_j is a non-zero ideal in $\mathbb{C}[x_{j+1}, \dots, x_n]$.

Elimination Theorem:

If $G \in I$ is a Gröbner basis for I w.r.t. the Lex order with $x_1 > \dots > x_n$, then $G_j := G \cap \mathbb{C}[x_{j+1}, \dots, x_n]$ is a Gröbner basis for I_j .

Corollary: Solve I by sequentially solving the univariate equations in $G_{n-1}, G_{n-2}, \dots, G_0 = G$.
the equations in G_j become univariate in x_{j+1} after substituting $x_{j+2}, \dots, x_n$ by the solutions of G_{j+1}

Solving univariate polynomials

For $f = x^d + c_{d-1}x^{d-1} + \dots + c_1x + c_0 \in \mathbb{C}[x]$, define

companion matrix $C(f) := \begin{bmatrix} 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & \dots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -c_{d-1} \end{bmatrix} \in \mathbb{C}^{d \times d}.$

For $z \in \mathbb{C}$: $f(z) = 0 \iff z$ is eigenvalue of $C(f)$.

Solving univariate polynomials

For $f = x^d + c_{d-1}x^{d-1} + \dots + c_1x + c_0 \in \mathbb{C}[x]$, define

companion matrix $C(f) := \begin{bmatrix} 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & \dots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -c_{d-1} \end{bmatrix} \in \mathbb{C}^{d \times d}.$

For $z \in \mathbb{C}$: $f(z) = 0 \iff z$ is eigenvalue of $C(f)$.

Reason:

Exercise: $\det(xI - C(f)) = f(x)$.

Counting Solutions

Sometimes, we want proof of how many solutions a given equation system has, e.g. to estimate the complexity of solving it or to establish that numerical methods (polynomial homotopy continuation / monodromy) have found all solutions.

Counting Solutions

Sometimes, we want proof of how many solutions a given equation system has, e.g. to estimate the complexity of solving it or to establish that numerical methods (polynomial homotopy continuation / monodromy) have found all solutions.

Let $\mathcal{I} \subseteq \mathbb{C}[\mathbf{x}] = \mathbb{C}[x_1, \dots, x_n]$ be an ideal & $\succ$ a monomial order.

Definition: $\mathbf{x}^\alpha$ is a **standard monomial** of $\mathcal{I}$ w.r.t. $\succ$ if $\mathbf{x}^\alpha \notin \text{LT}(\mathcal{I})$.

Counting Solutions

Sometimes, we want proof of how many solutions a given equation system has, e.g. to estimate the complexity of solving it or to establish that numerical methods (polynomial homotopy continuation / monodromy) have found all solutions.

Let $\mathcal{I} \subseteq \mathbb{C}[x] = \mathbb{C}[x_1, \dots, x_n]$ be an ideal & $\succ$ a monomial order.

Definition: x^α is a **standard monomial** of $\mathcal{I}$ w.r.t. $\succ$ if $x^\alpha \notin \text{LT}(\mathcal{I})$.

Theorem: Let S be the set of standard monomials of $\mathcal{I}$ w.r.t. $\succ$. Then:

① $|S| < \infty \iff |\mathcal{Z}(\mathcal{I})| < \infty$

② If $|S| < \infty$, then $|S| = \text{number of points in } \mathcal{Z}(\mathcal{I}) \subseteq \mathbb{C}^n$
counting multiplicities.

Counting Solutions

Sometimes, we want proof of how many solutions a given equation system has, e.g. to estimate the complexity of solving it or to establish that numerical methods (polynomial homotopy continuation / monodromy) have found all solutions.

Let $\mathcal{I} \subseteq \mathbb{C}[x] = \mathbb{C}[x_1, \dots, x_n]$ be an ideal & $>$ a monomial order.

Definition: x^α is a **standard monomial** of $\mathcal{I}$ w.r.t. $>$ if $x^\alpha \notin \text{LT}(\mathcal{I})$.

Theorem: Let S be the set of standard monomials of $\mathcal{I}$ w.r.t. $>$. Then:

① $|S| < \infty \iff |\mathcal{Z}(\mathcal{I})| < \infty$

② If $|S| < \infty$, then $|S| = \text{number of points in } \mathcal{Z}(\mathcal{I}) \subseteq \mathbb{C}^n$
counting multiplicities.

$|S|$ can be read off from a Gröbner basis! 😊

Example: $I = \langle x^2 + y^2 + z^2 - 1, \\ x^2 + z^2 - y, \\ x - z \rangle$

$$\langle LT(g) \mid g \in G \rangle = LT(I)$$

2 Gröbner bases:

Lex order $x > y > z$:

$$G = \{ 4z^4 + 2z^2 - 1, \\$$

leading terms $\rightarrow y - 2z^2, \\ x - z \}$

Lex order $z > x > y$:

$$G = \{ y^2 + y - 1, \\$$

leading terms $\rightarrow 2x^2 - y, \\ z - x \}$

What are the
standard monomials
?

Example: $I = \langle x^2 + y^2 + z^2 - 1, \\ x^2 + z^2 - y, \\ x - z \rangle$

$$\langle LT(g) \mid g \in G \rangle = LT(I)$$

2 Gröbner bases:

Lex order $x > y > z$:

$$G = \{ 4z^4 + 2z^2 - 1, \\ y - 2z^2, \\ x - z \}$$

leading terms $\rightarrow$

Lex order $z > x > y$:

$$G = \{ y^2 + y - 1, \\ 2x^2 - y, \\ z - x \}$$

leading terms $\rightarrow$

What are the
standard monomials
?

Exercise: $x^\beta \in \langle x^{\alpha_1}, \dots, x^{\alpha_k} \rangle \Leftrightarrow \exists i: x^{\alpha_i} \mid x^\beta$

Example: $I = \langle x^2 + y^2 + z^2 - 1, \\ x^2 + z^2 - y, \\ x - z \rangle$

$$\langle LT(g) \mid g \in G \rangle = LT(I)$$

2 Gröbner bases:

Lex order $x > y > z$:

$$G = \{ 4z^4 + 2z^2 - 1, \\ y - 2z^2, \\ x - z \}$$

leading terms $\rightarrow y - 2z^2, \\ x - z$

$$1, z, z^2, z^3$$

Lex order $z > x > y$:

$$G = \{ y^2 + y - 1, \\ 2x^2 - y, \\ z - x \}$$

leading terms $\rightarrow y^2 + y - 1, \\ 2x^2 - y, \\ z - x$

$$1, x, y, xy$$

What are the
standard monomials
?

Exercise: $x^\beta \in \langle x^{\alpha_1}, \dots, x^{\alpha_k} \rangle \Leftrightarrow \exists i: x^{\alpha_i} \mid x^\beta$

Example: $I = \langle x^2 + y^2 + z^2 - 1, \\ x^2 + z^2 - y, \\ x - z \rangle$

$$\langle LT(g) \mid g \in G \rangle = LT(I)$$

2 Gröbner bases:

Lex order $x > y > z$:

$$G = \{ 4z^4 + 2z^2 - 1, \\ y - 2z^2, \\ x - z \}$$

leading terms $\rightarrow y - 2z^2, \\ x - z$

$$1, z, z^2, z^3$$

4 solutions

Lex order $z > x > y$:

$$G = \{ y^2 + y - 1, \\ 2x^2 - y, \\ z - x \}$$

leading terms $\rightarrow y^2 + y - 1, \\ z - x$

$$1, x, y, xy$$

4 solutions

What are the
standard monomials
?

Exercise: $x^\beta \in \langle x^{\alpha_1}, \dots, x^{\alpha_k} \rangle \Leftrightarrow \exists i: x^{\alpha_i} \mid x^\beta$

Example: $\mathcal{I} = \langle x^d + c_{d-1}x^{d-1} + \dots + c_1x + c_0 \rangle$

Exercise: There is just one monomial ordering $>$ on univariate monomials: $\dots > x^3 > x^2 > x > 1$.

What is $\text{LT}(\mathcal{I})$?

What are the standard monomials?

Example: $\mathcal{I} = \langle x^d + c_{d-1}x^{d-1} + \dots + c_1x + c_0 \rangle$

Exercise: There is just one monomial ordering $>$ on univariate monomials: $\dots > x^3 > x^2 > x > 1$.

What is $LT(\mathcal{I})$?

$$LT(\mathcal{I}) = \langle x^d \rangle$$

What are the standard monomials?

Example: $\mathcal{I} = \langle x^d + c_{d-1}x^{d-1} + \dots + c_1x + c_0 \rangle$

Exercise: There is just one monomial ordering $>$ on univariate monomials: $\dots > x^3 > x^2 > x > 1$.

What is $LT(\mathcal{I})$?

$$LT(\mathcal{I}) = \langle x^d \rangle$$

What are the standard monomials?

$$1, x, \dots, x^{d-1}$$

Example: $\mathcal{I} = \langle x^d + c_{d-1}x^{d-1} + \dots + c_1x + c_0 \rangle$

Exercise: There is just one monomial ordering $>$ on univariate monomials: $\dots > x^3 > x^2 > x > 1$.

What is $LT(\mathcal{I})$?

$$LT(\mathcal{I}) = \langle x^d \rangle$$

What are the standard monomials?

$$1, x, \dots, x^{d-1}$$

Corollary: A complex univariate polynomial of degree d has d complex solutions (counted with multiplicity).

This is the Fundamental Theorem of Algebra!

Example: $\mathcal{I} = \langle x^d + c_{d-1}x^{d-1} + \dots + c_1x + c_0 \rangle$

Exercise: There is just one monomial ordering $>$ on univariate monomials: $\dots > x^3 > x^2 > x > 1$.

What is $LT(\mathcal{I})$?

$$LT(\mathcal{I}) = \langle x^d \rangle$$

What are the standard monomials?

$$1, x, \dots, x^{d-1}$$

Corollary: A complex univariate polynomial of degree d has d complex solutions (counted with multiplicity).

This is the Fundamental Theorem of Algebra!

Ex.: $x^2 + 1 = 0$ has 2 distinct solutions,
 $x^2 = 0$ has 1 solution of multiplicity 2

Example:

$\swarrow x > y$

```

QQ[x,y, MonomialOrder => Lex]
I = ideal {(x-1)*(x-2)*(x^2+y^2-1), (y-1)*(y-3)*(x^2+y^2-1)}
G = gb I
transpose gens G

```

∞ many solutions

output:

$$\begin{pmatrix} x^2y^2 - 4x^2y + 3x^2 + y^4 - 4y^3 + 2y^2 + 4y - 3 \\ x^4 - 3x^3 + 4x^2y - 2x^2 - 3xy^2 + 3x - y^4 + 4y^3 - 4y + 1 \end{pmatrix}$$

What is $LT(I)$?

What are the standard monomials?

Example:

$\swarrow x > y$

```

QQ[x,y, MonomialOrder => Lex]
I = ideal {(x-1)*(x-2)*(x^2+y^2-1), (y-1)*(y-3)*(x^2+y^2-1)}
G = gb I
transpose gens G

```

∞ many solutions

output:

$$\begin{pmatrix} x^2 y^2 - 4x^2 y + 3x^2 + y^4 - 4y^3 + 2y^2 + 4y - 3 \\ x^4 - 3x^3 + 4x^2 y - 2x^2 - 3xy^2 + 3x - y^4 + 4y^3 - 4y + 1 \end{pmatrix}$$

What is $LT(I)$?

$$LT(I) = \langle x^4, x^2 y^2 \rangle$$

What are the standard monomials?

Example:

$\swarrow x > y$

```

QQ[x,y, MonomialOrder => Lex]
I = ideal {(x-1)*(x-2)*(x^2+y^2-1), (y-1)*(y-3)*(x^2+y^2-1)}
G = gb I
transpose gens G

```

∞ many solutions

output:

$$\begin{pmatrix} x^2 y^2 - 4x^2 y + 3x^2 + y^4 - 4y^3 + 2y^2 + 4y - 3 \\ x^4 - 3x^3 + 4x^2 y - 2x^2 - 3xy^2 + 3x - y^4 + 4y^3 - 4y + 1 \end{pmatrix}$$

What is $LT(I)$?

$$LT(I) = \langle x^4, x^2 y^2 \rangle$$

What are the standard monomials?

$\downarrow$

$$1, x, x^2, x^3, y, xy, x^2y, x^3y, y^2, xy^2, y^3, xy^3, y^4, xy^4, \dots$$

Counting Solutions

Fundamental Theorem of Algebra: 1 complex polynomial in 1 variable has $\deg(f)$ many solutions (counted with multiplicities).

What about 2 polynomials in 2 variables?
Or n polynomials in n variables?

Counting Solutions

Fundamental Theorem of Algebra: 1 complex polynomial in 1 variable has $\deg(f)$ many solutions (counted with multiplicities).

What about 2 polynomials in 2 variables?
Or n polynomials in n variables?

Theorem: A general system $f_1(x) = 0, \dots, f_n(x) = 0$ of n complex polynomials in n variables has $\deg(f_1) \cdot \deg(f_2) \cdots \deg(f_n)$ solutions in $\mathbb{C}^n$ (each of multiplicity 1).

Counting Solutions

Fundamental Theorem of Algebra: Every complex polynomial in 1 variable has $\deg(f)$ many solutions (counted with multiplicities).

What about 2 polynomials in 2 variables?
Or n polynomials in n variables?

Theorem: A general system $f_1(x) = 0, \dots, f_n(x) = 0$ of n complex polynomials in n variables has $\deg(f_1) \cdot \deg(f_2) \cdots \deg(f_n)$ solutions in $\mathbb{C}^n$ (each of multiplicity 1).

Recall:

Let $\mathbf{x} = (x_1, \dots, x_n)$, $\mathbf{p} = (p_1, \dots, p_k)$,
 $\uparrow$ variables $\uparrow$ parameters

$\mathcal{F} = \{f_1(\mathbf{x}, \mathbf{p}), \dots, f_n(\mathbf{x}, \mathbf{p})\} \subseteq \mathbb{C}[x_1, \dots, x_n, p_1, \dots, p_k]$
 parametrized family of square polynomial systems.

For $\mathbf{p} \in \mathbb{C}^k$, let $N(\mathbf{p})$ be the number of regular zeros of $\mathcal{F}$ at $\mathbf{p}$.

$$N := \sup_{\mathbf{p} \in \mathbb{C}^k} N(\mathbf{p})$$

Parameter Continuation Theorem: $N < \infty$ &
 there is a proper algebraic subvariety $\Delta \subsetneq \mathbb{C}^k$ such that
 $N(\mathbf{p}) = N$ for all $\mathbf{p} \notin \Delta$.

Recall:

Let $\mathbf{x} = (x_1, \dots, x_n)$, $\mathbf{p} = (p_1, \dots, p_k)$,
 $\uparrow$ variables $\uparrow$ parameters

$\mathcal{F} = \{f_1(\mathbf{x}, \mathbf{p}), \dots, f_n(\mathbf{x}, \mathbf{p})\} \subseteq \mathbb{C}[x_1, \dots, x_n, p_1, \dots, p_k]$
 parametrized family of square polynomial systems.

For $\mathbf{p} \in \mathbb{C}^k$, let $N(\mathbf{p})$ be the number of regular zeros of $\mathcal{F}$ at $\mathbf{p}$.

$$N := \sup_{\mathbf{p} \in \mathbb{C}^k} N(\mathbf{p})$$

Parameter Continuation Theorem: $N < \infty$ &
 there is a proper algebraic subvariety $\Delta \subsetneq \mathbb{C}^k$ such that
 $N(\mathbf{p}) = N$ for all $\mathbf{p} \notin \Delta$.

For $f_i = \sum_{\alpha \in \mathbb{Z}_{\geq 0}^n} p_{i,\alpha} \mathbf{x}^\alpha$, $N = \deg(f_1) \cdots \deg(f_n)$.
 $\nwarrow$ every coefficient is an independent parameter

Recall:

Let $\mathbf{x} = (x_1, \dots, x_n)$, $\mathbf{p} = (p_1, \dots, p_k)$,
 $\uparrow$ variables $\uparrow$ parameters

$\mathcal{F} = \{f_1(\mathbf{x}, \mathbf{p}), \dots, f_n(\mathbf{x}, \mathbf{p})\} \subseteq \mathbb{C}[x_1, \dots, x_n, p_1, \dots, p_k]$
 parametrized family of square polynomial systems.

For $\mathbf{p} \in \mathbb{C}^k$, let $N(\mathbf{p})$ be the number of regular zeros of $\mathcal{F}$ at $\mathbf{p}$.

$$N := \sup_{\mathbf{p} \in \mathbb{C}^k} N(\mathbf{p})$$

Parameter Continuation Theorem: $N < \infty$ &
 there is a proper algebraic subvariety $\Delta \subsetneq \mathbb{C}^k$ such that
 $N(\mathbf{p}) = N$ for all $\mathbf{p} \notin \Delta$.

For $f_i = \sum_{\alpha \in \mathbb{Z}_{\geq 0}^n} p_{i,\alpha} \mathbf{x}^\alpha$, $N = \deg(f_1) \cdots \deg(f_n)$.
 $\swarrow$ every coefficient is an independent parameter

Corollary: Every system of n complex polynomials $f_1, \dots, f_n$ in n variables has at most $\deg(f_1) \cdots \deg(f_n)$ regular zeros in $\mathbb{C}^n$.

Example

The system $\begin{bmatrix} x_1^{d_1} - 1 = 0 \\ \vdots \\ x_n^{d_n} - 1 = 0 \end{bmatrix}$ has $d_1 \cdots d_n$ distinct complex zeros:

$(\omega_1^{k_1}, \dots, \omega_n^{k_n})$, where ω_i is a primitive d_i -th root of unity & $k_i = 1, \dots, d_i$

Example

The system $\begin{bmatrix} x_1^{d_1} - 1 = 0 \\ \vdots \\ x_n^{d_n} - 1 = 0 \end{bmatrix}$ has $d_1 \cdots d_n$ distinct complex zeros:

$(\omega_1^{k_1}, \dots, \omega_n^{k_n})$, where ω_i is a primitive d_i -th root of unity & $k_i = 1, \dots, d_i$

Every root is regular:

$$\det \begin{bmatrix} d_1 \omega_1^{k_1(d_1-1)} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ 0 & \cdots & d_n \omega_n^{k_n(d_n-1)} & 0 \end{bmatrix} \neq 0$$

Example

The system $\begin{bmatrix} x_1^{d_1} - 1 = 0 \\ \vdots \\ x_n^{d_n} - 1 = 0 \end{bmatrix}$ has $d_1, \dots, d_n$ distinct complex zeros:

$(\omega_1^{k_1}, \dots, \omega_n^{k_n})$, where ω_i is a primitive d_i -th root of unity & $k_i = 1, \dots, d_i$

Every root is regular:

$$\det \begin{bmatrix} d_1 \omega_1^{k_1(d_1-1)} & \circ & \circ \\ \circ & \ddots & \circ \\ \circ & \circ & d_n \omega_n^{k_n(d_n-1)} \end{bmatrix} \neq 0$$

Corollary: This system can be used as a **start system** to solve a target system of n equations in n variables via polynomial homotopy continuation (as explained in last lecture).

Proposition 3.27 Let $\mathcal{F}$ be a family of polynomial systems with k parameters. Let $N \geq 2$ and Δ be as in Theorem 3.18. Given $\mathbf{q} \in \mathbb{C}^k \setminus \Delta$ and $\mathbf{p} \in \mathbb{C}^k$, for almost all choices of $\mathbf{p}_{\text{mid}} \in \mathbb{C}^k$, the piecewise linear path

$$\gamma(t) = \begin{cases} (2t-1)\mathbf{q} + 2(1-t)\mathbf{p}_{\text{mid}} & \text{if } \frac{1}{2} \leq t \leq 1, \\ 2t\mathbf{p}_{\text{mid}} + (1-2t)\mathbf{p} & \text{if } 0 < t \leq \frac{1}{2}, \end{cases}$$

satisfies:

- (a) $\gamma((0, 1]) \cap \Delta = \emptyset$.
- (b) The homotopy $H(\mathbf{x}, t) := F(\mathbf{x}; \gamma(t))$ defines N smooth curves $\mathbf{x}(t)$ with the property that $H(\mathbf{x}(t), t) = 0$ for $0 < t \leq 1$. These curves are called solution paths.
- (c) As $t \rightarrow 0$, the limits of the solution paths include all regular solutions of $F(\mathbf{x}; \mathbf{p}) = 0$.
- (d) If moreover $\gamma(0) \notin \Delta$, then every solution path $\mathbf{x}(t)$ converges for $t \rightarrow 0$ to a regular zero of $F(\mathbf{x}; \mathbf{p})$.

"total degree
start system"

Example

The system $\begin{bmatrix} x_1^{d_1} - 1 = 0 \\ \vdots \\ x_n^{d_n} - 1 = 0 \end{bmatrix}$ has $d_1, \dots, d_n$ distinct complex zeros:

$(\omega_1^{k_1}, \dots, \omega_n^{k_n})$, where ω_i is a primitive d_i -th root of unity & $k_i = 1, \dots, d_i$

Every root is regular:

$$\det \begin{bmatrix} d_1 \omega_1^{k_1(d_1-1)} & & 0 \\ & \ddots & \\ 0 & & d_n \omega_n^{k_n(d_n-1)} \end{bmatrix} \neq 0$$

Corollary: This system can be used as a **start system** to solve a target system of n equations in n variables via polynomial homotopy continuation (as explained in last lecture).

Proposition 3.27 Let $\mathcal{F}$ be a family of polynomial systems with k parameters. Let $N \geq 2$ and Δ be as in Theorem 3.18. Given $\mathbf{q} \in \mathbb{C}^k \setminus \Delta$ and $\mathbf{p} \in \mathbb{C}^k$, for almost all choices of $\mathbf{p}_{\text{mid}} \in \mathbb{C}^k$, the piecewise linear path

$$\gamma(t) = \begin{cases} (2t-1)\mathbf{q} + 2(1-t)\mathbf{p}_{\text{mid}} & \text{if } \frac{1}{2} \leq t \leq 1, \\ 2t\mathbf{p}_{\text{mid}} + (1-2t)\mathbf{p} & \text{if } 0 < t \leq \frac{1}{2}, \end{cases}$$

satisfies:

- (a) $\gamma((0, 1]) \cap \Delta = \emptyset$.
- (b) The homotopy $H(\mathbf{x}, t) := F(\mathbf{x}; \gamma(t))$ defines N smooth curves $\mathbf{x}(t)$ with the property that $H(\mathbf{x}(t), t) = 0$ for $0 < t \leq 1$. These curves are called solution paths.
- (c) As $t \rightarrow 0$, the limits of the solution paths include all regular solutions of $F(\mathbf{x}; \mathbf{p}) = 0$.
- (d) If moreover $\gamma(0) \notin \Delta$, then every solution path $\mathbf{x}(t)$ converges for $t \rightarrow 0$ to a regular zero of $F(\mathbf{x}; \mathbf{p})$.

Another Example

$$\mathcal{Z} = \begin{bmatrix} 1 + x + y + xy = 0 \\ xy = 0 \end{bmatrix}$$

has $\leq 2 \cdot 2 = 4$ regular zeros in $\mathbb{C}^2$

In fact, its zeros are

2.

Corollary: Every system of n complex polynomials $f_1, \dots, f_n$ in n variables has at most $\deg(f_1) \cdots \deg(f_n)$ regular zeros in $\mathbb{C}^n$.

Another Example

$$\mathcal{Z} = \begin{bmatrix} 1 + x + y + xy = 0 \\ xy = 0 \end{bmatrix}$$

Corollary: Every system of n complex polynomials $f_1, \dots, f_n$ in n variables has at most $\deg(f_1) \cdots \deg(f_n)$ regular zeros in $\mathbb{C}^n$.

has $\leq 2 \cdot 2 = 4$ regular zeros in $\mathbb{C}^2$

In fact, its zeros are $(0, -1)$ and $(-1, 0)$. (both are regular)

Another Example

$$\tilde{F} = \begin{bmatrix} 1 + x + y + xy = 0 \\ xy = 0 \end{bmatrix}$$

Corollary: Every system of n complex polynomials $f_1, \dots, f_n$ in n variables has at most $\deg(f_1) \cdots \deg(f_n)$ regular zeros in $\mathbb{C}^n$.

has $\leq 2 \cdot 2 = 4$ regular zeros in $\mathbb{C}^2$

In fact, its zeros are $(0, -1)$ and $(-1, 0)$. (both are regular)

$\Rightarrow$ The total degree start system (with 4 regular solutions $(\pm 1, \pm 1)$) is not optimal for solving $\tilde{F}$ with polynomial homotopy continuation as 2 of its zeros would diverge.

Another Example

$$\tilde{F} = \begin{bmatrix} 1 + x + y + xy = 0 \\ xy = 0 \end{bmatrix}$$

Corollary: Every system of n complex polynomials $f_1, \dots, f_n$ in n variables has at most $\deg(f_1) \cdots \deg(f_n)$ regular zeros in $\mathbb{C}^n$.

has $\leq 2 \cdot 2 = 4$ regular zeros in $\mathbb{C}^2$

In fact, its zeros are $(0, -1)$ and $(-1, 0)$. (both are regular)

$\Rightarrow$ The total degree start system (with 4 regular solutions $(\pm 1, \pm 1)$) is not optimal for solving $\tilde{F}$ with polynomial homotopy continuation as 2 of its zeros would diverge.

There are better upper bounds on the number of zeros of sparse polynomial systems (e.g. BKK Theorem) & better start systems (e.g. polyhedral start systems).
 default in HomotopyContinuation.jl

17
Fundamental Theorem of Algebra: Every complex polynomial in 1 variable has $\deg(f)$ many solutions (counted with multiplicities).

More generally, we know so far:

Every system of n complex polynomials $f_1, \dots, f_n$ in n variables has at most $\deg(f_1) \cdots \deg(f_n)$ regular zeros in $\mathbb{C}^n$, and a general system has exactly that many zeros.

17
Fundamental Theorem of Algebra: Every complex polynomial in 1 variable has $\deg(f)$ many solutions (counted with multiplicities).

More generally, we know so far:

Every system of n complex polynomials $f_1, \dots, f_n$ in n variables has at most $\deg(f_1) \cdots \deg(f_n)$ regular zeros in $\mathbb{C}^n$, and a general system has exactly that many zeros.

Can we make an exact statement (with multiplicities)
for every multivariate square system too?

17

Fundamental Theorem of Algebra: Every complex polynomial in 1 variable has $\deg(f)$ many solutions (counted with multiplicities).

More generally, we know so far:

Every system of n complex polynomials $f_1, \dots, f_n$ in n variables has at most $\deg(f_1) \cdots \deg(f_n)$ regular zeros in $\mathbb{C}^n$, and a general system has exactly that many zeros.

Can we make an exact statement (with multiplicities)
for every multivariate square system too?

YES

Remember from Lecture 1: Projective space is your friend

Given $f_1, \dots, f_n \in \mathbb{C}[x_1, \dots, x_n]$, *homogenize* them:

$$F_i := x_0^{\deg(f_i)} \cdot f_i\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) \in \mathbb{C}[x_0, \dots, x_n]$$



every monomial in F_i has degree equal to $\deg(f_i)$

Given $f_1, \dots, f_n \in \mathbb{C}[x_1, \dots, x_n]$, **homogenize** them:

$$F_i := x_0^{\deg(f_i)} \cdot f_i\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) \in \mathbb{C}[x_0, x_1, \dots, x_n]$$

↑
every monomial in F_i has degree equal to $\deg(f_i)$

Bézout's Theorem: The system of n homogeneous polynomials $F_1, \dots, F_n \in \mathbb{C}[x_0, \dots, x_n]$ has either ∞ many zeros or $\deg(F_1) \cdots \deg(F_n)$ many zeros counted with multiplicity.

Given $f_1, \dots, f_n \in \mathbb{C}[x_1, \dots, x_n]$, **homogenize** them:

$$F_i := x_0^{\deg(f_i)} \cdot f_i\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) \in \mathbb{C}[x_0, x_1, \dots, x_n]$$

↑
every monomial in F_i has degree equal to $\deg(f_i)$

Bézout's Theorem: The system of n homogeneous polynomials $F_1, \dots, F_n \in \mathbb{C}[x_0, \dots, x_n]$ has either ∞ many zeros or $\deg(F_1) \cdots \deg(F_n)$ many zeros counted with multiplicity.

Example:
$$\begin{cases} 1 + x + y + xy = 0 \\ xy = 0 \end{cases}$$

zeros: $(0, -1)$ & $(-1, 0)$

Given $f_1, \dots, f_n \in \mathbb{C}[x_1, \dots, x_n]$, **homogenize** them:

$$F_i := x_0^{\deg(f_i)} \cdot f_i\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) \in \mathbb{C}[x_0, x_1, \dots, x_n]$$

↑
every monomial in F_i has degree equal to $\deg(f_i)$

Bézout's Theorem: The system of n homogeneous polynomials $F_1, \dots, F_n \in \mathbb{C}[x_0, \dots, x_n]$ has either ∞ many zeros or $\deg(F_1) \cdots \deg(F_n)$ many zeros counted with multiplicity.

Example:
$$\begin{cases} 1 + x + y + xy = 0 \\ xy = 0 \end{cases} \xrightarrow{\text{homogenize}} \begin{cases} z^2 + xz + yz + xy = 0 \\ xy = 0 \end{cases}$$

zeros: $(0, -1)$ & $(-1, 0)$

Given $f_1, \dots, f_n \in \mathbb{C}[x_1, \dots, x_n]$, **homogenize** them:

$$F_i := x_0^{\deg(f_i)} \cdot f_i\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) \in \mathbb{C}[x_0, x_1, \dots, x_n]$$

↑
every monomial in F_i has degree equal to $\deg(f_i)$

Bézout's Theorem: The system of n homogeneous polynomials $F_1, \dots, F_n \in \mathbb{C}[x_0, \dots, x_n]$ has either ∞ many zeros or $\deg(F_1) \cdots \deg(F_n)$ many zeros counted with multiplicity.

Example:
$$\begin{cases} 1 + x + y + xy = 0 \\ xy = 0 \end{cases} \xrightarrow{\text{homogenize}} \begin{cases} z^2 + xz + yz + xy = 0 \\ xy = 0 \end{cases}$$

zeros: $(0, -1)$ & $(-1, 0)$

What are the zeros?

Given $f_1, \dots, f_n \in \mathbb{C}[x_1, \dots, x_n]$, **homogenize** them:

$$F_i := x_0^{\deg(f_i)} \cdot f_i\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) \in \mathbb{C}[x_0, x_1, \dots, x_n]$$

↑
every monomial in F_i has degree equal to $\deg(f_i)$

Bézout's Theorem: The system of n homogeneous polynomials $F_1, \dots, F_n \in \mathbb{C}[x_0, \dots, x_n]$ has either ∞ many zeros or $\deg(F_1) \cdots \deg(F_n)$ many zeros counted with multiplicity.

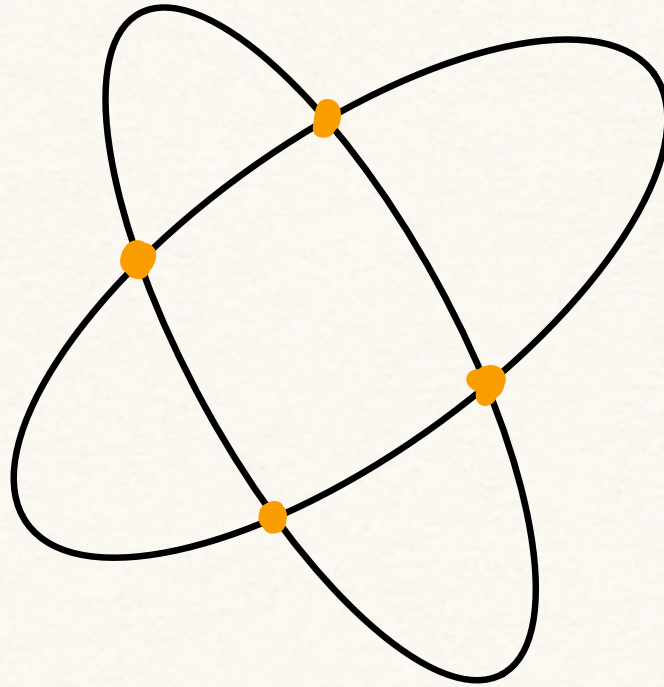
Example:
$$\begin{cases} 1 + x + y + xy = 0 \\ xy = 0 \end{cases} \xrightarrow{\text{homogenize}} \begin{cases} z^2 + xz + yz + xy = 0 \\ xy = 0 \end{cases}$$

zeros: $(0, -1)$ & $(-1, 0)$

$$\begin{matrix} x & y & z \\ (0 : -1 : 1), & (-1 : 0 : 1), \end{matrix}$$

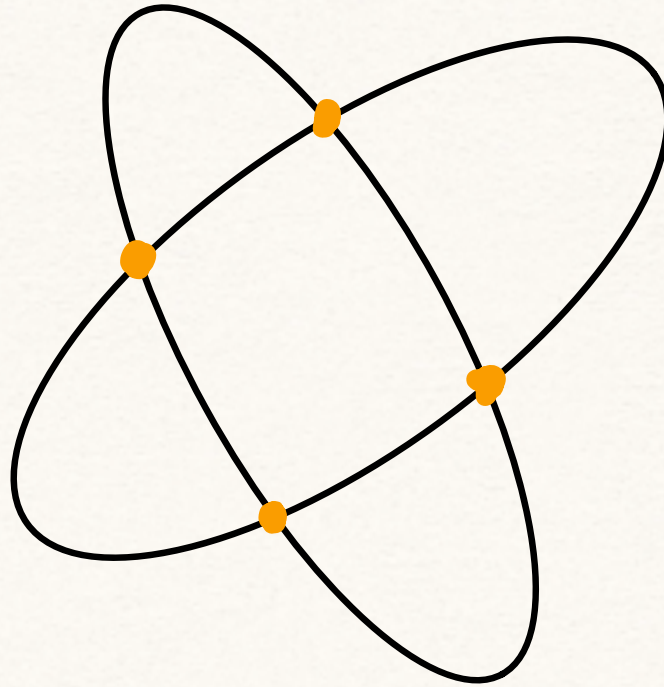
$$\begin{matrix} \text{"at } \infty" \\ (z = 0) \end{matrix} \rightarrow (0 : 1 : 0), \quad (1 : 0 : 0)$$

Example: Intersecting 2 ellipses typically has 4 solutions in $\mathbb{C}$



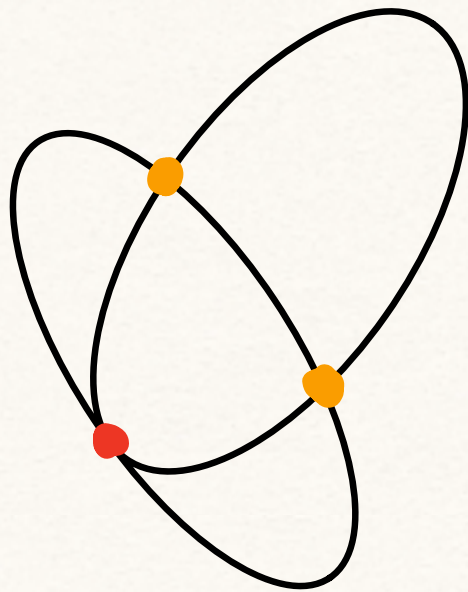
How can there be less than 4 solutions (in $\mathbb{C}$) ?

Example: Intersecting 2 ellipses typically has 4 solutions in $\mathbb{C}$

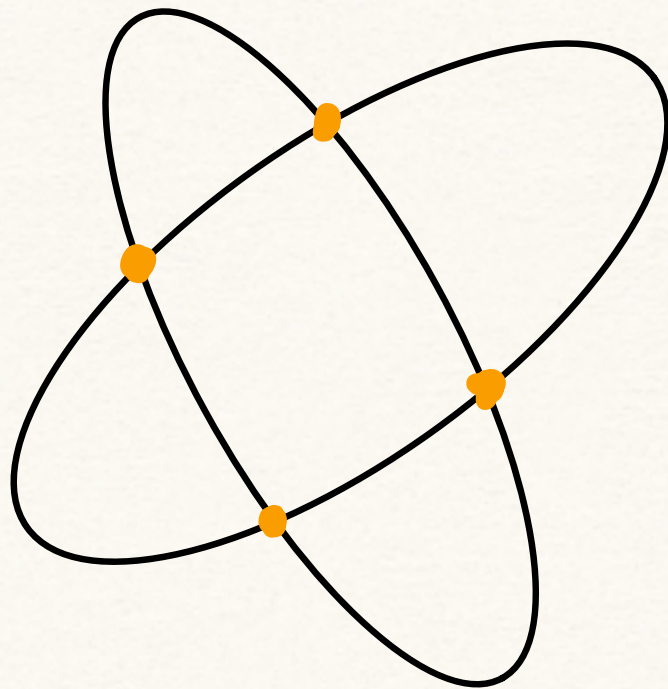


How can there be less than 4 solutions (in $\mathbb{C}$) ?

multiplicities

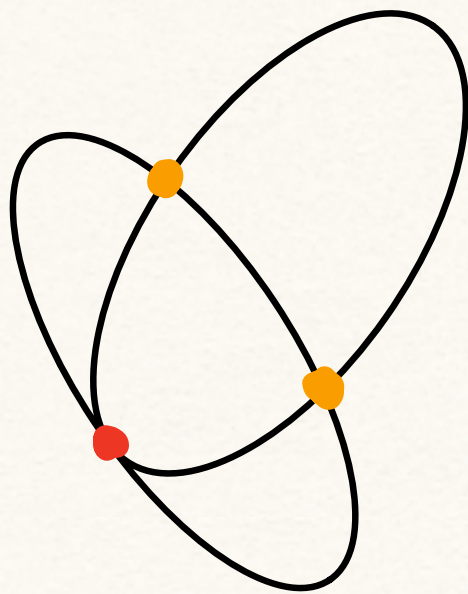


Example: Intersecting 2 ellipses typically has 4 solutions in $\mathbb{C}$

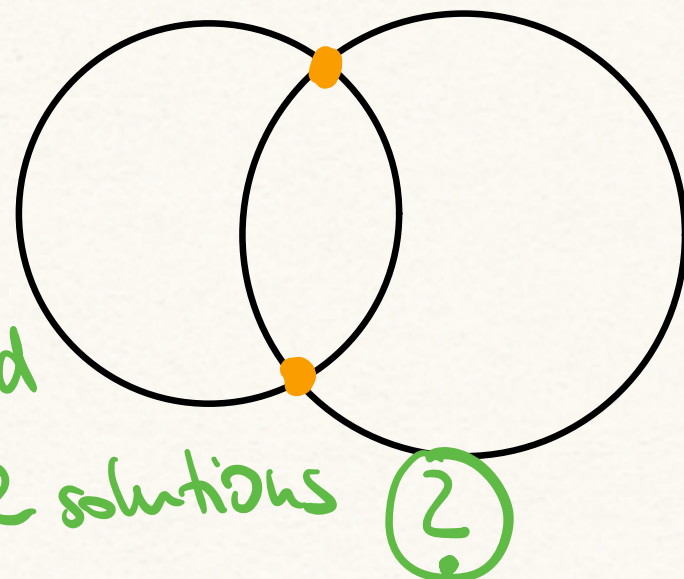


How can there be less than 4 solutions (in $\mathbb{C}$)?

multiplicities

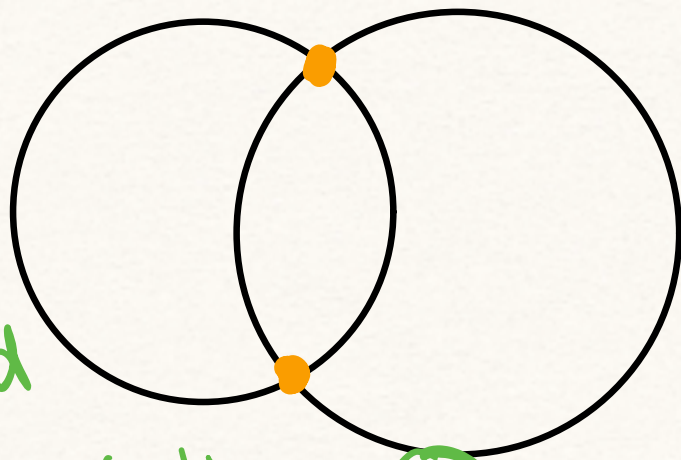


special
ellipses



What happened
to the other 2 solutions (2)

What happened
to the other 2 solutions (2)



They are at ∞ ! 😊

(remember: projective space is compact ♡)

Exercise: Every circle passes through the same 2 points at ∞ .

Given $f_1, \dots, f_n \in \mathbb{C}[x_1, \dots, x_n]$, **homogenize** them:

$$F_i := x_0^{\deg(f_i)} \cdot f_i\left(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}\right) \in \mathbb{C}[x_0, x_1, \dots, x_n]$$

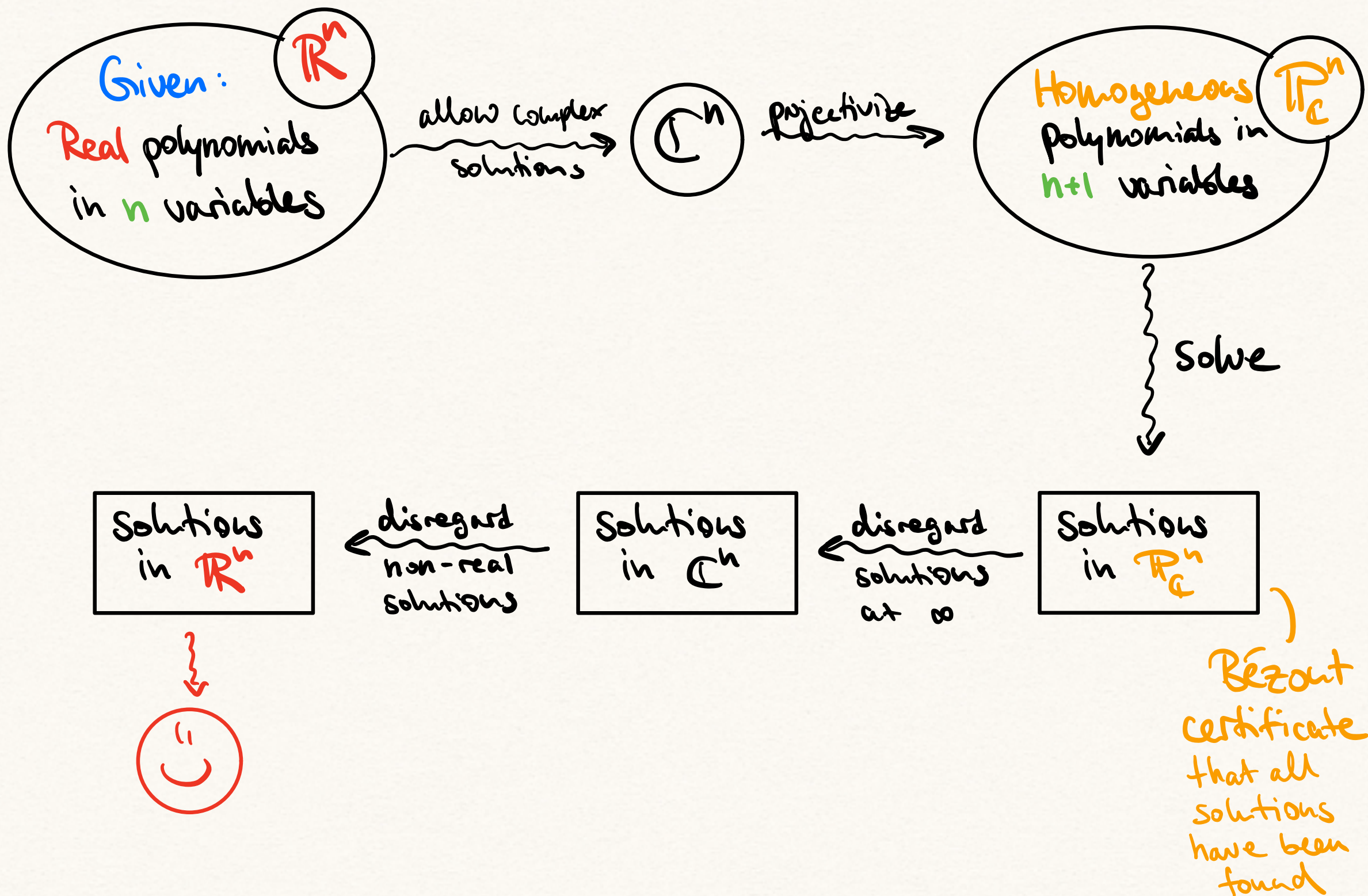
↑
every monomial in F_i has degree equal to $\deg(f_i)$

Bézout's Theorem: The system of n homogeneous polynomials $F_1, \dots, F_n \in \mathbb{C}[x_0, \dots, x_n]$ has either ∞ many zeros or $\deg(F_1) \cdots \deg(F_n)$ many zeros counted with multiplicity.

When doing **polynomial homotopy continuation** with a start system with this many regular zeros: In **projective space**, all solution paths converge & k paths colliding yields a zero of multiplicity k .

↑
compact
😊

How to actually find all solutions to a polynomial system:



Algebraic Inverse Problems

Let $\varphi: X \rightarrow Y$ be an algebraic map between irreducible varieties^(over $\mathbb{C}$)
 s.t. $Y = \overline{\text{im}(\varphi)}$ & $\dim Y = \dim X$.

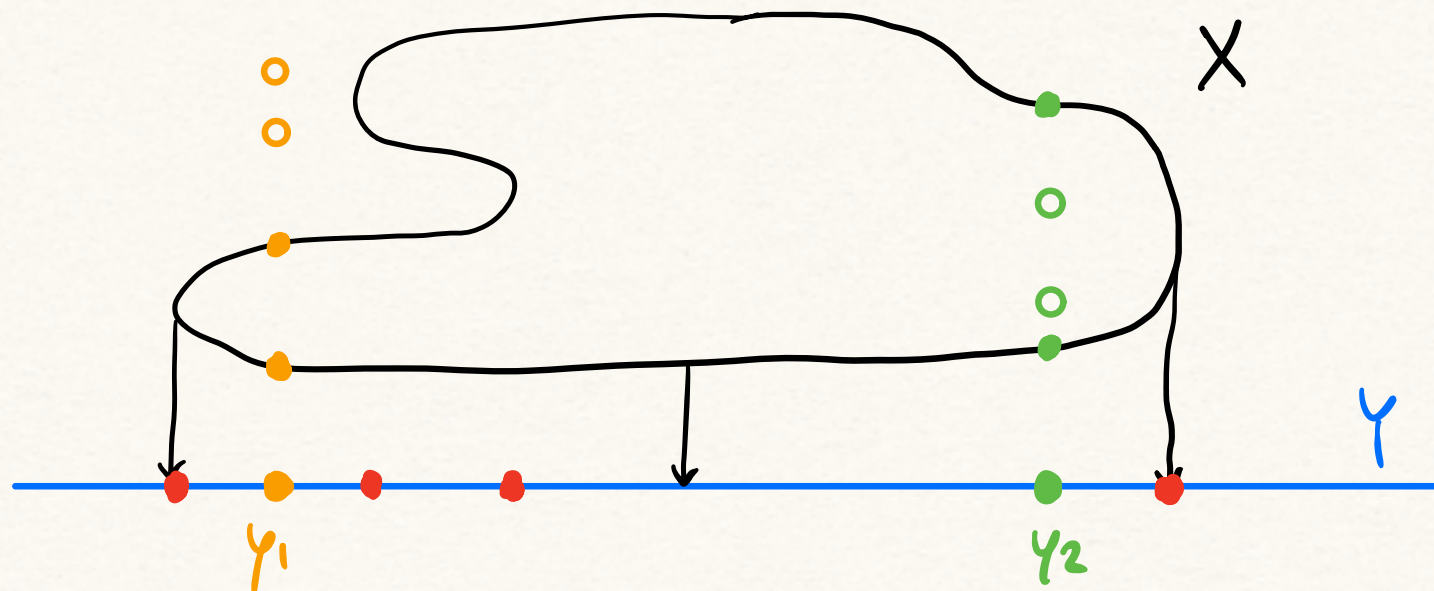
fiber-dim. thm

$\Rightarrow$ for almost all $y \in Y$, $|\varphi^{-1}(y)| < \infty$

parameter-
continuation thm.

$\Rightarrow$ there is a subvariety $\Delta \subsetneq Y$ s.t. $|\varphi^{-1}(y)| = d$
 for all $y \in Y \setminus \Delta$

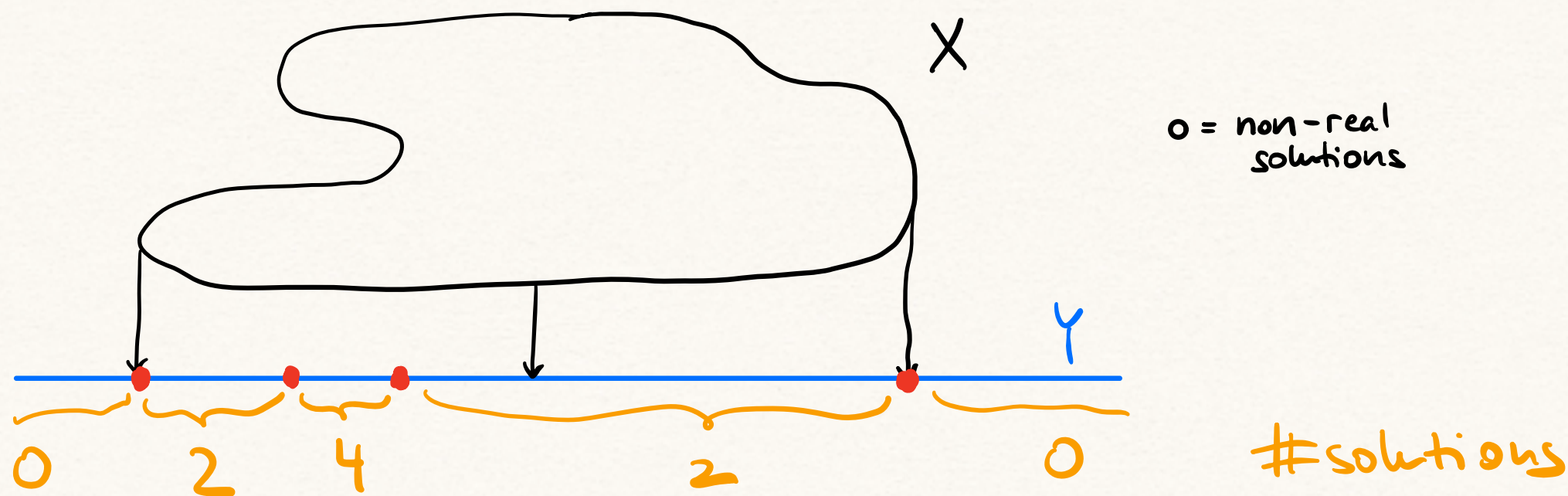
$\uparrow$
degree of φ



$\circ$ = non-real
solutions

$$\deg(\varphi) = 4$$

over $\mathbb{R}$: different Euclidean open regions have different number of solutions



over $\mathbb{R}$: different Euclidean open regions have different number of solutions

$$\begin{aligned} \varphi: \mathbb{R}^2 &\longrightarrow \mathbb{R}^2 \\ (a, b) &\longmapsto (-a-b, ab) \end{aligned}$$

inverse problem:

given $x^2 + px + q$, find the roots

$$(x-a) \cdot (x-b) = x^2 - (a+b)x + ab$$

$$\deg(\varphi) = \textcircled{?}$$

over $\mathbb{R}$: different Euclidean open regions have different number of solutions

$$\varphi: \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

$$(a, b) \mapsto (-a-b, ab)$$

$$(x-a) \cdot (x-b) = x^2 - (a+b)x + ab$$

$$\deg(\varphi) = 2$$

Fundamental Theorem of Algebra:

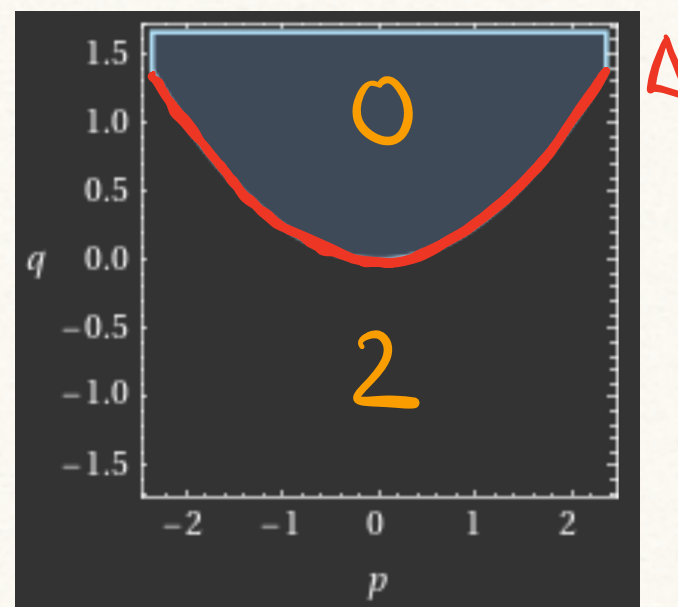
Every univariate polynomial of degree d has d roots in $\mathbb{C}$ (counted with multiplicity).

inverse problem:

given $x^2 + px + q$, find the roots

has 2 real roots if $p^2 > 4q$

has 0 real roots if $p^2 < 4q$



over $\mathbb{R}$: different Euclidean open regions have different number of solutions

matrix recovery:

$$\varphi: \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbb{R}^{2 \times 2} \mid ad = bc \right\} \longrightarrow \mathbb{R}^3,$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \longmapsto (b, c, a-d)$$

Exercise: a) $\text{im}(\varphi) = \{(b, c, s) \mid \underbrace{\frac{s^2}{4} + bc}_{\triangle} \geq 0\}$

b) $\deg(\varphi) = 2$