Symbolic Homotopy Techniques for Structured Multivariate Polynomial Systems

Thi Xuan Vu

Université de Lille, France

Outline

Outline

1. **Polynomial System Solving**

2. **Symbolic Homotopy Techniques to Solve Polynomial Systems**

3. **Solving Rank-constrained Polynomial Systems**

4. **Invariant Algebraic Systems**

System of Polynomials

polynomials: x^2, $3xyz^2$, $5x^3y - 2yz^2 + x - 3xz + 2, \ldots$ in n variables

Solving system of polynomials: $f_1 = \cdots = f_m = 0$

System of Polynomials

polynomials: x^2, $3xyz^2$, $5x^3y - 2yz^2 + x - 3xz + 2, \ldots$ in n variables

$$x^2 + y - 3 = y^2 + 8x - 12 = 0$$

Solutions: (1,2); (-3, -6)

System of Polynomials

polynomials: x^2, $3xyz^2$, $5x^3y - 2yz^2 + x - 3xz + 2, \ldots$ in n variables

Solving system of polynomials: $f_1 = \cdots = f_m = 0$

NP-hard problem
(even over $\mathbb{F}_2$)

System of Polynomials

polynomials: x^2, $3xyz^2$, $5x^3y - 2yz^2 + x - 3xz + 2, \ldots$ in n variables

Solving system of polynomials: $f_1 = \cdots = f_m = 0$

NP-hard problem
(even over $\mathbb{F}_2$)

? "solving" exactly: compute algebraic data-structures to extract information

System of Polynomials

polynomials: x^2, $3xyz^2$, $5x^3y - 2yz^2 + x - 3xz + 2, \ldots$ in n variables

Solving system of polynomials: $f_1 = \cdots = f_m = 0$

NP-hard problem
(even over $\mathbb{F}_2$)

? "solving" exactly: compute algebraic data-structures to extract information

⚠ complexity of solving a generic (or random) polynomial system is at least exponential in n

System of Polynomials

polynomials: x^2, $3xyz^2$, $5x^3y - 2yz^2 + x - 3xz + 2, \ldots$ in n variables

Solving system of polynomials: $f_1 = \cdots = f_m = 0$

NP-hard problem
(even over $\mathbb{F}_2$)

? "solving" exactly: compute algebraic data-structures to extract information

⚠ complexity of solving a generic (or random) polynomial system is at least exponential in n

exponential in n
$\Rightarrow$ sub-exponential in n?

System of Polynomials

polynomials: x^2, $3xyz^2$, $5x^3y - 2yz^2 + x - 3xz + 2, \dots$ in n variables

Solving system of polynomials: $f_1 = \cdots = f_m = 0$

NP-hard problem
(even over $\mathbb{F}_2$)

? "solving" exactly: compute algebraic data-structures to extract information

⚠ complexity of solving a generic (or random) polynomial system is at least exponential in n

exponential in n
$\Rightarrow$ sub-exponential in n?

sparsity

overdetermined

polynomials with structures

symmetry

...

rank-constrained

multi-linear

System of Polynomials

polynomials: x^2, $3xyz^2$, $5x^3y - 2yz^2 + x - 3xz + 2, \ldots$ in n variables

Solving system of polynomials: $f_1 = \cdots = f_m = 0$

NP-hard problem
(even over $\mathbb{F}_2$)

? "solving" exactly: compute algebraic data-structures to extract information

⚠ complexity of solving a generic (or random) polynomial system is at least exponential in n

alternative intrinsic measure of complexity:
polynomial in the number of solutions

System of Polynomials

polynomials: x^2, $3xyz^2$, $5x^3y - 2yz^2 + x - 3xz + 2, \dots$ in n variables

Solving system of polynomials: $f_1 = \dots = f_m = 0$

NP-hard problem
(even over $\mathbb{F}_2$)

? "solving" exactly: compute algebraic data-structures to extract information

⚠ complexity of solving a generic (or random) polynomial system is at least exponential in n

alternative intrinsic measure of complexity:
polynomial in the number of solutions

sparsity

overdetermined

polynomials with structures

symmetry

...

rank-constrained

multi-linear

Gröbner-basis Methods to Solve Polynomial Systems

$F(x_1, \dots, x_n)$ — homogeneous, generic, square, total degrees $(d_1, \dots, d_n)$ (zero-dimensional)

$\downarrow$

Buchberger [Buchberger,1976]
F_4 [Faugère, 1999]
F_5 [Faugère, 2002]
…

$\downarrow$

grevlex basis

$\downarrow$

FGLM [Faugère-Gianni-Lazard-Mora, 1993]

$\downarrow$

lex basis

Gröbner-basis Methods to Solve Polynomial Systems

$F(x_1, \dots, x_n)$

homogeneous, generic, total degrees $(d_1, \dots, d_n)$
(zero-dimensional)

F_5

Highest degree : $d_{\max} \leq \sum_{i=1}^{n} (d_i - 1) + 1$

Size of a matrix at degree d : $\binom{n+d-1}{d}$

grevlex basis

FGLM

Number of solutions : $\prod_{i=1}^{n} d_i$ (Bézout bound)

lex basis

$$O\left(\left(\binom{n+d_{\max}-1}{d_{\max}}\right)^3 + n\left(\prod_{i=1}^{n} d_i\right)^3\right)$$

Straight-Line Programs – Model for the Input

General speaking, it is a sequence of elementary operations $\{+, -, \times\}$.

Straight-Line Programs – Model for the Input

General speaking, it is a sequence of elementary operations $\{+, -, \times\}$.

Definition (SLP)

A SLP of length L computing $f_1, \dots, f_m \in \mathbb{K}[x_1, \dots, x_n]$ is a sequence

$$\gamma = (\gamma_{-n+1}, \cdots, \gamma_0, \gamma_1, \cdots, \gamma_L)$$

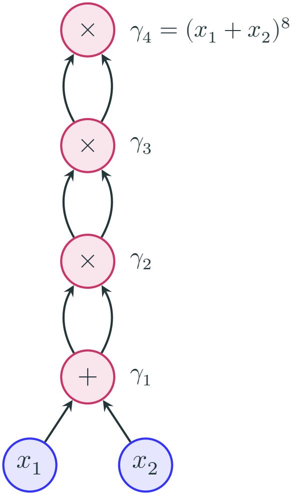
where $f_1, \dots, f_m \in \gamma$, with initial inputs $\gamma_{-n+1} := x_1, \dots, \gamma_0 := x_n$.
For each instruction $k > 0$, γ_k takes one of the forms:

$$\gamma_k = a \star \gamma_i \quad \text{or} \quad \gamma_k = \gamma_i \star \gamma_j$$

where $\star \in \{+, -, \times\}$, $a \in \mathbb{K}$, and $i, j < k$.

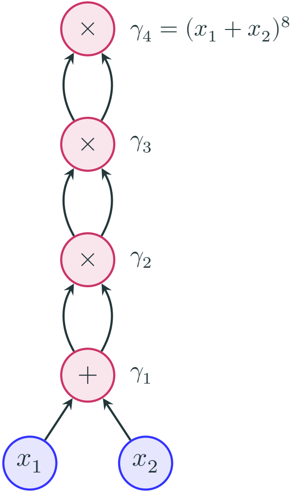
Example: $(x_1 + x_2)^8$

- $\gamma_{-1} := x_1, \gamma_0 := x_2$
- $\gamma_1 = \gamma_{-1} + \gamma_0$
- $\gamma_2 = \gamma_1 \times \gamma_1$
- $\gamma_3 = \gamma_2 \times \gamma_2$
- $\gamma_4 = \gamma_3 \times \gamma_3$



Example: $(x_1 + x_2)^8$

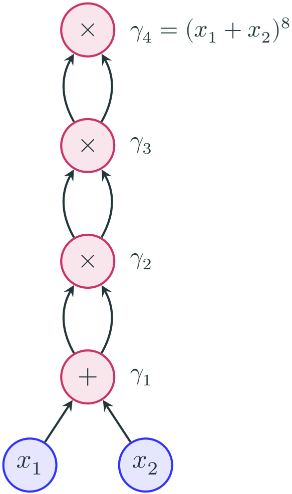
- $\gamma_{-1} := x_1, \gamma_0 := x_2$
- $\gamma_1 = \gamma_{-1} + \gamma_0$
- $\gamma_2 = \gamma_1 \times \gamma_1$
- $\gamma_3 = \gamma_2 \times \gamma_2$
- $\gamma_4 = \gamma_3 \times \gamma_3$



- length of SLP is 4

Example: $(x_1 + x_2)^8$

- $\gamma_{-1} := x_1, \gamma_0 := x_2$
- $\gamma_1 = \gamma_{-1} + \gamma_0$
- $\gamma_2 = \gamma_1 \times \gamma_1$
- $\gamma_3 = \gamma_2 \times \gamma_2$
- $\gamma_4 = \gamma_3 \times \gamma_3$



- length of SLP is 4
- dense representation uses 9 terms

$$(x_1 + x_2)^8 = x_1^8 + 8x_1^7x_2 + 28x_1^6x_2^2 + 56x_1^5x_2^3 + 70x_1^4x_2^4 + 56x_1^3x_2^5 + 28x_1^2x_2^6 + 8x_1x_2^7 + x_2^8$$

Data Structures – Representing the Output

Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$, and $Z \subset \overline{\mathbb{K}}^n$ be a finite set.

Definition

A zero-dimensional parametrization of Z consists of $(n+1)$ univariate polynomials $(q, v_1, \dots, v_n))$ in $\mathbb{K}[T]$ and linear form $\lambda = \lambda_1 x_1 + \dots + \lambda_n x_n$ s.t

- q is square-free, $\deg(q) = |Z|$, $\deg(v_i) < \deg(q)$
- $q(T) = 0, \quad x_1 = v_1(T), \dots, x_n = v_n(T)$
- $\lambda(v_1, \dots, v_n) \equiv T \pmod q$

Data Structures – Representing the Output

Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$, and $Z \subset \overline{\mathbb{K}}^n$ be a finite set.

Definition

A zero-dimensional parametrization of Z consists of $(n+1)$ univariate polynomials $(q, v_1, \dots, v_n))$ in $\mathbb{K}[T]$ and linear form $\lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n$ s.t

- q is square-free, $\deg(q) = |Z|$, $\deg(v_i) < \deg(q)$
- $q(T) = 0, \quad x_1 = v_1(T), \dots, x_n = v_n(T)$
- $\lambda(v_1, \dots, v_n) \equiv T \pmod{q}$

Example: Consider $Z = \{(1,0), (0,1)\}$.

Data Structures – Representing the Output

Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$, and $Z \subset \overline{\mathbb{K}}^n$ be a finite set.

Definition

A zero-dimensional parametrization of Z consists of $(n+1)$ univariate polynomials $(q, v_1, \dots, v_n))$ in $\mathbb{K}[T]$ and linear form $\lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n$ s.t

- q is square-free, $\deg(q) = |Z|$, $\deg(v_i) < \deg(q)$
- $q(T) = 0, \quad x_1 = v_1(T), \dots, x_n = v_n(T)$
- $\lambda(v_1, \dots, v_n) \equiv T \pmod{q}$

Example: Consider $Z = \{(1,0),(0,1)\}$. A zero-dimensional para. of Z consists of

$$q(T) = T^2 - 4T + 3, \quad v_1(T) = \frac{3}{2} - \frac{T}{2}, \quad v_2(T) = -\frac{1}{2} + \frac{T}{2}, \quad \lambda = x_1 + 3x_2$$

Data Structures – Representing the Output

Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$, and $Z \subset \overline{\mathbb{K}}^n$ be a finite set.

Definition

A zero-dimensional parametrization of Z consists of $(n+1)$ univariate polynomials $(q, v_1, \ldots, v_n))$ in $\mathbb{K}[T]$ and linear form $\lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n$ s.t

- q is square-free, $\deg(q) = |Z|$, $\deg(v_i) < \deg(q)$
- $q(T) = 0, \quad x_1 = v_1(T), \ldots, x_n = v_n(T)$
- $\lambda(v_1, \ldots, v_n) \equiv T \pmod{q}$

Example: Consider $Z = \{(1,0),(0,1)\}$. A zero-dimensional para. of Z consists of

$$q(T) = T^2 - 4T + 3, \quad v_1(T) = \frac{3}{2} - \frac{T}{2}, \quad v_2(T) = -\frac{1}{2} + \frac{T}{2}, \quad \lambda = x_1 + 3x_2$$

$q(T)$ has two solutions $T \in \{1, 3\}$

Data Structures – Representing the Output

Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$, and $Z \subset \overline{\mathbb{K}}^n$ be a finite set.

Definition

A zero-dimensional parametrization of Z consists of $(n+1)$ univariate polynomials $(q, v_1, \dots, v_n))$ in $\mathbb{K}[T]$ and linear form $\lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n$ s.t

- q is square-free, $\deg(q) = |Z|$, $\deg(v_i) < \deg(q)$
- $q(T) = 0, \quad x_1 = v_1(T), \dots, x_n = v_n(T)$
- $\lambda(v_1, \dots, v_n) \equiv T \pmod{q}$

Example: Consider $Z = \{(1,0),(0,1)\}$. A zero-dimensional para. of Z consists of

$$q(T) = T^2 - 4T + 3, \quad v_1(T) = \frac{3}{2} - \frac{T}{2}, \quad v_2(T) = -\frac{1}{2} + \frac{T}{2}, \quad \lambda = x_1 + 3x_2$$

$q(T)$ has two solutions $T \in \{1, 3\}$

- $T = 1$, $v_1(1) = 1$ and $v_2(0) = 0 \rightsquigarrow$ the point $(1,0)$
- $T = 3$, $v_1(3) = 0$ and $v_2(3) = 1 \rightsquigarrow$ the point $1,0)$

Data Structures – Representing the Output

Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$, and $Z \subset \overline{\mathbb{K}}^n$ be a finite set.

Definition

A zero-dimensional parametrization of Z consists of $(n+1)$ univariate polynomials $(q, v_1, \dots, v_n))$ in $\mathbb{K}[T]$ and linear form $\lambda = \lambda_1 x_1 + \dots + \lambda_n x_n$ s.t

- q is square-free, $\deg(q) = |Z|$, $\deg(v_i) < \deg(q)$
- $q(T) = 0, \quad x_1 = v_1(T), \dots, x_n = v_n(T)$
- $\lambda(v_1, \dots, v_n) \equiv T \pmod q$

Used to represent the isolated points
of the zero set of a polynomial system

Data Structures – Representing the Output

Let $\mathbb{K}$ be a field, $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$, and $Z \subset \overline{\mathbb{K}}^n$ be a finite set.

Definition

A zero-dimensional parametrization of Z consists of $(n+1)$ univariate polynomials $(q, v_1, \dots, v_n))$ in $\mathbb{K}[T]$ and linear form $\lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n$ s.t

- q is square-free, $\deg(q) = |Z|$, $\deg(v_i) < \deg(q)$
- $q(T) = 0, \quad x_1 = v_1(T), \dots, x_n = v_n(T)$
- $\lambda(v_1, \dots, v_n) \equiv T \pmod{q}$

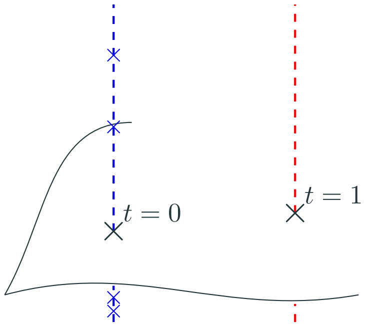
Used to represent the isolated points of the zero set of a polynomial system

- not unique
- introduced in [Kronecker, 1882] and [Macaulay, 1916]
- used in many algorithms: [Rouillier, 1999], [Gianni-Mora, 1989], [Giusti et al., 1998, 1995], [Giusti-Lecerf-Salvy, 2001], ...

Outline

Symbolic Homotopies

Solve target system $\boldsymbol{C} = (c_i(\boldsymbol{X}))_{1\leq i\leq m}$, knowing the solutions of a **start system** $\boldsymbol{A} = (a_i)_{1\leq i\leq m}$.

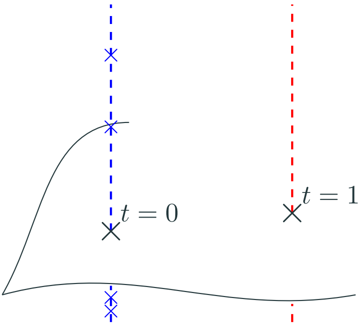


$q(T), \dots, x_1 = v_1(T), \dots, x_n = v_n(T)$ in $\mathbb{K}[T]$

Symbolic Homotopies

Solve **target system** $\boldsymbol{C} = (c_i(\boldsymbol{X}))_{1 \leq i \leq m}$, knowing the solutions of a **start system** $\boldsymbol{A} = (a_i)_{1 \leq i \leq m}$.

(i.) find deformed system $\boldsymbol{B}(t, \boldsymbol{X})$ s.t $\boldsymbol{B}(1, \boldsymbol{X}) = \boldsymbol{C}$ and $\boldsymbol{B}(0, \boldsymbol{X}) = \boldsymbol{A}$



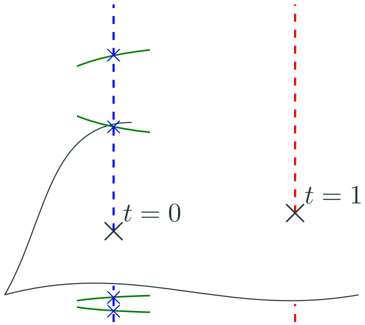
$q(T), \ldots, x_1 = v_1(T), \ldots, x_n = v_n(T)$ in $\mathbb{K}[T]$

Symbolic Homotopies

Solve **target system** $\boldsymbol{C} = (c_i(\boldsymbol{X}))_{1 \le i \le m}$, knowing the solutions of a **start system** $\boldsymbol{A} = (a_i)_{1 \le i \le m}$.

(i.) find deformed system $\boldsymbol{B}(t, \boldsymbol{X})$ s.t $\boldsymbol{B}(1, \boldsymbol{X}) = \boldsymbol{C}$ and $\boldsymbol{B}(0, \boldsymbol{X}) = \boldsymbol{A}$

(ii.) compute a description of the $\boldsymbol{B}(t, \boldsymbol{X}) = 0$ for "symbolic" t



symbolic Newton iteration

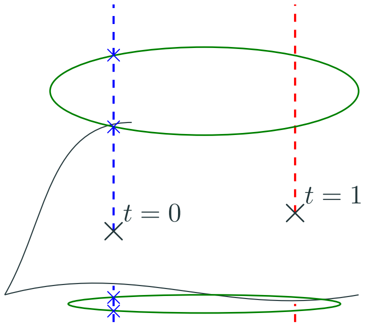
$Q(t, T), \dots, x_1 = V_1(t, T), \dots, x_n = V_n(t, T)$ in $\mathbb{K}[[t]][T]$

Symbolic Homotopies

Solve target system $\boldsymbol{C} = (c_i(\boldsymbol{X}))_{1 \le i \le m}$, knowing the solutions of a **start system** $\boldsymbol{A} = (a_i)_{1 \le i \le m}$.

(i.) find deformed system $\boldsymbol{B}(t, \boldsymbol{X})$ s.t $\boldsymbol{B}(1, \boldsymbol{X}) = \boldsymbol{C}$ and $\boldsymbol{B}(0, \boldsymbol{X}) = \boldsymbol{A}$

(ii.) compute a description of the $\boldsymbol{B}(t, \boldsymbol{X}) = 0$ for "symbolic" t



rational reconstruction

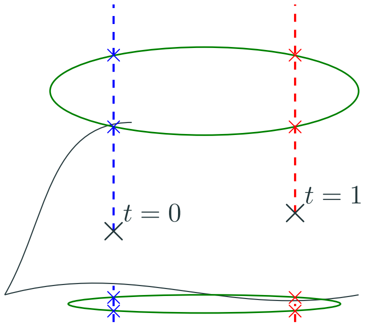
$\Gamma(t, T), \dots, x_1 = \gamma_1(t, T), \dots, x_n = \gamma_n(t, T)$ in $\mathbb{K}(t)[T]$

Symbolic Homotopies

Solve **target system** $\boldsymbol{C} = (c_i(\boldsymbol{X}))_{1 \le i \le m}$, knowing the solutions of a **start system** $\boldsymbol{A} = (a_i)_{1 \le i \le m}$.

(i.) find deformed system $\boldsymbol{B}(t, \boldsymbol{X})$ s.t $\boldsymbol{B}(1, \boldsymbol{X}) = \boldsymbol{C}$ and $\boldsymbol{B}(0, \boldsymbol{X}) = \boldsymbol{A}$

(ii.) compute a description of the $\boldsymbol{B}(t, \boldsymbol{X}) = 0$ for "symbolic" t and let $t = 1$



$w(T), \ldots, x_1 = w_1(T), \ldots, x_n = w_n(T)$ in $\mathbb{K}[T]$

Previous Work on Symbolic Homotopies

[Giusti-Lecerf-Salvy, 2001]

- ◇ symbolic Newton iteration (aka Newton-Hensel Lifting)

[Jeronimo et al., 2009]

- ◇ symbolic polyhedral homotopies

[Safey El Din-Schost, 2018]

- ◇ bit complexity of multi-homogeneous homotopies

Homotopies for Non-square Systems

Recall: target system $\boldsymbol{C} = (c_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; start system $\boldsymbol{A} = (a_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; deformed system $\boldsymbol{B} = (b_i)_{i \leq m} \in \mathbb{K}[t, \boldsymbol{X}]$.

Homotopies for Non-square Systems

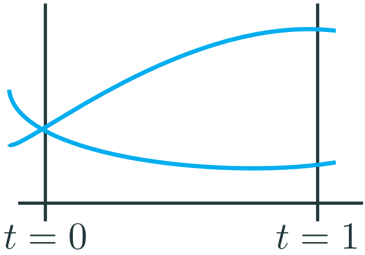
Recall: target system $\boldsymbol{C} = (c_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; start system $\boldsymbol{A} = (a_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; deformed system $\boldsymbol{B} = (b_i)_{i \leq m} \in \mathbb{K}[t, \boldsymbol{X}]$. **Here** $m > n$.

Homotopies for Non-square Systems

Recall: target system $\boldsymbol{C} = (c_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; start system $\boldsymbol{A} = (a_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; deformed system $\boldsymbol{B} = (b_i)_{i \leq m} \in \mathbb{K}[t, \boldsymbol{X}]$. **Here** $m > n$.

Assumptions:

- the ideal $\langle \boldsymbol{A} \rangle \subset \mathbb{K}[\boldsymbol{X}]$ is radical
-
-
-



Bad Situation 1

Homotopies for Non-square Systems

Recall: target system $\boldsymbol{C} = (c_i)_{i \le m} \in \mathbb{K}[\boldsymbol{X}]$; start system $\boldsymbol{A} = (a_i)_{i \le m} \in \mathbb{K}[\boldsymbol{X}]$; deformed system $\boldsymbol{B} = (b_i)_{i \le m} \in \mathbb{K}[t, \boldsymbol{X}]$. **Here** $m > n$.

Assumptions:

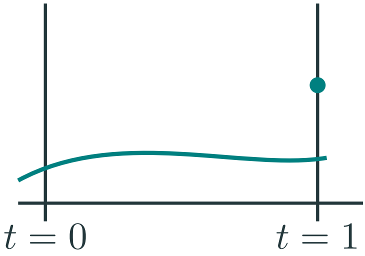
- the ideal $\langle \boldsymbol{A} \rangle \subset \mathbb{K}[\boldsymbol{X}]$ is radical
-
-
-

Homotopies for Non-square Systems

Recall: target system $\boldsymbol{C} = (c_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; start system $\boldsymbol{A} = (a_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; deformed system $\boldsymbol{B} = (b_i)_{i \leq m} \in \mathbb{K}[t, \boldsymbol{X}]$. **Here** $m > n$.

Assumptions:

- the ideal $\langle \boldsymbol{A} \rangle \subset \mathbb{K}[\boldsymbol{X}]$ is radical
- all components of $V(\boldsymbol{B}) \subset \overline{\mathbb{K}}^{n+1}$ have dimension at least 1
-
-



Bad Situation 2

Homotopies for Non-square Systems

Recall: target system $\boldsymbol{C} = (c_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; start system $\boldsymbol{A} = (a_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; deformed system $\boldsymbol{B} = (b_i)_{i \leq m} \in \mathbb{K}[t, \boldsymbol{X}]$. **Here** $m > n$.

Assumptions:

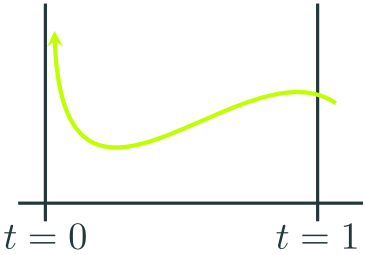
- the ideal $\langle \boldsymbol{A} \rangle \subset \mathbb{K}[\boldsymbol{X}]$ is radical
- all components of $V(\boldsymbol{B}) \subset \overline{\mathbb{K}}^{n+1}$ have dimension at least 1
-
-

Homotopies for Non-square Systems

Recall: target system $\boldsymbol{C} = (c_i)_{i \le m} \in \mathbb{K}[\boldsymbol{X}]$; start system $\boldsymbol{A} = (a_i)_{i \le m} \in \mathbb{K}[\boldsymbol{X}]$; deformed system $\boldsymbol{B} = (b_i)_{i \le m} \in \mathbb{K}[t, \boldsymbol{X}]$. **Here** $m > n$.

Assumptions:

- the ideal $\langle \boldsymbol{A} \rangle \subset \mathbb{K}[\boldsymbol{X}]$ is radical
- all components of $V(\boldsymbol{B}) \subset \overline{\mathbb{K}}^{n+1}$ have dimension at least 1
- $\deg_{\boldsymbol{X}}(\boldsymbol{A}) = \deg_{\boldsymbol{X}}(\boldsymbol{B})$, with no solution at infinity at $t = 0$
-



Bad Situation 3

Homotopies for Non-square Systems

Recall: target system $\boldsymbol{C} = (c_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; start system $\boldsymbol{A} = (a_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; deformed system $\boldsymbol{B} = (b_i)_{i \leq m} \in \mathbb{K}[t, \boldsymbol{X}]$. **Here** $m > n$.

Assumptions:

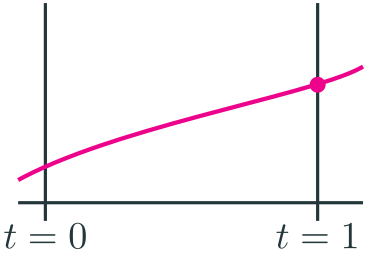
- the ideal $\langle \boldsymbol{A} \rangle \subset \mathbb{K}[\boldsymbol{X}]$ is radical
- all components of $V(\boldsymbol{B}) \subset \overline{\mathbb{K}}^{n+1}$ have dimension at least 1
- $\deg_{\boldsymbol{X}}(\boldsymbol{A}) = \deg_{\boldsymbol{X}}(\boldsymbol{B})$, with no solution at infinity $t = 0$
-

Homotopies for Non-square Systems

Recall: target system $\boldsymbol{C} = (c_i)_{i \le m} \in \mathbb{K}[\boldsymbol{X}]$; start system $\boldsymbol{A} = (a_i)_{i \le m} \in \mathbb{K}[\boldsymbol{X}]$; deformed system $\boldsymbol{B} = (b_i)_{i \le m} \in \mathbb{K}[t, \boldsymbol{X}]$. **Here** $m > n$.

Assumptions:

- the ideal $\langle \boldsymbol{A} \rangle \subset \mathbb{K}[\boldsymbol{X}]$ is radical
- all components of $V(\boldsymbol{B}) \subset \overline{\mathbb{K}}^{n+1}$ have dimension at least 1
- $\deg_{\boldsymbol{X}}(\boldsymbol{A}) = \deg_{\boldsymbol{X}}(\boldsymbol{B})$, with no solution at infinity $t = 0$
- if a localization $\mathbb{K}[t, \boldsymbol{X}]_{\mathfrak{m}}$ of $\boldsymbol{B}$ has height n, it is unmixed ($\mathfrak{m}$: maximal ideal)



Bad Situation 4

Homotopies for Non-square Systems

Recall: target system $\boldsymbol{C} = (c_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; start system $\boldsymbol{A} = (a_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; deformed system $\boldsymbol{B} = (b_i)_{i \leq m} \in \mathbb{K}[t, \boldsymbol{X}]$. **Here** $m > n$.

Assumptions:

- the ideal $\langle \boldsymbol{A} \rangle \subset \mathbb{K}[\boldsymbol{X}]$ is radical
- all components of $V(\boldsymbol{B}) \subset \overline{\mathbb{K}}^{n+1}$ have dimension at least 1
- $\deg_{\boldsymbol{X}}(\boldsymbol{A}) = \deg_{\boldsymbol{X}}(\boldsymbol{B})$, with no solution at infinity $t = 0$
- if a localization $\mathbb{K}[t, \boldsymbol{X}]_{\mathfrak{m}}$ of $\boldsymbol{B}$ has height n, it is unmixed ($\mathfrak{m}$: maximal ideal)

Theorem [Hauenstein-Safey El Din-Schost-**Vu**, 2021]

Let κ be the number of solutions of the start system $\boldsymbol{A}$. Under four above assumptions,

- the target system $\boldsymbol{C}$ has at most κ solutions, counted with multiplicities
- can be computed by a symbolic homotopy

Subroutines

Recall: target system $\boldsymbol{C} = (c_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; start system $\boldsymbol{A} = (a_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; deformed system $\boldsymbol{B} = (b_i)_{i \leq m} \in \mathbb{K}[t, \boldsymbol{X}]$.

Classical mainly ingredients:

- symbolic Newton iteration,
- rational reconstruction, ...

Subroutines

Recall: target system $\boldsymbol{C} = (c_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; start system $\boldsymbol{A} = (a_i)_{i \leq m} \in \mathbb{K}[\boldsymbol{X}]$; deformed system $\boldsymbol{B} = (b_i)_{i \leq m} \in \mathbb{K}[t, \boldsymbol{X}]$.

Classical mainly ingredients:

- symbolic Newton iteration,
- rational reconstruction, ...

An important subroutine:

Proposition (Local Dimension Testing) [Hauenstein-Safey El Din-Schost-**Vu**, 2021]

Given $\boldsymbol{x}$ s.t. $\boldsymbol{C}(\boldsymbol{x}) = 0$. Suppose that

- $\boldsymbol{C}$ is given by a SLP of length σ
- $\boldsymbol{x}$ belongs to a positive-dimensional component of $V(\boldsymbol{C})$ or is isolated with multiplicity at most κ

Then, we can decide whether $\boldsymbol{x}$ is an isolated point of $V(\boldsymbol{C})$ using $(\kappa\, \sigma\, m)^{O(1)}$ operations in $\mathbb{K}$.

Outline

An Example

Minimize x_1 on $x_1^{10} + x_2^{10} + x_3^{10} = 1$

An Example

Minimize x_1 on $x_1^{10} + x_2^{10} + x_3^{10} = 1$

The minima satisfy

$$x_1^{10} + x_2^{10} + x_3^{10} = 1$$

and

$$\operatorname{rank} \begin{bmatrix} 10x_1^9 & 10x_2^9 & 10x_3^9 \\ 1 & 0 & 0 \end{bmatrix} < 2$$

An Example

Minimize x_1 on $x_1^{10} + x_2^{10} + x_3^{10} = 1$

The minima satisfy

$$x_1^{10} + x_2^{10} + x_3^{10} = 1$$

and

$$\mathrm{rank} \begin{bmatrix} 10x_1^9 & 10x_2^9 & 10x_3^9 \\ 1 & 0 & 0 \end{bmatrix} < 2$$

This type of systems appear in:

- optimization,
- real algebraic geometry (polar varieties),
- cryptography (e.g., MinRank Problem),
- ...

Determinantal Systems

$\mathbb{K}$ a field of characteristic zero and $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$

Determinantal Systems

$\mathbb{K}$ a field of characteristic zero and $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$

Problem

Given:

- polynomials $\boldsymbol{G} = (g_1, \dots, g_s)$ in $\mathbb{K}[x_1, \dots, x_n]$
- matrix $\boldsymbol{F} = \left[f_{i,j}\right] \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}$

with

$$p \leq q \text{ and } n = q - p + s + 1$$

Compute: the isolated points of the set

$$V_p(\boldsymbol{F}, \boldsymbol{G}) = \left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : \boldsymbol{G}(\boldsymbol{x}) = 0 \quad \text{and} \quad \operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < p\right\}$$

Determinantal Systems

$\mathbb{K}$ a field of characteristic zero and $\overline{\mathbb{K}}$ an algebraic closure of $\mathbb{K}$

Problem

Given:

- $\diamond$ polynomials $\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[x_1, \ldots, x_n]$
- $\diamond$ matrix $\boldsymbol{F} = \left[f_{i,j}\right] \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$

with

$$p \leq q \text{ and } n = q - p + s + 1$$

Compute: the isolated points of the set

$$V_p(\boldsymbol{F}, \boldsymbol{G}) = \left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : \boldsymbol{G}(\boldsymbol{x}) = 0 \quad \text{and} \quad \operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < p\right\}$$

- $V_p(\boldsymbol{F}, \boldsymbol{G})$ is an algebraic set defined by $\boldsymbol{G}$ and all p-minors of $\boldsymbol{F}$

Why $p \leq q$ and $n = q - p + s + 1$?

$\boldsymbol{G} = (g_1, \dots, g_s)$ in $\mathbb{K}[x_1, \dots x_n]$ and $\boldsymbol{F} \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}$

Why $p \leq q$ and $n = q - p + s + 1$?

$\boldsymbol{G} = (g_1, \dots, g_s)$ in $\mathbb{K}[x_1, \dots x_n]$ and $\boldsymbol{F} \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}$

W.l.o.g. if $p > q$, consider the transpose $\boldsymbol{F}^T$, instead of $\boldsymbol{F}$.

Why $p \leq q$ and $n = q - p + s + 1$?

$\boldsymbol{G} = (g_1, \dots, g_s)$ in $\mathbb{K}[x_1, \dots x_n]$ and $\boldsymbol{F} \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}$

W.l.o.g. if $p > q$, consider the transpose $\boldsymbol{F}^T$, instead of $\boldsymbol{F}$.

Macaulay, Eagon-Northcott Theorem

All irreducible components of the algebraic set

$$\left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : \mathrm{rank}(\boldsymbol{F}(\boldsymbol{x})) < p\right\}$$

have codimension at most $q - p + 1$

Why $p \leq q$ and $n = q - p + s + 1$?

$\boldsymbol{G} = (g_1, \ldots, g_s)$ in $\mathbb{K}[x_1, \ldots x_n]$ and $\boldsymbol{F} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$

W.l.o.g. if $p > q$, consider the transpose $\boldsymbol{F}^T$, instead of $\boldsymbol{F}$.

Macaulay, Eagon-Northcott Theorem

All irreducible components of the algebraic set

$$\left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : \mathrm{rank}(\boldsymbol{F}(\boldsymbol{x})) < p\right\}$$

have codimension at most $q - p + 1$

Then by [Krull's Theorem], all irreducible components of

$$V_p(\boldsymbol{F}, \boldsymbol{G}) = \left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : \boldsymbol{G}(\boldsymbol{x}) = 0 \quad \text{and} \quad \mathrm{rank}(\boldsymbol{F}(\boldsymbol{x})) < p\right\}$$

have codimension at most $q - p + 1 + s$

Why $p \leq q$ and $n = q - p + s + 1$?

$\boldsymbol{G} = (g_1, \dots, g_s)$ in $\mathbb{K}[x_1, \dots x_n]$ and $\boldsymbol{F} \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}$

W.l.o.g. if $p > q$, consider the transpose $\boldsymbol{F}^T$, instead of $\boldsymbol{F}$.

Macaulay, Eagon-Northcott Theorem

All irreducible components of the algebraic set

$$\left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : \operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < p\right\}$$

have codimension at most $q - p + 1$

Then by [Krull's Theorem], all irreducible components of

$$V_p(\boldsymbol{F}, \boldsymbol{G}) = \left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : \boldsymbol{G}(\boldsymbol{x}) = 0 \quad \text{and} \quad \operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < p\right\}$$

have codimension at most $q - p + 1 + s$, i.e., dimension at least $n - (q - p + s + 1)$.

Our Result – Column Degrees

Suppose that:

- the degrees of $\boldsymbol{G} = (g_1, \dots, g_s)$ are at most $d_1, \dots, d_s$
- the column-degrees of $\boldsymbol{F}$ are at most $\alpha_1, \dots, \alpha_q$
- $n = q - p + s + 1$
- all polynomials are given by a SLP af size L
- E_k: k-th elementary symmetric function

Our Result – Column Degrees

Suppose that:

- the degrees of $\boldsymbol{G} = (g_1, \ldots, g_s)$ are at most $d_1, \ldots, d_s$
- the column-degrees of $\boldsymbol{F}$ are at most $\alpha_1, \ldots, \alpha_q$
- $n = q - p + s + 1$
- all polynomials are given by a SLP af size L
- E_k: k-th elementary symmetric function

Theorem [Hauenstein-Safey El Din-Schost-**Vu**, 2021]

- there are at most

$$c = d_1 \ldots d_s E_{n-s}(\alpha_1, \ldots, \alpha_q)$$

isolated solutions in $V_p(\boldsymbol{F}, \boldsymbol{G})$, counted with multiplicities;

Our Result – Column Degrees

Suppose that:

- the degrees of $\boldsymbol{G} = (g_1, \dots, g_s)$ are at most $d_1, \dots, d_s$
- the column-degrees of $\boldsymbol{F}$ are at most $\alpha_1, \dots, \alpha_q$
- $n = q - p + s + 1$
- all polynomials are given by a SLP af size L
- E_k: k-th elementary symmetric function

Theorem [Hauenstein-Safey El Din-Schost-**Vu**, 2021]

- there are at most

$$c = d_1 \dots d_s E_{n-s}(\alpha_1, \dots, \alpha_q)$$

  isolated solutions in $V_p(\boldsymbol{F}, \boldsymbol{G})$, counted with multiplicities;
- can be computed in time $(cL)^{O(1)}$ by a randomized algorithm.

Remark: Algs. for **sparse** and **weighted** polys in [Labahn-Safey El Din-Schost-**Vu**, 2021].

Our Result – Row Degrees

Suppose that:

- the degrees of $\boldsymbol{G} = (g_1, \dots, g_s)$ are at most $d_1, \dots, d_s$
- the row-degrees of $\boldsymbol{F}$ are at most $\beta_1, \dots, \beta_p$
- $n = q - p + s + 1$
- all polynomials are given by a SLP af size L
- S_k: k-th complete symmetric function

Our Result – Row Degrees

Suppose that:

- the degrees of $\boldsymbol{G} = (g_1, \dots, g_s)$ are at most $d_1, \dots, d_s$
- the row-degrees of $\boldsymbol{F}$ are at most $\beta_1, \dots, \beta_p$
- $n = q - p + s + 1$
- all polynomials are given by a SLP af size L
- S_k: k-th complete symmetric function

Theorem [Hauenstein-Safey El Din-Schost-**Vu**, 2021]

- there are at most

$$c' = d_1 \dots d_s S_{n-s}(\beta_1, \dots, \beta_p)$$

isolated solutions in $V_p(\boldsymbol{F}, \boldsymbol{G})$, counted with multiplicities;

Our Result – Row Degrees

Suppose that:

- the degrees of $\boldsymbol{G} = (g_1, \ldots, g_s)$ are at most $d_1, \ldots, d_s$
- the row-degrees of $\boldsymbol{F}$ are at most $\beta_1, \ldots, \beta_p$
- $n = q - p + s + 1$
- all polynomials are given by a SLP af size L
- S_k: k-th complete symmetric function

Theorem [Hauenstein-Safey El Din-Schost-**Vu**, 2021]

- there are at most

$$c' = d_1 \ldots d_s S_{n-s}(\beta_1, \ldots, \beta_p)$$

  isolated solutions in $V_p(\boldsymbol{F}, \boldsymbol{G})$, counted with multiplicities;
- can be computed in time $(c'L)^{O(1)}$ by a randomized algorithm.

Example (with $\mathbb{K} = \mathbb{Q}, n = 2, p = 2, q = 3$)

<u>**Compute:**</u> $\boldsymbol{x} \in \mathbb{C}^2$ such that $\operatorname{rank}(\boldsymbol{F}_1(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F}_1 = \begin{bmatrix} 3x_1 + x_2 - 1 & x_1 + 2x_2 + 4 & 5x_1 - 3x_2 + 2 \\ 2x_1 - 4x_2 + 3 & 3x_1 + 5x_2 - 2 & x_1^2 + 2x_1x_2 + x_2 - 1 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{2\times 3}$$

Example (with $\mathbb{K} = \mathbb{Q}, n = 2, p = 2, q = 3$)

Compute: $\boldsymbol{x} \in \mathbb{C}^2$ such that $\operatorname{rank}(\boldsymbol{F}_1(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F}_1 = \begin{bmatrix} 3x_1 + x_2 - 1 & x_1 + 2x_2 + 4 & 5x_1 - 3x_2 + 2 \\ 2x_1 - 4x_2 + 3 & 3x_1 + 5x_2 - 2 & x_1^2 + 2x_1x_2 + x_2 - 1 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{2\times 3}$$

Matrix of total degrees of $\boldsymbol{F}_1$: $\begin{bmatrix} [1] & [1] & [1] \\ [1] & [1] & [2] \end{bmatrix}$

Example (with $\mathbb{K} = \mathbb{Q}, n = 2, p = 2, q = 3$)

Compute: $\boldsymbol{x} \in \mathbb{C}^2$ such that $\operatorname{rank}(\boldsymbol{F}_1(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F}_1 = \begin{bmatrix} 3x_1 + x_2 - 1 & x_1 + 2x_2 + 4 & 5x_1 - 3x_2 + 2 \\ 2x_1 - 4x_2 + 3 & 3x_1 + 5x_2 - 2 & x_1^2 + 2x_1x_2 + x_2 - 1 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{2\times 3}$$

Matrix of total degrees of $\boldsymbol{F}_1$: $\begin{bmatrix} [1] & [1] & [1] \\ [1] & [1] & [2] \end{bmatrix}$

Column-Degree Bound:

- $\operatorname{cdeg}(\boldsymbol{F}_1) = (1, 1, 2)$
- $c = E_2(1, 1, 2) = 1^2 + 1\cdot 2 + 1\cdot 2 = \mathbf{5}$

Example (with $\mathbb{K} = \mathbb{Q}, n = 2, p = 2, q = 3$)

Compute: $\boldsymbol{x} \in \mathbb{C}^2$ such that $\operatorname{rank}(\boldsymbol{F}_1(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F}_1 = \begin{bmatrix} 3x_1 + x_2 - 1 & x_1 + 2x_2 + 4 & 5x_1 - 3x_2 + 2 \\ 2x_1 - 4x_2 + 3 & 3x_1 + 5x_2 - 2 & x_1^2 + 2x_1x_2 + x_2 - 1 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{2\times 3}$$

Matrix of total degrees of $\boldsymbol{F}_1$: $\begin{bmatrix} [1] & [1] & [1] \\ [1] & [1] & [2] \end{bmatrix}$

Column-Degree Bound:

- $\operatorname{cdeg}(\boldsymbol{F}_1) = (1, 1, 2)$
- $c = E_2(1, 1, 2) = 1^2 + 1\cdot 2 + 1\cdot 2 = \mathbf{5}$

Row-Degree Bound:

- $\operatorname{rdeg}(\boldsymbol{F}_1) = (1, 2)$
- $c' = S_2(1, 2) = 1^1 + 1 \cdot 2 + 2^2 = \mathbf{7}$

Example (with $\mathbb{K} = \mathbb{Q}, n = 2, p = 2, q = 3$)

Compute: $\boldsymbol{x} \in \mathbb{C}^2$ such that $\operatorname{rank}(\boldsymbol{F}_1(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F}_1 = \begin{bmatrix} 3x_1 + x_2 - 1 & x_1 + 2x_2 + 4 & 5x_1 - 3x_2 + 2 \\ 2x_1 - 4x_2 + 3 & 3x_1 + 5x_2 - 2 & x_1^2 + 2x_1x_2 + x_2 - 1 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{2\times 3}$$

Matrix of total degrees of $\boldsymbol{F}_1$: $\begin{bmatrix} [1] & [1] & [1] \\ [1] & [1] & [2] \end{bmatrix}$

Column-Degree Bound:

- $\text{cdeg}(\boldsymbol{F}_1) = (1, 1, 2)$
- $c = E_2(1, 1, 2) = 1^2 + 1\cdot 2 + 1\cdot 2 = \mathbf{5}$

Row-Degree Bound:

- $\text{rdeg}(\boldsymbol{F}_1) = (1, 2)$
- $c' = S_2(1, 2) = 1^1 + 1\cdot 2 + 2^2 = \mathbf{7}$

$$\boxed{c < c'}$$

Example (with $\mathbb{K} = \mathbb{Q}, n = 2, p = 2, q = 3$)

Compute: $\boldsymbol{x} \in \mathbb{C}^2$ such that $\operatorname{rank}(\boldsymbol{F}_2(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F}_2 = \begin{bmatrix} x_1 + x_2 & 3x_1 + 5x_2 + 2 & 10x_1 + x_2 - 1 \\ x_2^2 + x_1 + 10x_2 + 3 & x_1^2 + 3x_1x_2 + x_1 - 1 & x_1^2 - 4x_1x_2 + x_2^2 + 3 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{p \times q}$$

Example (with $\mathbb{K} = \mathbb{Q}, n = 2, p = 2, q = 3$)

<u>**Compute:**</u> $\boldsymbol{x} \in \mathbb{C}^2$ such that $\operatorname{rank}(\boldsymbol{F}_2(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F}_2 = \begin{bmatrix} x_1 + x_2 & 3x_1 + 5x_2 + 2 & 10x_1 + x_2 - 1 \\ x_2^2 + x_1 + 10x_2 + 3 & x_1^2 + 3x_1x_2 + x_1 - 1 & x_1^2 - 4x_1x_2 + x_2^2 + 3 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{p \times q}$$

Matrix of total degrees of $\boldsymbol{F}_2$:

$$\begin{bmatrix} [1] & [1] & [1] \\ [2] & [2] & [2] \end{bmatrix}$$

Example (with $\mathbb{K} = \mathbb{Q}, n = 2, p = 2, q = 3$)

<u>**Compute:**</u> $\boldsymbol{x} \in \mathbb{C}^2$ such that $\operatorname{rank}(\boldsymbol{F}_2(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F}_2 = \begin{bmatrix} x_1 + x_2 & 3x_1 + 5x_2 + 2 & 10x_1 + x_2 - 1 \\ x_2^2 + x_1 + 10x_2 + 3 & x_1^2 + 3x_1x_2 + x_1 - 1 & x_1^2 - 4x_1x_2 + x_2^2 + 3 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{p \times q}$$

Matrix of total degrees of $\boldsymbol{F}_2$:

$$\begin{bmatrix} [1] & [1] & [1] \\ [2] & [2] & [2] \end{bmatrix}$$

Column-Degree Bound:

- cdeg$(\boldsymbol{F}_2) = (2, 2, 2)$
- $c = E_2(2, 2, 2) = 2^2 + 2^2 + 2^2 = \mathbf{12}$

Example (with $\mathbb{K} = \mathbb{Q}, n = 2, p = 2, q = 3$)

Compute: $\boldsymbol{x} \in \mathbb{C}^2$ such that $\operatorname{rank}(\boldsymbol{F}_2(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F}_2 = \begin{bmatrix} x_1 + x_2 & 3x_1 + 5x_2 + 2 & 10x_1 + x_2 - 1 \\ x_2^2 + x_1 + 10x_2 + 3 & x_1^2 + 3x_1x_2 + x_1 - 1 & x_1^2 - 4x_1x_2 + x_2^2 + 3 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{p \times q}$$

Matrix of total degrees of $\boldsymbol{F}_2$:

$$\begin{bmatrix} [1] & [1] & [1] \\ [2] & [2] & [2] \end{bmatrix}$$

Column-Degree Bound:

- $\operatorname{cdeg}(\boldsymbol{F}_2) = (2, 2, 2)$
- $c = E_2(2, 2, 2) = 2^2 + 2^2 + 2^2 = \mathbf{12}$

Row-Degree Bound:

- $\operatorname{rdeg}(\boldsymbol{F}_2) = (1, 2)$
- $c' = S_2(1, 2) = 1^1 + 1 \cdot 2 + 2^2 = \mathbf{7}$

Example (with $\mathbb{K} = \mathbb{Q}, n = 2, p = 2, q = 3$)

Compute: $\boldsymbol{x} \in \mathbb{C}^2$ such that $\operatorname{rank}(\boldsymbol{F}_2(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F}_2 = \begin{bmatrix} x_1 + x_2 & 3x_1 + 5x_2 + 2 & 10x_1 + x_2 - 1 \\ x_2^2 + x_1 + 10x_2 + 3 & x_1^2 + 3x_1x_2 + x_1 - 1 & x_1^2 - 4x_1x_2 + x_2^2 + 3 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{p \times q}$$

Matrix of total degrees of $\boldsymbol{F}_2$:

$$\begin{bmatrix} [1] & [1] & [1] \\ [2] & [2] & [2] \end{bmatrix}$$

Column-Degree Bound:

- $\operatorname{cdeg}(\boldsymbol{F}_2) = (2, 2, 2)$
- $c = E_2(2, 2, 2) = 2^2 + 2^2 + 2^2 = \mathbf{12}$

Row-Degree Bound:

- $\operatorname{rdeg}(\boldsymbol{F}_2) = (1, 2)$
- $c' = S_2(1, 2) = 1^1 + 1 \cdot 2 + 2^2 = \mathbf{7}$

$$\boxed{c > c'}$$

Previous Work

[Giambelli], [Conca-Herzog], [Miller-Sturmfels]

- Hilbert function of determinantal ideals of generic matrices

[Huber-Sottile-Sturmfels], [Verschelde]

- Schbert calculus
- minors of generic matrices

[Nie-Ranestad]

- degree bounds $E_{n-s}()$ and $S_{n-s}()$ are sharp for generic polynomials (we reuse their construction for column degrees)

[Faugère-Safey El Din-Spaenlehauer], [Spaenlehauer]

- complexity of Gröbner basis for generic polynomials

[Gopalakrishnan-Neiger-Safey El Din], [Gopalakrishnan]

- optimizing Gröbner basis computation for more structured determinantal ideals

Homotopies for Determinantal Systems ($s = 0$, to simplify)

Recall our Problem

Given: matrix $\boldsymbol{F} = \left[f_{i,j} \right] \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}$ with $n = q - p + 1$

Compute: the isolated points of $V_p(\boldsymbol{F}) = \left\{ \boldsymbol{x} \in \overline{\mathbb{K}}^n : \operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < p \right\}$

- The target system we want to solve $\boldsymbol{C} = (c_i)_{i \leq \binom{q}{p}} = (p\text{-minors of } \boldsymbol{F})$

Homotopies for Determinantal Systems ($s = 0$, to simplify)

Recall our Problem

Given: matrix $\boldsymbol{F} = \left[f_{i,j}\right] \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}$ with $n = q - p + 1$

Compute: the isolated points of $V_p(\boldsymbol{F}) = \left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : \operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < p\right\}$

- The target system we want to solve $\boldsymbol{C} = (c_i)_{i \leq \binom{q}{p}} = (p\text{-minors of } \boldsymbol{F})$
- Find a **start matrix** $\boldsymbol{L} \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}$ such that it is **easy** to compute

$$V_p(\boldsymbol{L}) = \left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : \operatorname{rank}(\boldsymbol{L}(\boldsymbol{x})) < p\right\}$$

Homotopies for Determinantal Systems ($s = 0$, to simplify)

Recall our Problem

Given: matrix $\boldsymbol{F} = \left[f_{i,j}\right] \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}$ with $n = q - p + 1$

Compute: the isolated points of $V_p(\boldsymbol{F}) = \left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : \operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < p\right\}$

- The target system we want to solve $\boldsymbol{C} = (c_i)_{i \leq \binom{q}{p}} = (p\text{-minors of } \boldsymbol{F})$
- Find a **start matrix** $\boldsymbol{L} \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}$ such that it is **easy** to compute

$$V_p(\boldsymbol{L}) = \left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : p\text{-minors of } \boldsymbol{L} \text{ vanish}\right\}$$

Homotopies for Determinantal Systems ($s = 0$, to simplify)

Recall our Problem

Given: matrix $\boldsymbol{F} = \left[f_{i,j}\right] \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}$ with $n = q - p + 1$

Compute: the isolated points of $V_p(\boldsymbol{F}) = \left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : \operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < p\right\}$

- The target system we want to solve $\boldsymbol{C} = (c_i)_{i \leq \binom{q}{p}} = (p\text{-minors of } \boldsymbol{F})$
- Find a **start matrix** $\boldsymbol{L} \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}$ such that it is **easy** to compute

$$V_p(\boldsymbol{L}) = \left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : p\text{-minors of } \boldsymbol{L} \text{ vanish}\right\}$$

- Start system $\boldsymbol{A} = (a_i)_{i \leq \binom{q}{p}} = (p\text{-minors of } \boldsymbol{L})$

Homotopies for Determinantal Systems ($s = 0$, to simplify)

Recall our Problem

Given: matrix $\boldsymbol{F} = \left[f_{i,j}\right] \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}$ with $n = q - p + 1$

Compute: the isolated points of $V_p(\boldsymbol{F}) = \left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : \operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < p\right\}$

- The target system we want to solve $\boldsymbol{C} = (c_i)_{i \le \binom{q}{p}} = (p\text{-minors of } \boldsymbol{F})$
- Find a **start matrix** $\boldsymbol{L} \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}$ such that it is **easy** to compute

$$V_p(\boldsymbol{L}) = \left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : p\text{-minors of } \boldsymbol{L} \text{ vanish}\right\}$$

- Start system $\boldsymbol{A} = (a_i)_{i \le \binom{q}{p}} = (p\text{-minors of } \boldsymbol{L})$
- Deformed system $\boldsymbol{B} = (b_i)_{i \le \binom{q}{p}} = (p\text{-minors of } \boldsymbol{H})$, where

$$\boldsymbol{H} = (1 - t) \cdot \boldsymbol{L} + t \cdot \boldsymbol{F} \in \mathbb{K}[t, \boldsymbol{X}]^{p \times q}$$

Homotopies for Determinantal Systems ($s = 0$, to simplify)

Recall our Problem

Given: matrix $\boldsymbol{F} = \left[f_{i,j}\right] \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ with $n = q - p + 1$

Compute: the isolated points of $V_p(\boldsymbol{F}) = \left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : \operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < p\right\}$

- The target system we want to solve $\boldsymbol{C} = (c_i)_{i \leq \binom{q}{p}} = (p\text{-minors of } \boldsymbol{F})$
- Find a **start matrix** $\boldsymbol{L} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$ such that it is **easy** to compute

$$V_p(\boldsymbol{L}) = \left\{\boldsymbol{x} \in \overline{\mathbb{K}}^n : p\text{-minors of } \boldsymbol{L} \text{ vanish}\right\}$$

- Start system $\boldsymbol{A} = (a_i)_{i \leq \binom{q}{p}} = (p\text{-minors of } \boldsymbol{L})$
- Deformed system $\boldsymbol{B} = (b_i)_{i \leq \binom{q}{p}} = (p\text{-minors of } \boldsymbol{H})$, where

$$\boldsymbol{H} = (1 - t) \cdot \boldsymbol{L} + t \cdot \boldsymbol{F} \in \mathbb{K}[t, \boldsymbol{X}]^{p \times q}$$

In particular, $\boldsymbol{B}(0, \boldsymbol{X}) = \boldsymbol{A}$ and $\boldsymbol{B}(1, \boldsymbol{X}) = \boldsymbol{C}$.

Row Degrees Homotopies ($s = 0$, to simplify)

Start Matrix Structure: $\boldsymbol{L} =$

$$\begin{bmatrix} \ell_{1,1} & & & & \ell_{1,p+1} & \cdots & \ell_{1,q} \\ & \ell_{2,2} & & & \ell_{2,p+1} & \cdots & \ell_{2,q} \\ & & \ddots & & \vdots & & \vdots \\ & & & \ell_{p,p} & \ell_{p,p+1} & \cdots & \ell_{p,q}, \end{bmatrix}$$

where each $\ell_{i,j}$ is a product of β_i random linear forms.

Row Degrees Homotopies ($s = 0$, to simplify)

Start Matrix Structure: $L = \begin{bmatrix} \ell_{1,1} & & & & \ell_{1,p+1} & \cdots & \ell_{1,q} \\ & \ell_{2,2} & & & \ell_{2,p+1} & \cdots & \ell_{2,q} \\ & & \ddots & & \vdots & & \vdots \\ & & & \ell_{p,p} & \ell_{p,p+1} & \cdots & \ell_{p,q}, \end{bmatrix}$

where each $\ell_{i,j}$ is a product of β_i random linear forms.

Theorem [Hauenstein-Safey El Din-Schost-**Vu**, 2021]

For generic $\ell_{i,j}$, the row homotopy is well-defined and succeeds.

Row Degrees Homotopies ($s = 0$, to simplify)

Start Matrix Structure: $\boldsymbol{L} = \begin{bmatrix} \ell_{1,1} & & & & \ell_{1,p+1} & \cdots & \ell_{1,q} \\ & \ell_{2,2} & & & \ell_{2,p+1} & \cdots & \ell_{2,q} \\ & & \ddots & & \vdots & & \vdots \\ & & & \ell_{p,p} & \ell_{p,p+1} & \cdots & \ell_{p,q}, \end{bmatrix}$

where each $\ell_{i,j}$ is a product of β_i random linear forms.

Theorem [Hauenstein-Safey El Din-Schost-**Vu**, 2021]

For generic $\ell_{i,j}$, the row homotopy is well-defined and succeeds.

Properties

$\mathrm{rank}(\boldsymbol{L}) < p \iff$ some τ diagonal forms $\ell_{i,i}$ vanish **and**

Row Degrees Homotopies ($s = 0$, to simplify)

Start Matrix Structure: $\boldsymbol{L} = \begin{bmatrix} \ell_{1,1} & & & & \ell_{1,p+1} & \cdots & \ell_{1,q} \\ & \ell_{2,2} & & & \ell_{2,p+1} & \cdots & \ell_{2,q} \\ & & \ddots & & \vdots & & \vdots \\ & & & \ell_{p,p} & \ell_{p,p+1} & \cdots & \ell_{p,q}, \end{bmatrix}$

where each $\ell_{i,j}$ is a product of β_i random linear forms.

Theorem [Hauenstein-Safey El Din-Schost-**Vu**, 2021]

For generic $\ell_{i,j}$, the row homotopy is well-defined and succeeds.

Properties

$\operatorname{rank}(\boldsymbol{L}) < p \iff$ some τ diagonal forms $\ell_{i,i}$ vanish **and** the corresponding right-block is rank-deficient.

Row Degrees Homotopies ($s = 0$, to simplify)

Start Matrix Structure: $\boldsymbol{L} = \begin{bmatrix} \ell_{1,1} & & & & \ell_{1,p+1} & \cdots & \ell_{1,q} \\ & \ell_{2,2} & & & \ell_{2,p+1} & \cdots & \ell_{2,q} \\ & & \ddots & & \vdots & & \vdots \\ & & & \ell_{p,p} & \ell_{p,p+1} & \cdots & \ell_{p,q}, \end{bmatrix}$

where each $\ell_{i,j}$ is a product of β_i random linear forms.

Theorem [Hauenstein-Safey El Din-Schost-**Vu**, 2021]

For generic $\ell_{i,j}$, the row homotopy is well-defined and succeeds.

Properties

$\operatorname{rank}(\boldsymbol{L}) < p \iff$ some τ diagonal forms $\ell_{i,i}$ vanish **and** the corresponding right-block is rank-deficient.

$\implies$ a $\tau \times (n-1)$ matrix in $n - \tau$ variables.

Row Degrees Homotopies ($s = 0$, to simplify)

Start Matrix Structure: $$\boldsymbol{L} = \begin{bmatrix} \ell_{1,1} & & & & \ell_{1,p+1} & \cdots & \ell_{1,q} \\ & \ell_{2,2} & & & \ell_{2,p+1} & \cdots & \ell_{2,q} \\ & & \ddots & & \vdots & & \vdots \\ & & & \ell_{p,p} & \ell_{p,p+1} & \cdots & \ell_{p,q}, \end{bmatrix}$$

where each $\ell_{i,j}$ is a product of β_i random linear forms.

Theorem [Hauenstein-Safey El Din-Schost-**Vu**, 2021]

For generic $\ell_{i,j}$, the row homotopy is well-defined and succeeds.

Properties

$\mathrm{rank}(\boldsymbol{L}) < p \iff$ some τ diagonal forms $\ell_{i,i}$ vanish **and** the corresponding right-block is rank-deficient.

$\implies$ a $\tau \times (n-1)$ matrix in $n - \tau$ variables.

We recursively use a homotopy to solve the start system

Example (rdeg$(\boldsymbol{F}) = (1,2)$ and bound $c' = 7$)

Compute: $\boldsymbol{x} \in \mathbb{C}^2$ such that $\operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F} = \begin{bmatrix} x_1 + x_2 & 3x_1 + 5x_2 + 2 & 10x_1 + x_2 - 1 \\ x_2^2 + x_1 + 10x_2 + 3 & x_1^2 + 3x_1x_2 + x_1 - 1 & x_1^2 - 4x_1x_2 + x_2^2 + 3 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{p \times q}$$

Example ($\mathrm{rdeg}(\boldsymbol{F}) = (1, 2)$ and bound $c' = 7$)

Compute: $\boldsymbol{x} \in \mathbb{C}^2$ such that $\mathrm{rank}\,(\boldsymbol{F}(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F} = \begin{bmatrix} x_1 + x_2 & 3x_1 + 5x_2 + 2 & 10x_1 + x_2 - 1 \\ x_2^2 + x_1 + 10x_2 + 3 & x_1^2 + 3x_1x_2 + x_1 - 1 & x_1^2 - 4x_1x_2 + x_2^2 + 3 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{p \times q}$$

Start matrix:

$$\boldsymbol{L} = \begin{bmatrix} -x_1 + 10x_2 + 1 & 0 & x_1 + x_2 + 2 \\ 0 & (x_1 - 3x_2 + 5)(x_1 + 2x_2 - 4) & (3x_1 + 2x_2 - 1)(2x_1 - 3x_2 + 5) \end{bmatrix}$$

Example ($\mathrm{rdeg}(\boldsymbol{F}) = (1,2)$ and bound $c' = 7$)

Compute: $\boldsymbol{x} \in \mathbb{C}^2$ such that $\mathrm{rank}\,(\boldsymbol{F}(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F} = \begin{bmatrix} x_1 + x_2 & 3x_1 + 5x_2 + 2 & 10x_1 + x_2 - 1 \\ x_2^2 + x_1 + 10x_2 + 3 & x_1^2 + 3x_1x_2 + x_1 - 1 & x_1^2 - 4x_1x_2 + x_2^2 + 3 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{p \times q}$$

Start matrix:

$$\boldsymbol{L} = \begin{bmatrix} -x_1 + 10x_2 + 1 & 0 & x_1 + x_2 + 2 \\ 0 & (x_1 - 3x_2 + 5)(x_1 + 2x_2 - 4) & (3x_1 + 2x_2 - 1)(2x_1 - 3x_2 + 5) \end{bmatrix}$$

Rank-contrained for $\boldsymbol{L}$: $\quad \mathrm{rank}(\boldsymbol{L}) < 2 \iff \begin{cases} -x_1 + 10x_2 + 1 = 0 \\ x_1 + x_2 + 2 = 0 \end{cases}$ or

Example ($\mathrm{rdeg}(\boldsymbol{F}) = (1,2)$ and bound $c' = 7$)

Compute: $\boldsymbol{x} \in \mathbb{C}^2$ such that $\mathrm{rank}\left(\boldsymbol{F}(\boldsymbol{x})\right) < 2$, where

$$\boldsymbol{F} = \begin{bmatrix} x_1 + x_2 & 3x_1 + 5x_2 + 2 & 10x_1 + x_2 - 1 \\ x_2^2 + x_1 + 10x_2 + 3 & x_1^2 + 3x_1x_2 + x_1 - 1 & x_1^2 - 4x_1x_2 + x_2^2 + 3 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{p \times q}$$

Start matrix:

$$\boldsymbol{L} = \begin{bmatrix} -x_1 + 10x_2 + 1 & 0 & x_1 + x_2 + 2 \\ 0 & (x_1 - 3x_2 + 5)(x_1 + 2x_2 - 4) & (3x_1 + 2x_2 - 1)(2x_1 - 3x_2 + 5) \end{bmatrix}$$

Rank-contrained for $\boldsymbol{L}$: $\quad \mathrm{rank}(\boldsymbol{L}) < 2 \iff \begin{cases} -x_1 + 10x_2 + 1 = 0 \\ x_1 + x_2 + 2 = 0 \end{cases}$ or

$$\begin{cases} (x_1 - 3x_2 + 5)(x_1 + 2x_2 - 4) = 0 \\ (3x_1 + 2x_2 - 1)(2x_1 - 3x_2 + 5) = 0 \end{cases}$$

Example ($\mathrm{rdeg}(\boldsymbol{F}) = (1, 2)$ and bound $c' = 7$)

Compute: $\boldsymbol{x} \in \mathbb{C}^2$ such that $\mathrm{rank}\,(\boldsymbol{F}(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F} = \begin{bmatrix} x_1 + x_2 & 3x_1 + 5x_2 + 2 & 10x_1 + x_2 - 1 \\ x_2^2 + x_1 + 10x_2 + 3 & x_1^2 + 3x_1x_2 + x_1 - 1 & x_1^2 - 4x_1x_2 + x_2^2 + 3 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{p \times q}$$

Start matrix:

$$\boldsymbol{L} = \begin{bmatrix} -x_1 + 10x_2 + 1 & 0 & x_1 + x_2 + 2 \\ 0 & (x_1 - 3x_2 + 5)(x_1 + 2x_2 - 4) & (3x_1 + 2x_2 - 1)(2x_1 - 3x_2 + 5) \end{bmatrix}$$

Rank-contrained for $\boldsymbol{L}$: $\mathrm{rank}(\boldsymbol{L}) < 2 \iff \begin{cases} -x_1 + 10x_2 + 1 = 0 \\ x_1 + x_2 + 2 = 0 \end{cases}$ or

$$\begin{cases} (x_1 - 3x_2 + 5)(x_1 + 2x_2 - 4) = 0 \\ (3x_1 + 2x_2 - 1)(2x_1 - 3x_2 + 5) = 0 \end{cases} \quad \text{or} \quad \begin{cases} -x_1 + 10x_2 + 1 = 0 \\ (x_1 - 3x_2 + 5)(x_1 + 2x_2 - 4) = 0 \end{cases}$$

Example ($\text{rdeg}(\boldsymbol{F}) = (1, 2)$ and bound $c' = 7$)

Compute: $\boldsymbol{x} \in \mathbb{C}^2$ such that $\operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F} = \begin{bmatrix} x_1 + x_2 & 3x_1 + 5x_2 + 2 & 10x_1 + x_2 - 1 \\ x_2^2 + x_1 + 10x_2 + 3 & x_1^2 + 3x_1x_2 + x_1 - 1 & x_1^2 - 4x_1x_2 + x_2^2 + 3 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{p \times q}$$

Start matrix:

$$\boldsymbol{L} = \begin{bmatrix} -x_1 + 10x_2 + 1 & 0 & x_1 + x_2 + 2 \\ 0 & (x_1 - 3x_2 + 5)(x_1 + 2x_2 - 4) & (3x_1 + 2x_2 - 1)(2x_1 - 3x_2 + 5) \end{bmatrix}$$

Rank-contrained for $\boldsymbol{L}$: $\operatorname{rank}(\boldsymbol{L}) < 2 \iff \begin{cases} -x_1 + 10x_2 + 1 = 0 \\ x_1 + x_2 + 2 = 0 \end{cases}$ or

$$\begin{cases} (x_1 - 3x_2 + 5)(x_1 + 2x_2 - 4) = 0 \\ (3x_1 + 2x_2 - 1)(2x_1 - 3x_2 + 5) = 0 \end{cases} \quad \text{or} \quad \begin{cases} -x_1 + 10x_2 + 1 = 0 \\ (x_1 - 3x_2 + 5)(x_1 + 2x_2 - 4) = 0 \end{cases}$$

$$\boxed{c' = 1^2 + 2^2 + 1 \cdot 2}$$

Column Homotopies ($s = 0$, to simplify)

Start Matrix Structure:

$$\boldsymbol{L} = \begin{bmatrix} 1 & 2 & \cdots & q \\ 1 & 2^2 & \cdots & q^2 \\ \vdots & \vdots & & \vdots \\ 1 & 2^p & \cdots & q^p \end{bmatrix} \begin{bmatrix} \ell_1 & & \\ & \ddots & \\ & & \ell_q \end{bmatrix} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$$

Column Homotopies ($s = 0$, to simplify)

Start Matrix Structure:

$$\boldsymbol{L} = \begin{bmatrix} 1 & 2 & \cdots & q \\ 1 & 2^2 & \cdots & q^2 \\ \vdots & \vdots & & \vdots \\ 1 & 2^p & \cdots & q^p \end{bmatrix} \begin{bmatrix} \ell_1 & & \\ & \ddots & \\ & & \ell_q \end{bmatrix} \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}$$

Case / Context	**Structure of ℓ_i**
column total-degree case	a product δ_i random linear forms
column-support case	a generic sparse polynomial
weighted column-degree case	a generic weighted polynomial

Column Homotopies ($s = 0$, to simplify)

Start Matrix Structure:

$$\boldsymbol{L} = \begin{bmatrix} 1 & 2 & \cdots & q \\ 1 & 2^2 & \cdots & q^2 \\ \vdots & \vdots & & \vdots \\ 1 & 2^p & \cdots & q^p \end{bmatrix} \begin{bmatrix} \ell_1 & & \\ & \ddots & \\ & & \ell_q \end{bmatrix} \in \mathbb{K}[x_1, \ldots, x_n]^{p \times q}$$

Case / Context	**Structure of ℓ_i**
column total-degree case	a product δ_i random linear forms
column-support case	a generic sparse polynomial
weighted column-degree case	a generic weighted polynomial

Theorem [Hauenstein-Safey El Din-Schost-**Vu**, 2021] [Labahn-Safey El Din-Schost-**Vu**, 2021]

For each case, all assumptions for our homotopy algorithms are satisfied.

Column Degrees Homotopies - Solving the Start Systems

Start Matrix Structure:

$$\boldsymbol{L} = \begin{bmatrix} 1 & 2 & \cdots & q \\ 1 & 2^2 & \cdots & q^2 \\ \vdots & \vdots & & \vdots \\ 1 & 2^p & \cdots & q^p \end{bmatrix} \begin{bmatrix} \ell_1 & & \\ & \ddots & \\ & & \ell_q \end{bmatrix} \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}.$$

where ℓ_i is a product of δ_i random linear forms.

Column Degrees Homotopies - Solving the Start Systems

Start Matrix Structure:

$$\boldsymbol{L} = \begin{bmatrix} 1 & 2 & \cdots & q \\ 1 & 2^2 & \cdots & q^2 \\ \vdots & \vdots & & \vdots \\ 1 & 2^p & \cdots & q^p \end{bmatrix} \begin{bmatrix} \ell_1 & & \\ & \ddots & \\ & & \ell_q \end{bmatrix} \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}.$$

where ℓ_i is a product of δ_i random linear forms.

Properties:

$$\operatorname{rank}(\boldsymbol{L}) < p \iff \operatorname{rank}\left(\begin{bmatrix} \ell_1 & & \\ & \ddots & \\ & & \ell_q \end{bmatrix} \right) < p$$

Column Degrees Homotopies - Solving the Start Systems

Start Matrix Structure:

$$\boldsymbol{L} = \begin{bmatrix} 1 & 2 & \cdots & q \\ 1 & 2^2 & \cdots & q^2 \\ \vdots & \vdots & & \vdots \\ 1 & 2^p & \cdots & q^p \end{bmatrix} \begin{bmatrix} \ell_1 & & \\ & \ddots & \\ & & \ell_q \end{bmatrix} \in \mathbb{K}[x_1, \dots, x_n]^{p \times q}.$$

where ℓ_i is a product of δ_i random linear forms.

Properties:

$$\operatorname{rank}(\boldsymbol{L}) < p \iff \operatorname{rank}\left(\begin{bmatrix} \ell_1 & & \\ & \ddots & \\ & & \ell_q \end{bmatrix}\right) < p \iff n \text{ equations } \ell_i \text{ vanish.}$$

Example (cdeg$(\boldsymbol{F}) = (1, 1, 2)$ and bound $c = 5$)

Compute: $\boldsymbol{x} \in \mathbb{C}^2$ such that $\operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F} = \begin{bmatrix} 3x_1 + x_2 - 1 & x_1 + 2x_2 + 4 & 5x_1 - 3x_2 + 2 \\ 2x_1 - 4x_2 + 3 & 3x_1 + 5x_2 - 2 & x_1^2 + 2x_1x_2 + x_2 - 1 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{2\times 3}$$

Example ($\mathrm{cdeg}(\boldsymbol{F}) = (1, 1, 2)$ and bound $c = 5$)

<u>**Compute:**</u> $\boldsymbol{x} \in \mathbb{C}^2$ such that $\mathrm{rank}\,(\boldsymbol{F}(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F} = \begin{bmatrix} 3x_1 + x_2 - 1 & x_1 + 2x_2 + 4 & 5x_1 - 3x_2 + 2 \\ 2x_1 - 4x_2 + 3 & 3x_1 + 5x_2 - 2 & x_1^2 + 2x_1x_2 + x_2 - 1 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{2\times 3}$$

Start matrix:

$$\boldsymbol{L} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2^2 & 3^2 \end{bmatrix} \begin{bmatrix} 4x_1 - 3x_2 + 5 & & \\ & 3x_1 + 5x_2 - 2 & \\ & & (3x_1 + 2x_2 - 1)(x_1 - 5x_2 + 4) \end{bmatrix}$$

Example (cdeg($\boldsymbol{F}$) $= (1,1,2)$ and bound $c = 5$)

Compute: $\boldsymbol{x} \in \mathbb{C}^2$ such that $\operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F} = \begin{bmatrix} 3x_1 + x_2 - 1 & x_1 + 2x_2 + 4 & 5x_1 - 3x_2 + 2 \\ 2x_1 - 4x_2 + 3 & 3x_1 + 5x_2 - 2 & x_1^2 + 2x_1x_2 + x_2 - 1 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{2\times 3}$$

Start matrix:

$$\boldsymbol{L} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2^2 & 3^2 \end{bmatrix} \begin{bmatrix} 4x_1 - 3x_2 + 5 & & \\ & 3x_1 + 5x_2 - 2 & \\ & & (3x_1 + 2x_2 - 1)(x_1 - 5x_2 + 4) \end{bmatrix}$$

Rank-contrained for $\boldsymbol{L}$:

$$\operatorname{rank}(\boldsymbol{L}) < 2 \iff \begin{cases} (4x_1 - 3x_2 + 5)(3x_1 + 5x_2 - 2) = 0 \\ (4x_1 - 3x_2 + 5)(3x_1 + 2x_2 - 1)(x_1 - 5x_2 + 4) = 0 \\ (3x_1 + 5x_2 - 2)(3x_1 + 2x_2 - 1)(x_1 - 5x_2 + 4) = 0 \end{cases}$$

Example ($\mathrm{cdeg}(\boldsymbol{F}) = (1,1,2)$ and bound $c=5$)

Compute: $\boldsymbol{x} \in \mathbb{C}^2$ such that $\mathrm{rank}\,(\boldsymbol{F}(\boldsymbol{x})) < 2$, where

$$\boldsymbol{F} = \begin{bmatrix} 3x_1 + x_2 - 1 & x_1 + 2x_2 + 4 & 5x_1 - 3x_2 + 2 \\ 2x_1 - 4x_2 + 3 & 3x_1 + 5x_2 - 2 & x_1^2 + 2x_1x_2 + x_2 - 1 \end{bmatrix} \in \mathbb{Q}[x_1, x_2]^{2\times 3}$$

Start matrix:

$$\boldsymbol{L} = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2^2 & 3^2 \end{bmatrix} \begin{bmatrix} 4x_1 - 3x_2 + 5 & & \\ & 3x_1 + 5x_2 - 2 & \\ & & (3x_1 + 2x_2 - 1)(x_1 - 5x_2 + 4) \end{bmatrix}$$

Rank-contrained for $\boldsymbol{L}$:

$$\mathrm{rank}(\boldsymbol{L}) < 2 \iff \begin{cases} (4x_1 - 3x_2 + 5)(3x_1 + 5x_2 - 2) = 0 \\ (4x_1 - 3x_2 + 5)(3x_1 + 2x_2 - 1)(x_1 - 5x_2 + 4) = 0 \\ (3x_1 + 5x_2 - 2)(3x_1 + 2x_2 - 1)(x_1 - 5x_2 + 4) = 0 \end{cases}$$

$$\begin{cases} 4x_1 - 3x_2 + 5 = 0 \\ 3x_1 + 2x_2 - 1 = 0 \end{cases} \text{ or } \begin{cases} 4x_1 - 3x_2 + 5 = 0 \\ x_1 - 5x_2 + 4 = 0 \end{cases} \text{ or } \begin{cases} 3x_1 + 5x_2 - 2 \\ x_1 - 5x_2 + 4 = 0 \end{cases} \text{ or } \cdots$$

5 linear square systems

Why Sparse and Weighted Degree Polynomials?

Classical Bézout Theorem

A system of n polynomial equations $f_1(\boldsymbol{X}) = 0, \ldots, f_n(\boldsymbol{X}) = 0$ with degrees $d_1, \ldots, d_n$ has at most

$$d_1 \cdots d_n \text{ isolated solutions.}$$

Why Sparse and Weighted Degree Polynomials?

Bernstein-Kushnirenko-Khovanskii (BKK) Theorem

A system of n sparse polynomial equations $f_1(\boldsymbol{X}) = 0, \dots, f_n(\boldsymbol{X}) = 0$ with Newton polytopes $P_1, \dots, P_n \subset \mathbb{R}^n$ has at most

$$\mathcal{M}(P_1, \dots, P_n) \text{ isolated solution,}$$

where $\mathcal{M}$ denotes the mixed volume.

Why Sparse and Weighted Degree Polynomials?

Weighted Bézout Theorem

A system of n weighted polynomial equations $f_1(\boldsymbol{X}) = 0, \dots, f_n(\boldsymbol{X}) = 0$ with respect to weight vector $\boldsymbol{w} = (w_1, \dots, w_n) \in \mathbb{Z}^n_{>0}$ and weighted degrees $d_1, \dots, d_n$ has at most

$$\frac{d_1 \cdots d_n}{w_1 \cdots w_n} \text{ isolated solutions.}$$

Why Sparse and Weighted Degree Polynomials?

Weighted Bézout Theorem

A system of n weighted polynomial equations $f_1(\boldsymbol{X}) = 0, \dots, f_n(\boldsymbol{X}) = 0$ with respect to weight vector $\boldsymbol{w} = (w_1, \dots, w_n) \in \mathbb{Z}^n_{>0}$ and weighted degrees $d_1, \dots, d_n$ has at most

$$\frac{d_1 \cdots d_n}{w_1 \cdots w_n} \text{ isolated solutions.}$$

$$\phi(\boldsymbol{X}) = x_1^2 + x_2^2 + x_3^2 - 3(x_1x_2 + x_1x_3 + x_2x_3)$$

Why Sparse and Weighted Degree Polynomials?

Weighted Bézout Theorem

A system of n weighted polynomial equations $f_1(\boldsymbol{X}) = 0, \ldots, f_n(\boldsymbol{X}) = 0$ with respect to weight vector $\boldsymbol{w} = (w_1, \ldots, w_n) \in \mathbb{Z}^n_{>0}$ and weighted degrees $d_1, \ldots, d_n$ has at most

$$\frac{d_1 \cdots d_n}{w_1 \cdots w_n} \text{ isolated solutions.}$$

$$\phi(\boldsymbol{X}) = x_1^2 + x_2^2 + x_3^2 - 3(x_1x_2 + x_1x_3 + x_2x_3)$$

- [Fundamental Theorem of Symmetric Polynomials], there is unique polynomial
$$\bar{\boldsymbol{\phi}} = \boldsymbol{e_1^2} - \boldsymbol{5e_2} \text{ such that } \bar{\phi}(E_1(\boldsymbol{X}), E_2(\boldsymbol{X})) = \phi(\boldsymbol{X}).$$
- $E_k(\boldsymbol{X})$: elementary symmetric polynomial of degree k

Why Sparse and Weighted Degree Polynomials?

Weighted Bézout Theorem

A system of n weighted polynomial equations $f_1(\boldsymbol{X}) = 0, \dots, f_n(\boldsymbol{X}) = 0$ with respect to weight vector $\boldsymbol{w} = (w_1, \dots, w_n) \in \mathbb{Z}^n_{>0}$ and weighted degrees $d_1, \dots, d_n$ has at most

$$\frac{d_1 \cdots d_n}{w_1 \cdots w_n} \text{ isolated solutions.}$$

$$\phi(\boldsymbol{X}) = x_1^2 + x_2^2 + x_3^2 - 3(x_1x_2 + x_1x_3 + x_2x_3)$$

- [Fundamental Theorem of Symmetric Polynomials], there is unique polynomial

  $\boldsymbol{\bar{\phi} = e_1^2 - 5e_2}$ such that $\bar{\phi}(E_1(\boldsymbol{X}), E_2(\boldsymbol{X})) = \phi(\boldsymbol{X})$.

- $E_k(\boldsymbol{X})$: elementary symmetric polynomial of degree k

- $E_2(\boldsymbol{X}) = x_1x_2 + x_1x_3 + x_2x_3$

Why Sparse and Weighted Degree Polynomials?

Weighted Bézout Theorem

A system of n weighted polynomial equations $f_1(\boldsymbol{X}) = 0, \dots, f_n(\boldsymbol{X}) = 0$ with respect to weight vector $\boldsymbol{w} = (w_1, \dots, w_n) \in \mathbb{Z}^n_{>0}$ and weighted degrees $d_1, \dots, d_n$ has at most

$$\frac{d_1 \cdots d_n}{w_1 \cdots w_n} \text{ isolated solutions.}$$

$$\phi(\boldsymbol{X}) = x_1^2 + x_2^2 + x_3^2 - 3(x_1x_2 + x_1x_3 + x_2x_3)$$

- [Fundamental Theorem of Symmetric Polynomials], there is unique polynomial

$$\bar{\boldsymbol{\phi}} = \boldsymbol{e_1^2} - \boldsymbol{5e_2} \text{ such that } \bar{\phi}(E_1(\boldsymbol{X}), E_2(\boldsymbol{X})) = \phi(\boldsymbol{X}).$$

- $E_k(\boldsymbol{X})$: elementary symmetric polynomial of degree k
- $E_2(\boldsymbol{X}) = x_1x_2 + x_1x_3 + x_2x_3 \rightsquigarrow \deg(E_2(\boldsymbol{X})) = 2$

Why Sparse and Weighted Degree Polynomials?

Weighted Bézout Theorem

A system of n weighted polynomial equations $f_1(\boldsymbol{X}) = 0, \ldots, f_n(\boldsymbol{X}) = 0$ with respect to weight vector $\boldsymbol{w} = (w_1, \ldots, w_n) \in \mathbb{Z}^n_{>0}$ and weighted degrees $d_1, \ldots, d_n$ has at most

$$\frac{d_1 \cdots d_n}{w_1 \cdots w_n} \text{ isolated solutions.}$$

$$\phi(\boldsymbol{X}) = x_1^2 + x_2^2 + x_3^2 - 3(x_1x_2 + x_1x_3 + x_2x_3)$$

- [Fundamental Theorem of Symmetric Polynomials], there is unique polynomial

$$\bar{\boldsymbol{\phi}} = \boldsymbol{e_1^2} - \boldsymbol{5e_2} \text{ such that } \bar{\phi}(E_1(\boldsymbol{X}), E_2(\boldsymbol{X})) = \phi(\boldsymbol{X}).$$

- $E_k(\boldsymbol{X})$: elementary symmetric polynomial of degree k
- $E_2(\boldsymbol{X}) = x_1x_2 + x_1x_3 + x_2x_3 \rightsquigarrow \deg(E_2(\boldsymbol{X})) = 2 \rightsquigarrow$ wdeg$(e_2) = 2$

Why Sparse and Weighted Degree Polynomials?

Weighted Bézout Theorem

A system of n weighted polynomial equations $f_1(\boldsymbol{X}) = 0, \ldots, f_n(\boldsymbol{X}) = 0$ with respect to weight vector $\boldsymbol{w} = (w_1, \ldots, w_n) \in \mathbb{Z}^n_{>0}$ and weighted degrees $d_1, \ldots, d_n$ has at most

$$\frac{d_1 \cdots d_n}{w_1 \cdots w_n} \text{ isolated solutions.}$$

$$\phi(\boldsymbol{X}) = x_1^2 + x_2^2 + x_3^2 - 3(x_1x_2 + x_1x_3 + x_2x_3)$$

- [Fundamental Theorem of Symmetric Polynomials], there is unique polynomial
  $$\bar{\boldsymbol{\phi}} = \boldsymbol{e_1^2} - \boldsymbol{5e_2} \text{ such that } \bar{\phi}(E_1(\boldsymbol{X}), E_2(\boldsymbol{X})) = \phi(\boldsymbol{X}).$$
- $E_k(\boldsymbol{X})$: elementary symmetric polynomial of degree k
- $\deg(E_k(\boldsymbol{X})) = k$

Why Sparse and Weighted Degree Polynomials?

Weighted Bézout Theorem

A system of n weighted polynomial equations $f_1(\boldsymbol{X}) = 0, \ldots, f_n(\boldsymbol{X}) = 0$ with respect to weight vector $\boldsymbol{w} = (w_1, \ldots, w_n) \in \mathbb{Z}^n_{>0}$ and weighted degrees $d_1, \ldots, d_n$ has at most

$$\frac{d_1 \cdots d_n}{w_1 \cdots w_n} \text{ isolated solutions.}$$

$$\phi(\boldsymbol{X}) = x_1^2 + x_2^2 + x_3^2 - 3(x_1x_2 + x_1x_3 + x_2x_3)$$

- [Fundamental Theorem of Symmetric Polynomials], there is unique polynomial

$$\bar{\boldsymbol{\phi}} = \boldsymbol{e_1^2} - \boldsymbol{5e_2} \text{ such that } \bar{\phi}(E_1(\boldsymbol{X}), E_2(\boldsymbol{X})) = \phi(\boldsymbol{X}).$$

- $E_k(\boldsymbol{X})$: elementary symmetric polynomial of degree k
- $\deg(E_k(\boldsymbol{X})) = k \rightsquigarrow \mathsf{wdeg}(e_k) = k$

Why Sparse and Weighted Degree Polynomials?

Weighted Bézout Theorem

A system of n weighted polynomial equations $f_1(\boldsymbol{X}) = 0, \ldots, f_n(\boldsymbol{X}) = 0$ with respect to weight vector $\boldsymbol{w} = (w_1, \ldots, w_n) \in \mathbb{Z}^n_{>0}$ and weighted degrees $d_1, \ldots, d_n$ has at most

$$\frac{d_1 \cdots d_n}{w_1 \cdots w_n} \text{ isolated solutions.}$$

$$\phi(\boldsymbol{X}) = x_1^2 + x_2^2 + x_3^2 - 3(x_1x_2 + x_1x_3 + x_2x_3)$$

- [Fundamental Theorem of Symmetric Polynomials], there is unique polynomial

$$\bar{\boldsymbol{\phi}} = \boldsymbol{e_1^2} - \boldsymbol{5e_2} \text{ such that } \bar{\phi}(E_1(\boldsymbol{X}), E_2(\boldsymbol{X})) = \phi(\boldsymbol{X}).$$

- $E_k(\boldsymbol{X})$: elementary symmetric polynomial of degree k
- $\deg(E_k(\boldsymbol{X})) = k \rightsquigarrow \mathrm{wdeg}(e_k) = k$

$\bar{\phi}$ is also a **sparse** polynomial in $(e_1, e_2, \ldots, e_n)$

Outline

1. Polynomial System Solving

2. Symbolic Homotopy Techniques to Solve Polynomial Systems

3. Solving Rank-constrained Polynomial Systems

4. **Invariant Algebraic Systems**

The Beauty of Symmetry

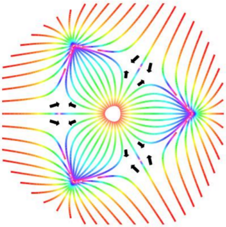
"Symmetry is a vast subject, significant in art and nature. Mathematics lies at its root, and it would be hard to find a better one on which to demonstrate the working of the mathematical intellect." – ***Hermann Weyl***

Equilibria in Dynamical Systems

$\dot{x} = p(x)$ where $p(\tau(g)x) = \tau(g)p(x)$

References:

- Chossat, Lauterbach (2000)
- Gatermann (2001)



Our Very Beginning Motivation, but with Symmetry

Minimize: $\phi(x_1, x_2, x_3) = x_1 x_2 x_3 - 3(x_1 + x_2 + x_3)$ subject to

$$g(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 - 6 = 0.$$

The minima satisfy

$$x_1^2 + x_2^2 + x_3^2 - 6 = 0$$

and

$$\operatorname{rank} \begin{bmatrix} 2x_1 & 2x_2 & 2x_3 \\ x_2 x_3 - 3 & x_1 x_3 - 3 & x_1 x_2 - 3 \end{bmatrix} < 2$$

Our Very Beginning Motivation, but with Symmetry

Minimize: $\phi(x_1, x_2, x_3) = x_1x_2x_3 - 3(x_1 + x_2 + x_3)$ subject to

$$g(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 - 6 = 0.$$

The minima satisfy

$$x_1^2 + x_2^2 + x_3^2 - 6 = 0$$

and

$$\operatorname{rank} \begin{bmatrix} 2x_1 & 2x_2 & 2x_3 \\ x_2x_3 - 3 & x_1x_3 - 3 & x_1x_2 - 3 \end{bmatrix} < 2$$

Observation: ϕ and g are both **symmetric**.

Our Very Beginning Motivation, but with Symmetry

Minimize: $\phi(x_1, x_2, x_3) = x_1x_2x_3 - 3(x_1 + x_2 + x_3)$ subject to

$$g(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 - 6 = 0.$$

The minima satisfy

$$x_1^2 + x_2^2 + x_3^2 - 6 = 0$$

and

$$\operatorname{rank} \begin{bmatrix} 2x_1 & 2x_2 & 2x_3 \\ x_2x_3 - 3 & x_1x_3 - 3 & x_1x_2 - 3 \end{bmatrix} < 2$$

Observation: ϕ and g are both **symmetric**.

Can we take the advantage of symmetry?

Computing Critical Points Problem with Symmetry

Problem

Given:

- symmetric polynomials $\boldsymbol{G} = (g_1, \dots, g_s)$ in $\mathbb{K}[x_1, \dots, x_n]$
- a symmetric polynomial map ϕ in $\mathbb{K}[x_1, \dots, x_n]$

such that the set

$$W(\phi, \boldsymbol{G}) := \{\boldsymbol{x} \in \overline{\mathbb{K}}^n : \boldsymbol{G}(\boldsymbol{x}) = 0 \text{ and } \mathsf{rank}(\mathsf{Jac}(\boldsymbol{G}, \phi)) < s + 1\}$$

is finite.

Compute: the set $W(\phi, \boldsymbol{G})$.

Computing Critical Points Problem with Symmetry

Problem

Given:

- symmetric polynomials $\boldsymbol{G} = (g_1, \dots, g_s)$ in $\mathbb{K}[x_1, \dots, x_n]$
- a symmetric polynomial map ϕ in $\mathbb{K}[x_1, \dots, x_n]$

such that the set

$$W(\phi, \boldsymbol{G}) := \{\boldsymbol{x} \in \overline{\mathbb{K}}^n : \boldsymbol{G}(\boldsymbol{x}) = 0 \text{ and } \mathrm{rank}(\mathrm{Jac}(\boldsymbol{G}, \phi)) < s + 1\}$$

is finite.

Compute: the set $W(\phi, \boldsymbol{G})$.

$$W(\phi, \boldsymbol{G}) = V_{s+1}(\boldsymbol{F}, \boldsymbol{G}), \text{ where } \boldsymbol{F} = \mathrm{Jac}(\boldsymbol{G}, \phi)$$

Computing Critical Points Problem with Symmetry

Problem

Given:

- symmetric polynomials $\boldsymbol{G} = (g_1, \dots, g_s)$ in $\mathbb{K}[x_1, \dots, x_n]$
- a symmetric polynomial map ϕ in $\mathbb{K}[x_1, \dots, x_n]$

such that the set

$$W(\phi, \boldsymbol{G}) := \{\boldsymbol{x} \in \overline{\mathbb{K}}^n : \boldsymbol{G}(\boldsymbol{x}) = 0 \text{ and } \mathrm{rank}(\mathrm{Jac}(\boldsymbol{G}, \phi)) < s + 1\}$$

is finite.

Compute: the set $W(\phi, \boldsymbol{G})$.

$$W(\phi, \boldsymbol{G}) = V_{s+1}(\boldsymbol{F}, \boldsymbol{G}), \text{ where } \boldsymbol{F} = \mathrm{Jac}(\boldsymbol{G}, \phi)$$

Not exploiting the symmetry!

Some Related work

[Labahn-Hubert]

- ◇ scaling invariants and symmetry reduction of dynamical systems

[Busé-Karasoulou]

- ◇ resultant of an equivariant polynomial system

[Faugère-Rahmany]

- ◇ use SAGBI-Gröbner bases to solve symmetric systems

[Faugère-Svartz]

- ◇ globally invariant systems

[Riener, 2012], [Riener-Safey El Din, 2018], [Labahn-Riener-Safey El Din-Schost-**Vu**, 2023], [Riener-Schabert-**Vu**, 2024], [Riener-Schabert-**Vu**, 2026]

- ◇ related questions in real algebraic geometry with symmetric polynomials (deciding the emptiness, real root finding, connectivity)

How Symmetries?

Original Problem

Minimize: $\phi = x_1 x_2 x_3 - 3(x_1 + x_2 + x_3)$
Subject to: $g = x_1^2 + x_2^2 + x_3^2 - 6 = 0$

$$\Downarrow$$

Rewrite in Elementary Symmetric Polynomials

E_k

Invariant Form

Minimize: $\bar{\phi} = e_3 - 3e_1$
Subject to: $\bar{g} = e_1^2 - 2e_2 - 6 = 0$

How Symmetries?

Original Problem

Minimize: $\phi = x_1x_2x_3 - 3(x_1+x_2+x_3)$
Subject to: $g = x_1^2 + x_2^2 + x_3^2 - 6 = 0$

$\Downarrow$

Rewrite in Elementary Symmetric Polynomials E_k

Invariant Form

Minimize: $\bar{\phi} = e_3 - 3e_1$
Subject to: $\bar{g} = e_1^2 - 2e_2 - 6 = 0$

Classical Degrees

$\deg(x_1 + x_2 + x_3) = 1$

$\deg(x_1x_2 + x_1x_3 + x_2x_3) = 2$

$\deg(x_1x_2x_3) = 3$

$\Downarrow$

Assign Degree Weights to e_k

Induced Weighted Degrees

$\text{wdeg}(e_1) = 1$

$\text{wdeg}(e_2) = 2$

$\text{wdeg}(e_3) = 3$

Original Problem

$\boldsymbol{G} = 0$ and $\mathrm{rank}(\mathrm{Jac}(\boldsymbol{G}, \phi)) < s + 1$

$$\Downarrow$$

Rewrite in Elementary Symmetric Polynomials E_k

Invariant Form

$\bar{\boldsymbol{G}} = 0$ and $\mathrm{rank}(\mathrm{Jac}(\bar{\boldsymbol{G}}, \bar{\phi})) < s + 1$

$\bar{\boldsymbol{G}}(E_1(\boldsymbol{X}), \ldots, E_n(\boldsymbol{X})) = \boldsymbol{G}$ and $\bar{\phi}(E_1(\boldsymbol{X}), \ldots, E_n(\boldsymbol{X})) = \phi$

Original Problem

$\boldsymbol{G} = 0$ and $\mathrm{rank}(\mathrm{Jac}(\boldsymbol{G}, \phi)) < s + 1$

$$\Downarrow$$

Rewrite in Elementary Symmetric Polynomials E_k

Invariant Form

$\bar{\boldsymbol{G}} = 0$ and $\mathrm{rank}(\mathrm{Jac}(\bar{\boldsymbol{G}}, \bar{\phi})) < s + 1$

$\bar{\boldsymbol{G}}(E_1(\boldsymbol{X}), \dots, E_n(\boldsymbol{X})) = \boldsymbol{G}$ and $\bar{\phi}(E_1(\boldsymbol{X}), \dots, E_n(\boldsymbol{X})) = \phi$

- By chain rule, $\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{G}, \phi) = \mathrm{Jac}_{\boldsymbol{e}}(\bar{\boldsymbol{G}}, \bar{\phi})(E(\boldsymbol{X})) \times \mathrm{Jac}_{\boldsymbol{X}}(E_1, \dots, E_n)$

Original Problem

$\boldsymbol{G} = 0$ and rank(Jac($\boldsymbol{G}, \phi$)) $< s+1$

$$\Downarrow$$

Rewrite in Elementary Symmetric Polynomials E_k

Invariant Form

$\bar{\boldsymbol{G}} = 0$ and rank(Jac($\bar{\boldsymbol{G}}, \bar{\phi}$)) $< s+1$

$$\bar{\boldsymbol{G}}(E_1(\boldsymbol{X}), \ldots, E_n(\boldsymbol{X})) = \boldsymbol{G} \text{ and } \bar{\phi}(E_1(\boldsymbol{X}), \ldots, E_n(\boldsymbol{X})) = \phi$$

- By chain rule, $\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{G}, \phi) = \mathrm{Jac}_{\boldsymbol{e}}(\bar{\boldsymbol{G}}, \bar{\phi})(E(\boldsymbol{X})) \times \mathrm{Jac}_{\boldsymbol{X}}(E_1, \ldots, E_n)$
- Then

$$\mathrm{rank}(\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{G}, \phi)) = \mathrm{rank}(\mathrm{Jac}_{\boldsymbol{e}}(\bar{\boldsymbol{G}}, \bar{\phi})(E(\boldsymbol{X}))) \iff \mathrm{Jac}_{\boldsymbol{X}}(E) \text{ is } \textbf{nonsingular}$$

Original Problem

$$\boldsymbol{G} = 0 \text{ and } \mathrm{rank}(\mathrm{Jac}(\boldsymbol{G}, \phi)) < s + 1$$

$$\Downarrow$$

Rewrite in Elementary Symmetric Polynomials E_k

Invariant Form

$$\bar{\boldsymbol{G}} = 0 \text{ and } \mathrm{rank}(\mathrm{Jac}(\bar{\boldsymbol{G}}, \bar{\phi})) < s + 1$$

$$\bar{\boldsymbol{G}}(E_1(\boldsymbol{X}), \ldots, E_n(\boldsymbol{X})) = \boldsymbol{G} \text{ and } \bar{\phi}(E_1(\boldsymbol{X}), \ldots, E_n(\boldsymbol{X})) = \phi$$

- By chain rule, $\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{G}, \phi) = \mathrm{Jac}_{\boldsymbol{e}}(\bar{\boldsymbol{G}}, \bar{\phi})(E(\boldsymbol{X})) \times \mathrm{Jac}_{\boldsymbol{X}}(E_1, \ldots, E_n)$
- Then

$$\mathrm{rank}(\mathrm{Jac}_{\boldsymbol{X}}(\boldsymbol{G}, \phi)) = \mathrm{rank}(\mathrm{Jac}_{\boldsymbol{e}}(\bar{\boldsymbol{G}}, \bar{\phi})(E(\boldsymbol{X}))) \iff \mathrm{Jac}_{\boldsymbol{X}}(E) \text{ is } \textbf{nonsingular}$$

which occurs when $x_i \neq x_j \quad \text{for all } 1 \leq i < j \leq n$

Original Problem

$\boldsymbol{G} = 0$ and $\text{rank}(\text{Jac}(\boldsymbol{G}, \phi)) < s + 1$

$\Downarrow$

Rewrite in Elementary Symmetric Polynomials E_k

Invariant Form

$\bar{\boldsymbol{G}} = 0$ and $\text{rank}(\text{Jac}(\bar{\boldsymbol{G}}, \bar{\phi})) < s + 1$

$\bar{\boldsymbol{G}}(E_1(\boldsymbol{X}), \ldots, E_n(\boldsymbol{X})) = \boldsymbol{G}$ and $\bar{\phi}(E_1(\boldsymbol{X}), \ldots, E_n(\boldsymbol{X})) = \phi$

- By chain rule, $\text{Jac}_{\boldsymbol{X}}(\boldsymbol{G}, \phi) = \text{Jac}_{\boldsymbol{e}}(\bar{\boldsymbol{G}}, \bar{\phi})(E(\boldsymbol{X})) \times \text{Jac}_{\boldsymbol{X}}(E_1, \ldots, E_n)$
- Then

$$\text{rank}(\text{Jac}_{\boldsymbol{X}}(\boldsymbol{G}, \phi)) = \text{rank}(\text{Jac}_{\boldsymbol{e}}(\bar{\boldsymbol{G}}, \bar{\phi})(E(\boldsymbol{X}))) \iff \text{Jac}_{\boldsymbol{X}}(E) \text{ is } \textbf{nonsingular}$$

which occurs when $x_i \neq x_j$ for all $1 \leq i < j \leq n$

What happens if some $x_i = x_j$?

Group Orbits: Integer Partitions

A tuple of positive integers $\lambda = (\underbrace{n_1, \ldots, n_1}_{\ell_1}, \ldots, \underbrace{n_r, \ldots, n_r}_{\ell_r})$ is a **partition** of n if $n_1\ell_1 + n_2\ell_2 + \cdots + n_r\ell_r = n$. The value $\ell := \ell_1 + \cdots + \ell_r$ is called the **length** of λ.

Group Orbits: Integer Partitions

A tuple of positive integers $\lambda = (\underbrace{n_1, \dots, n_1}_{\ell_1}, \dots, \underbrace{n_r, \dots, n_r}_{\ell_r})$ is a **partition** of n if $n_1\ell_1 + n_2\ell_2 + \cdots + n_r\ell_r = n$. The value $\ell := \ell_1 + \cdots + \ell_r$ is called the **length** of λ.

Example

Integer: $n = 5$

$n_1 = 1, \quad n_2 = 2$
$\ell_1 = 3, \quad \ell_2 = 1$
$r = 2, \quad \ell = 4$

Partition: $\lambda = (1, 1, 1, 2)$

Corresponding Variables

$(x_1, x_2, x_3, x_4, x_5)$

$\Downarrow x_4 = x_5$

Decompose into $r = 2$ blocks

$(z_{1,1}, z_{1,2}, z_{1,3}, z_{2,1}, z_{2,1})$

Group Orbits: Integer Partitions

A tuple of positive integers $\lambda = (\underbrace{n_1, \dots, n_1}_{\ell_1}, \dots, \underbrace{n_r, \dots, n_r}_{\ell_r})$ is a **partition** of n if $n_1\ell_1 + n_2\ell_2 + \cdots + n_r\ell_r = n$. The value $\ell := \ell_1 + \cdots + \ell_r$ is called the **length** of λ.

Corresponding Variables

$$(x_1, x_2, x_3, x_4, x_5)$$

$$\Downarrow x_4 = x_5$$

Decompose into $r = 2$ blocks

$$(z_{1,1}, z_{1,2}, z_{1,3}, z_{2,1}, z_{2,1})$$

Partition: $\lambda = (1, 1, 1, 2)$

Jacobian Matrix

$$g(\boldsymbol{X}) = x_1x_2x_3x_4x_5$$

$$\Downarrow x_4 = z_{2,1},\ x_5 = z_{2,1}$$

$$x_1 = z_{1,1},\ x_2 = z_{1,2},\ x_3 = z_{1,3}$$

Gradient vector of g has the form:

$$\mathrm{grad}(g) = (f_1, f_2, f_3, f_4, f_4) \in \mathbb{K}[\boldsymbol{Z}]^5$$

Group Orbits: Integer Partitions

A tuple of positive integers $\lambda = (\underbrace{n_1, \dots, n_1}_{\ell_1}, \dots, \underbrace{n_r, \dots, n_r}_{\ell_r})$ is a **partition** of n if $n_1\ell_1 + n_2\ell_2 + \cdots + n_r\ell_r = n$. The value $\ell := \ell_1 + \cdots + \ell_r$ is called the **length** of λ.

Corresponding Variables

$$(x_1, x_2, x_3, x_4, x_5)$$

$$\Downarrow \; x_4 = x_5$$

Decompose into $r = 2$ blocks

$$(z_{1,1}, z_{1,2}, z_{1,3}, z_{2,1}, z_{2,1})$$

Partition: $\lambda = (1, 1, 1, 2)$

Jacobian Matrix

$$g(\boldsymbol{X}) = x_1x_2x_3x_4x_5$$

$$\Downarrow \; x_4 = z_{2,1}, \; x_5 = z_{2,1}$$

$$x_1 = z_{1,1}, \; x_2 = z_{1,2}, \; x_3 = z_{1,3}$$

Gradient vector of g has the form:

$$\mathrm{grad}(g) = (f_1, f_2, f_3, f_4, f_4) \in \mathbb{K}[\boldsymbol{Z}]^5$$

- $\rightsquigarrow$ discard f_4 from $\mathrm{grad}(g)$

Group Orbits: Integer Partitions

A tuple of positive integers $\lambda = (\underbrace{n_1, \dots, n_1}_{\ell_1}, \dots, \underbrace{n_r, \dots, n_r}_{\ell_r})$ is a **partition** of n if

$n_1\ell_1 + n_2\ell_2 + \cdots + n_r\ell_r = n$. The value $\ell := \ell_1 + \cdots + \ell_r$ is called the **length** of λ.

Corresponding Variables

$$(x_1, x_2, x_3, x_4, x_5)$$

$$\Downarrow\ x_4 = x_5$$

Decompose into $r = 2$ blocks

$$(z_{1,1}, z_{1,2}, z_{1,3}, z_{2,1}, z_{2,1})$$

Partition: $\lambda = (1, 1, 1, 2)$

Jacobian Matrix

$$g(\boldsymbol{X}) = x_1x_2x_3x_4x_5$$

$$\Downarrow\ x_4 = z_{2,1},\ x_5 = z_{2,1}$$

$$x_1 = z_{1,1},\ x_2 = z_{1,2},\ x_3 = z_{1,3}$$

Gradient vector of g has the form:

$$\mathrm{grad}(g) = (f_1, f_2, f_3, f_4, f_4) \in \mathbb{K}[\boldsymbol{Z}]^5$$

- ◇ $\rightsquigarrow$ discard f_4 from $\mathrm{grad}(g)$
- ◇ (f_1, f_2, f_3, f_4) is **not invariant** but **S_λ-equivariant**, with $S_\lambda := S_{\ell_1} \times \cdots \times S_{\ell_r}$

From Equivariant to Invariant

Let

- $S_\lambda := S_{\ell_1} \times \cdots \times S_{\ell_r}$ direct product of symmetric groups with $\ell_1 + \cdots + \ell_r = \ell$

A sequence of polys. $\boldsymbol{F} = (f_1, \ldots, f_\ell) \in \mathbb{K}[z_1, \ldots, z_\ell]^\ell$ is called S_λ-**equivariant** if

$$f_{\sigma(i)}(z_1, \ldots, z_\ell) = f_i(z_{\sigma(1)}, \ldots, z_{\sigma(\ell)}) \text{for all } \; i = 1, \ldots, \ell \text{ and } \sigma \in S_\lambda$$

From Equivariant to Invariant

Let

- $S_\lambda := S_{\ell_1} \times \cdots \times S_{\ell_r}$ direct product of symmetric groups with $\ell_1 + \cdots + \ell_r = \ell$

A sequence of polys. $\boldsymbol{F} = (f_1, \ldots, f_\ell) \in \mathbb{K}[z_1, \ldots, z_\ell]^\ell$ is called S_λ-**equivariant** if

$$f_{\sigma(i)}(z_1, \ldots, z_\ell) = f_i(z_{\sigma(1)}, \ldots, z_{\sigma(\ell)}) \text{for all } \; i = 1, \ldots, \ell \text{ and } \sigma \in S_\lambda$$

Example

- $(z_1 z_2, z_2 z_3, z_1 z_3)$ is S_3-equivariant w.r.t (z_1, z_2, z_3)

From Equivariant to Invariant

Let

- $S_\lambda := S_{\ell_1} \times \cdots \times S_{\ell_r}$ direct product of symmetric groups with $\ell_1 + \cdots + \ell_r = \ell$

A sequence of polys. $\boldsymbol{F} = (f_1, \ldots, f_\ell) \in \mathbb{K}[z_1, \ldots, z_\ell]^\ell$ is called S_λ-**equivariant** if

$$f_{\sigma(i)}(z_1, \ldots, z_\ell) = f_i(z_{\sigma(1)}, \ldots, z_{\sigma(\ell)})\text{for all } \; i = 1, \ldots, \ell \text{ and } \sigma \in S_\lambda$$

Example

- (z_1z_2, z_2z_3, z_1z_3) is S_3-equivariant w.r.t (z_1, z_2, z_3)
- $(z_2z_3z_4^2, z_1z_3z_4^2, z_1z_2z_4^2, z_1z_2z_3z_4)$ is $S_3 \times S_1$-equivariant w.r.t (z_1, z_2, z_3) and (z_4)

From Equivariant to Invariant

Let

- ◇ $S_\lambda := S_{\ell_1} \times \cdots \times S_{\ell_r}$ direct product of symmetric groups with $\ell_1 + \cdots + \ell_r = \ell$

A sequence of polys. $\boldsymbol{F} = (f_1, \ldots, f_\ell) \in \mathbb{K}[z_1, \ldots, z_\ell]^\ell$ is called S_λ-**equivariant** if

$$f_{\sigma(i)}(z_1, \ldots, z_\ell) = f_i(z_{\sigma(1)}, \ldots, z_{\sigma(\ell)}) \text{for all } \; i = 1, \ldots, \ell \text{ and } \sigma \in S_\lambda$$

Example

- ◇ $(z_1 z_2, z_2 z_3, z_1 z_3)$ is S_3-equivariant w.r.t (z_1, z_2, z_3)
- ◇ $(z_2 z_3 z_4^2, z_1 z_3 z_4^2, z_1 z_2 z_4^2, z_1 z_2 z_3 z_4)$ is $S_3 \times S_1$-equivariant w.r.t (z_1, z_2, z_3) and (z_4)

Proposision [Faugère-Labahn-Safey El Din-Schost-**Vu**, 2023]

Given S_λ-**equivariant** polynomials $\boldsymbol{F} = (f_1, \ldots, f_\ell)$. There exists an algorithm Symmetrize that returns S_λ-**invariant** polynomials $\boldsymbol{P} = (p_1, \ldots, p_\ell)$ such that $\boldsymbol{F}$ and $\boldsymbol{P}$ generate the same ideal in a suitable localization.

Algorithm: Computing Critical Points

Let $\boldsymbol{G} = (g_1, \ldots, g_s)$ and ϕ be symmetric polynomials in $\mathbb{K}[x_1, \ldots, x_n]$. Suppose the critical point set

$$W(\phi, \boldsymbol{G}) := \left\{ \boldsymbol{x} \in \overline{\mathbb{K}}^n : \boldsymbol{g}(\boldsymbol{x}) = 0 \text{ and } \operatorname{rank}(\operatorname{Jac}(\boldsymbol{G}, \phi)) < s + 1 \right\}$$

is finite.

Theorem [Faugère-Labahn-Safey El Din-Schost-Vu**, 2023]**

The set $W(\phi, \boldsymbol{G})$ contains at most $d^s \binom{n+d-1}{n}$ points and can be computed in time $\left(d^s \binom{n+d}{n} \binom{n}{s+1} \right)^{O(1)}$.

Algorithm: Computing Critical Points

Let $\boldsymbol{G} = (g_1, \dots, g_s)$ and ϕ be symmetric polynomials in $\mathbb{K}[x_1, \dots, x_n]$. Suppose the critical point set

$$W(\phi, \boldsymbol{G}) := \left\{ \boldsymbol{x} \in \overline{\mathbb{K}}^n : \boldsymbol{g}(\boldsymbol{x}) = 0 \text{ and } \operatorname{rank}(\operatorname{Jac}(\boldsymbol{G}, \phi)) < s+1 \right\}$$

is finite.

Theorem [Faugère-Labahn-Safey El Din-Schost-**Vu**, 2023]

The set $W(\phi, \boldsymbol{G})$ contains at most $d^s\binom{n+d-1}{n}$ points and can be computed in time $\left(d^s\binom{n+d}{n}\binom{n}{s+1}\right)^{O(1)}$.

for each partition λ of n

Introduce new variables $\boldsymbol{Z}$ corresponding to partition λ
Form the matrix $\boldsymbol{J}_{\boldsymbol{Z}} \leftarrow \operatorname{Jac}(\boldsymbol{G}, \phi)$ evaluated at $\boldsymbol{Z}$
Eliminate duplicated columns in $\boldsymbol{J}_{\boldsymbol{Z}}$ to obtain a smaller matrix $\boldsymbol{J}$
for each row r of $\boldsymbol{J}$ **do**
    Apply Symmetrize(r) algorithm to row r
end for
Rewrite the entries of $\boldsymbol{J}$ in terms of elementary symmetric polynomials $\boldsymbol{e}$
Solve the reduced system using column homotopies with weighted degrees

Some Final Words

Joint Works:

- **Hauenstein, Safey El Din, Schost, Vu (2021)**
  Solving determinantal systems using homotopy techniques
  Journal of Symbolic Computation

- **Labahn, Safey El Din, Schost, Vu (2021)**
  Homotopy techniques for solving sparse column support determinantal polynomial systems
  Journal of Complexity

- **Faugère, Labahn, Safey El Din, Schost, Vu (2023)**
  Computing Critical Points for Invariant Algebraic Systems
  Journal of Symbolic Computation

Some Final Words

Joint Works:

- **Hauenstein, Safey El Din, Schost, Vu (2021)**
  Solving determinantal systems using homotopy techniques
  Journal of Symbolic Computation
- **Labahn, Safey El Din, Schost, Vu (2021)**
  Homotopy techniques for solving sparse column support determinantal polynomial systems
  Journal of Complexity
- **Faugère, Labahn, Safey El Din, Schost, Vu (2023)**
  Computing Critical Points for Invariant Algebraic Systems
  Journal of Symbolic Computation

Credits: Some pictures in this presentation were inspired by Éric Schost's abstract talk at CASC 2017 (which presented the very initial idea of our 2021 JSC paper).