Fast algorithm and sharp degree bounds for one block quantifier elimination over the reals

Huu Phuoc LE, Mohab SAFEY EL DIN

LIP6, Sorbonne Université

MAX Seminar
May 10, 2021

One block quantifier elimination (QE)

A *basic semi-algebraic* set: the set of real solutions of

$$f_1 = \cdots = f_s = 0,\ g_1 \bullet 0, \ldots,\ g_v \bullet 0,$$

with $\bullet \in \{>, \geq\}$, $f_i, g_j \in \mathbb{R}[x_1, \ldots, x_n]$.

A *semi-algebraic* set is a finite union of basic semi-algebraic sets.

One block quantifier elimination (QE)

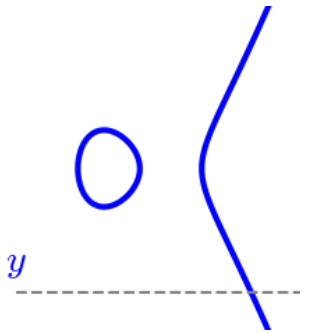
A *basic semi-algebraic* set: the set of real solutions of

$$f_1 = \cdots = f_s = 0,\ g_1 \bullet 0, \ldots,\ g_v \bullet 0,$$

with $\bullet \in \{>, \geq\}$, $f_i, g_j \in \mathbb{R}[x_1, \ldots, x_n]$.

A *semi-algebraic* set is a finite union of basic semi-algebraic sets.

$$\{(x, y) \in \mathbb{R}^2 \mid x^2 = y^3 - y\}$$



One block quantifier elimination (QE)

A *basic semi-algebraic* set: the set of real solutions of

$$f_1 = \cdots = f_s = 0,\ g_1 \bullet 0, \ldots,\ g_v \bullet 0,$$

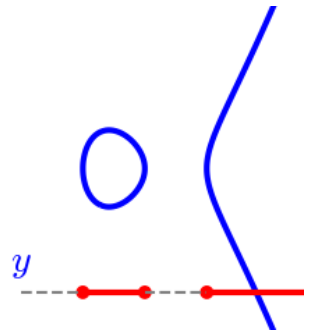
with $\bullet \in \{>, \geq\}$, $f_i, g_j \in \mathbb{R}[x_1, \ldots, x_n]$.

A *semi-algebraic* set is a finite union of basic semi-algebraic sets.

$$\{(x, y) \in \mathbb{R}^2 \mid x^2 = y^3 - y\}$$

Projection on the y-axis:

$$(\exists x : x^2 = y^3 - y) \ \Leftrightarrow\ (y^3 - y \geq 0)$$



One block quantifier elimination (QE)

A *basic semi-algebraic* set: the set of real solutions of

$$f_1 = \cdots = f_s = 0,\ g_1 \bullet 0, \ldots,\ g_v \bullet 0,$$

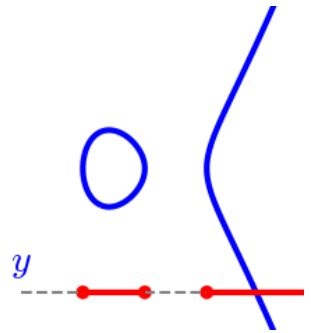
with $\bullet \in \{>, \geq\}$, $f_i, g_j \in \mathbb{R}[x_1, \ldots, x_n]$.

A *semi-algebraic* set is a finite union of basic semi-algebraic sets.

$$\{(x, y) \in \mathbb{R}^2 \mid x^2 = y^3 - y\}$$

Projection on the y-axis:

$$(\exists x : x^2 = y^3 - y) \ \Leftrightarrow\ (y^3 - y \geq 0)$$



Tarski's theorem (1951)

The projection of a semi-algebraic set is a semi-algebraic set.

One block quantifier elimination (QE)

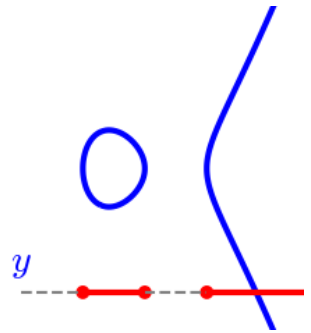
A *basic semi-algebraic* set: the set of real solutions of

$$f_1 = \cdots = f_s = 0,\ g_1 \bullet 0, \ldots,\ g_v \bullet 0,$$

with $\bullet \in \{>, \geq\}$, $f_i, g_j \in \mathbb{R}[x_1, \ldots, x_n]$.

A *semi-algebraic* set is a finite union of basic semi-algebraic sets.

$$\{(x, y) \in \mathbb{R}^2 \mid x^2 = y^3 - y\}$$



Projection on the y-axis:

$$(\exists x : x^2 = y^3 - y) \ \Leftrightarrow\ (y^3 - y \geq 0)$$

Tarski's theorem (1951)

The projection of a semi-algebraic set is a semi-algebraic set.

One block QE: $\underbrace{\exists\, \boldsymbol{x}\ :\ \Psi(\boldsymbol{x}, \boldsymbol{y}) \text{ is true}}_{\text{quantified}}$

One block quantifier elimination (QE)

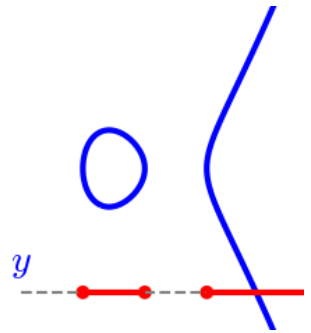
A *basic semi-algebraic* set: the set of real solutions of

$$f_1 = \cdots = f_s = 0,\ g_1 \bullet 0, \ldots,\ g_v \bullet 0,$$

with $\bullet \in \{>, \geq\}$, $f_i, g_j \in \mathbb{R}[x_1, \ldots, x_n]$.

A *semi-algebraic* set is a finite union of basic semi-algebraic sets.

$$\{(x, y) \in \mathbb{R}^2 \mid x^2 = y^3 - y\}$$



Projection on the y-axis:

$$(\exists x : x^2 = y^3 - y) \ \Leftrightarrow\ (y^3 - y \geq 0)$$

Tarski's theorem (1951)

The projection of a semi-algebraic set is a semi-algebraic set.

One block QE: $\underbrace{\exists\, \boldsymbol{x}\ :\ \Psi(\boldsymbol{x}, \boldsymbol{y}) \text{ is true}}_{\text{quantified}} \ \Leftrightarrow\ \underbrace{\Phi(\boldsymbol{y}) \text{ is true}}_{\text{quantifier-free}}$

One block quantifier elimination (QE)

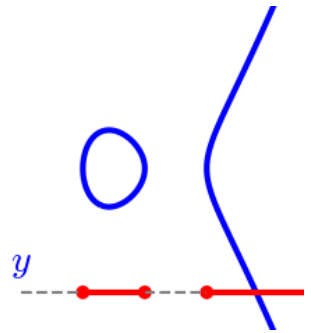
A *basic semi-algebraic* set: the set of real solutions of

$$f_1 = \cdots = f_s = 0,\ g_1 \bullet 0, \ldots,\ g_v \bullet 0,$$

with $\bullet \in \{>, \geq\}$, $f_i, g_j \in \mathbb{R}[x_1, \ldots, x_n]$.

A *semi-algebraic* set is a finite union of basic semi-algebraic sets.

$$\{(x, y) \in \mathbb{R}^2 \mid x^2 = y^3 - y\}$$



Projection on the y-axis:

$$(\exists x : x^2 = y^3 - y) \ \Leftrightarrow\ (y^3 - y \geq 0)$$

Tarski's theorem (1951)

The projection of a semi-algebraic set is a semi-algebraic set.

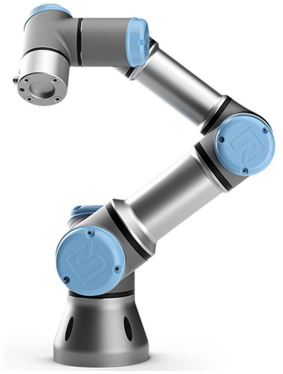
One block QE: $\underbrace{\exists\, \boldsymbol{x}\ :\ \Psi(\boldsymbol{x}, \boldsymbol{y}) \text{ is true}}_{\text{quantified}} \ \Leftrightarrow\ \underbrace{\Phi(\boldsymbol{y}) \text{ is true}}_{\text{quantifier-free}}$

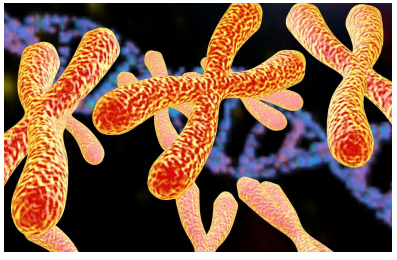
Algorithms, Complexity, Implementation

Motivations

Many applications

- Perspective-Three-Point Problem
  [Faugère, Moroz, Rouillier, Safey El Din '08]
- Kuramoto model of synchronization
  [Kuramoto '75; Harris, Hauenstein, Szanto '20]
- Dynamic of epidemics
  [Chauvin, Müller, Weber '94]
- Program verification [Kapur '06]
- Economics [Mulligan, Davenport, England '18]





Motivations

Many applications

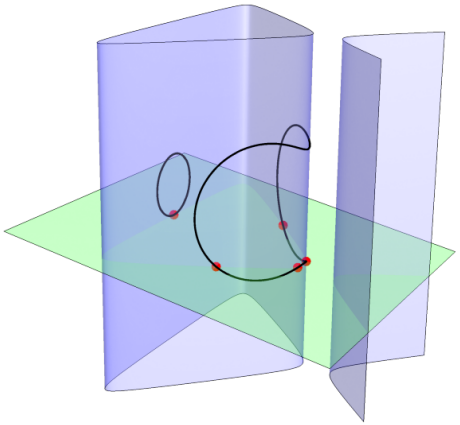
- Perspective-Three-Point Problem
  [Faugère, Moroz, Rouillier, Safey El Din '08]
- Kuramoto model of synchronization
  [Kuramoto '75; Harris, Hauenstein, Szanto '20]
- Dynamic of epidemics
  [Chauvin, Müller, Weber '94]
- Program verification [Kapur '06]
- Economics [Mulligan, Davenport, England '18]

Experimental mathematics

Counter-examples for a conjecture in [Huisman '03]

⇝ Compute a hyperplane that intersects a smooth curve at only real points.

(on-going work with Plaumann, Manevich and Safey El Din)



State-of-the-art

$\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{y} = (y_1, \ldots, y_t)$ and s polynomials of degree bounded by D

State-of-the-art

$\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{y} = (y_1, \ldots, y_t)$ and s polynomials of degree bounded by D

- [Tarski '51]: **Decidable** but not bounded by any finite tower of exponents.

State-of-the-art

$\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{y} = (y_1, \ldots, y_t)$ and s polynomials of degree bounded by D

- [Tarski '51]: **Decidable** but not bounded by any finite tower of exponents.

- CAD [Collins '76] and variants: [Arnon, Collins, McCallum '84; McCallum '88, '99; Hong '90; Collins, Hong '91; Brown '01;...]
  Doubly exponential in the number of variables.

$$(sD)^{2^{O(n+t)}}$$

State-of-the-art

$\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{y} = (y_1, \ldots, y_t)$ and s polynomials of degree bounded by D

- [Tarski '51]: **Decidable** but not bounded by any finite tower of exponents.
- CAD [Collins '76] and variants: [Arnon, Collins, McCallum '84; McCallum '88, '99; Hong '90; Collins, Hong '91; Brown '01;...]
  Doubly exponential in the number of variables.

$$(sD)^{2^{O(n+t)}}$$

- Algorithms exploiting the block structure of variables:
  [Grigoryev '88; Heintz, Roy, Solernó '90; Renegar '92; Basu, Pollack, Roy '96]
  Doubly exponential in the **number of blocks**.

State-of-the-art

$\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{y} = (y_1, \ldots, y_t)$ and s polynomials of degree bounded by D

- [Tarski '51]: **Decidable** but not bounded by any finite tower of exponents.

- CAD [Collins '76] and variants: [Arnon, Collins, McCallum '84; McCallum '88, '99; Hong '90; Collins, Hong '91; Brown '01;...]
  Doubly exponential in the number of variables.

$$(sD)^{2^{O(n+t)}}$$

- Algorithms exploiting the block structure of variables:
  [Grigoryev '88; Heintz, Roy, Solernó '90; Renegar '92; Basu, Pollack, Roy '96]
  Doubly exponential in the **number of blocks**.

  One-block: **singly exponential**

$$s^{n+1}D^{O(nt)}$$

State-of-the-art

$\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{y} = (y_1, \ldots, y_t)$ and s polynomials of degree bounded by D

- [Tarski '51]: **Decidable** but not bounded by any finite tower of exponents.

- CAD [Collins '76] and variants: [Arnon, Collins, McCallum '84; McCallum '88, '99; Hong '90; Collins, Hong '91; Brown '01;...]
  Doubly exponential in the number of variables.

$$(sD)^{2^{O(n+t)}}$$

- Algorithms exploiting the block structure of variables:
  [Grigoryev '88; Heintz, Roy, Solernó '90; Renegar '92; Basu, Pollack, Roy '96]
  Doubly exponential in the **number of blocks**.

One-block: **singly exponential** **(hidden constant in the exponent)**

$$s^{n+1}D^{O(nt)}$$

$\longrightarrow$ Difficult to obtain efficient implementation

State-of-the-art

$\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{y} = (y_1, \ldots, y_t)$ and s polynomials of degree bounded by D

- [Tarski '51]: **Decidable** but not bounded by any finite tower of exponents.

- CAD [Collins '76] and variants: [Arnon, Collins, McCallum '84; McCallum '88, '99; Hong '90; Collins, Hong '91; Brown '01;...]
  Doubly exponential in the number of variables.

$$(sD)^{2^{O(n+t)}}$$

- Algorithms exploiting the block structure of variables:
  [Grigoryev '88; Heintz, Roy, Solernó '90; Renegar '92; Basu, Pollack, Roy '96]
  Doubly exponential in the **number of blocks**.

  One-block: **singly exponential** **(hidden constant in the exponent)**

$$s^{n+1}D^{O(nt)}$$

  $\longrightarrow$ Difficult to obtain efficient implementation

- A variant of QE [Hong, Safey El Din '09, '12]
  Hypotheses: radicality, smoothness, **properness**.
  Output an **almost equivalent** formula.

Practical algorithm.
No complexity analysis.

State-of-the-art

$\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{y} = (y_1, \ldots, y_t)$ and s polynomials of degree bounded by D

- [Tarski '51]: **Decidable** but not bounded by any finite tower of exponents.

- CAD [Collins '76] and variants: [Arnon, Collins, McCallum '84; McCallum '88, '99; Hong '90; Collins, Hong '91; Brown '01;...]
  Doubly exponential in the number of variables.

$$(sD)^{2^{O(n+t)}}$$

- Algorithms exploiting the block structure of variables:
  [Grigoryev '88; Heintz, Roy, Solernó '90; Renegar '92; Basu, Pollack, Roy '96]
  Doubly exponential in the **number of blocks**.

  One-block: **singly exponential** **(hidden constant in the exponent)**

$$s^{n+1}D^{O(nt)}$$

  $\longrightarrow$ Difficult to obtain efficient implementation

- A variant of QE [Hong, Safey El Din '09, '12]
  Hypotheses: radicality, smoothness, **properness**.
  Output an **almost equivalent** formula.

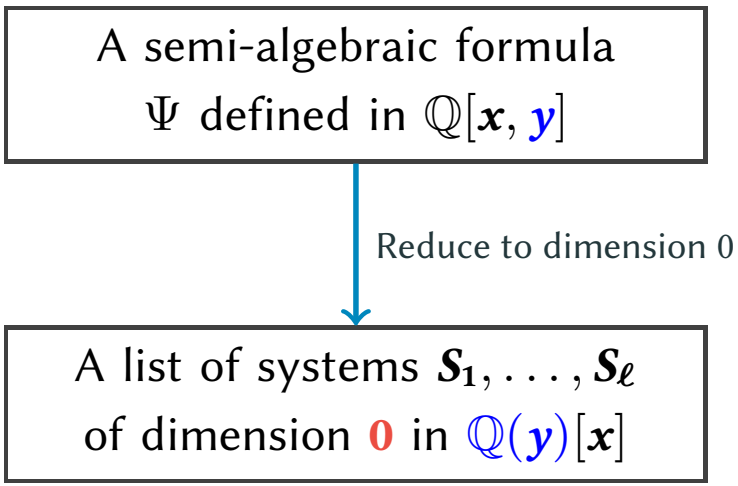
Practical algorithm.
No complexity analysis.

We need a practical algorithm and better complexity analysis!

Outline of the critical method for one block QE

A semi-algebraic formula
Ψ defined in $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$

Outline of the critical method for one block QE



Outline of the critical method for one block QE

A semi-algebraic formula
Ψ defined in $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$

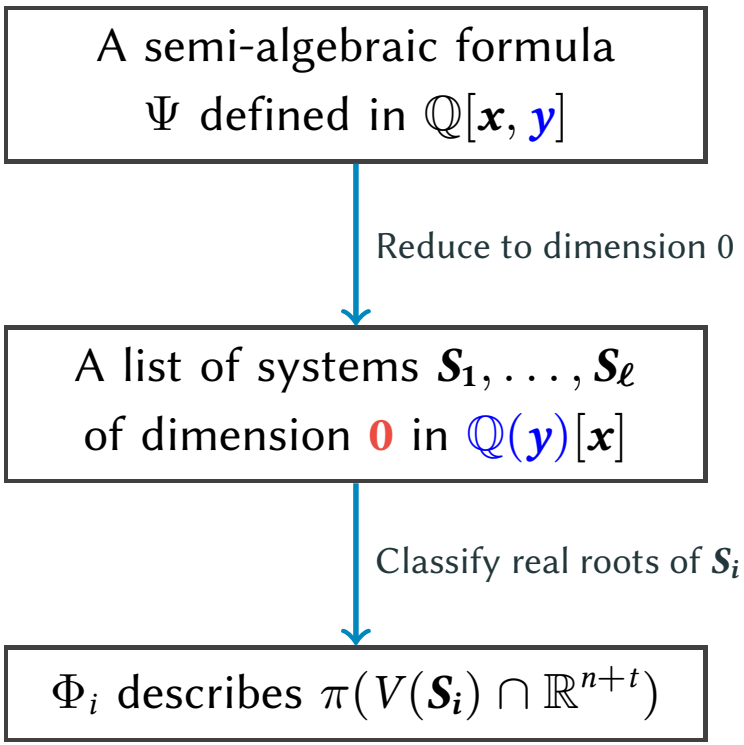
Reduce to dimension 0

A list of systems $\boldsymbol{S_1}, \ldots, \boldsymbol{S_\ell}$
of dimension **0** in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$

For almost every $\eta \in \mathbb{C}^t$:

- The sets of complex solutions of $\boldsymbol{S_i}(\boldsymbol{x}, \eta)$ are finite.
- If $\eta \in \mathbb{R}^t$, the union of solutions intersects every connected component of $\{\boldsymbol{x} \in \mathbb{R}^n \mid \Psi(\boldsymbol{x}, \eta) \text{ is true}\}$.

Outline of the critical method for one block QE



For almost every $\eta \in \mathbb{C}^t$:

- The sets of complex solutions of $\boldsymbol{S_i}(\boldsymbol{x}, \eta)$ are finite.
- If $\eta \in \mathbb{R}^t$, the union of solutions intersects every connected component of $\{\boldsymbol{x} \in \mathbb{R}^n \mid \Psi(\boldsymbol{x}, \eta) \text{ is true}\}$.

Outline of the critical method for one block QE

A semi-algebraic formula
Ψ defined in $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$

↓ Reduce to dimension 0

A list of systems $\boldsymbol{S_1}, \ldots, \boldsymbol{S_\ell}$
of dimension **0** in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$

↓ Classify real roots of $\boldsymbol{S_i}$

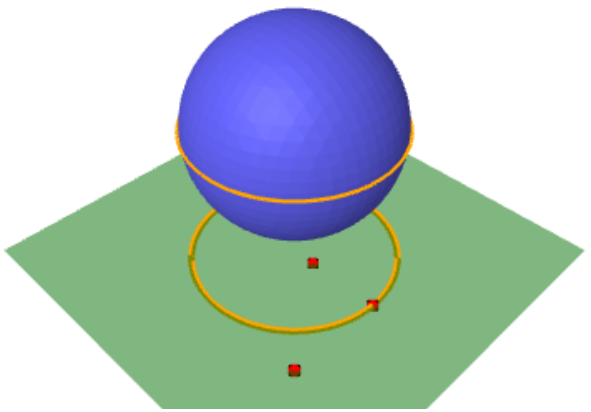
Φ_i describes $\pi(V(\boldsymbol{S_i}) \cap \mathbb{R}^{n+t})$

For almost every $\eta \in \mathbb{C}^t$:

- The sets of complex solutions of $\boldsymbol{S_i}(\boldsymbol{x}, \eta)$ are finite.
- If $\eta \in \mathbb{R}^t$, the union of solutions intersects every connected component of $\{\boldsymbol{x} \in \mathbb{R}^n \mid \Psi(\boldsymbol{x}, \eta) \text{ is true}\}$.

$$x^2 + {y_1}^2 + {y_2}^2 = 1$$

$$\Rightarrow \begin{cases} {y_1}^2 + {y_2}^2 < 1 & : \text{ 2 solutions} \\ {y_1}^2 + {y_2}^2 > 1 & : \text{ 0 solution} \\ {y_1}^2 + {y_2}^2 = 1 & : \text{ 1 solution} \end{cases}$$



Outline of the critical method for one block QE

A semi-algebraic formula
Ψ defined in $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$

↓ Reduce to dimension 0

A list of systems $\boldsymbol{S_1}, \ldots, \boldsymbol{S_\ell}$
of dimension **0** in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$

↓ Classify real roots of $\boldsymbol{S_i}$

Φ_i describes $\pi(V(\boldsymbol{S_i}) \cap \mathbb{R}^{n+t})$

↓

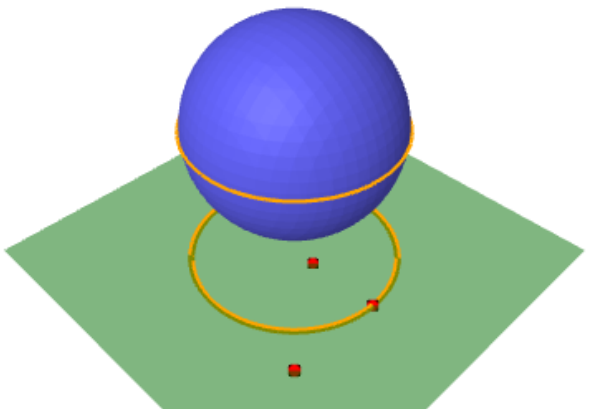
Return $\Phi = \vee_{i=1}^{\ell} \Phi_i$

For almost every $\eta \in \mathbb{C}^t$:

- The sets of complex solutions of $\boldsymbol{S_i}(\boldsymbol{x}, \eta)$ are finite.
- If $\eta \in \mathbb{R}^t$, the union of solutions intersects every connected component of $\{\boldsymbol{x} \in \mathbb{R}^n \mid \Psi(\boldsymbol{x}, \eta) \text{ is true}\}$.

$$x^2 + {y_1}^2 + {y_2}^2 = 1$$

$$\Rightarrow \begin{cases} {y_1}^2 + {y_2}^2 < 1 & : \text{ 2 solutions} \\ {y_1}^2 + {y_2}^2 > 1 & : \text{ 0 solution} \\ {y_1}^2 + {y_2}^2 = 1 & : \text{ 1 solution} \end{cases}$$



Description of Input-Output

Let $\boldsymbol{f} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$

$\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{y} = (y_1, \ldots, y_t)$

$\mathcal{V} = \{(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{C}^{n+t} \mid f_1 = \ldots = f_s = 0\}$

$\pi : (\boldsymbol{x}, \boldsymbol{y}) \mapsto \boldsymbol{y}$

Description of Input-Output

Let $\boldsymbol{f} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ $\quad \boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_t)$

$\mathcal{V} = \{(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{C}^{n+t} \mid f_1 = \ldots = f_s = 0\}$ $\quad \pi : (\boldsymbol{x}, \boldsymbol{y}) \mapsto \boldsymbol{y}$

Regularity assumptions

- $\boldsymbol{f}$ generates a radical ideal in $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$
- $\mathcal{V}$ is smooth and equi-dimensional
- $\pi(\mathcal{V} \cap \mathbb{R}^{n+t})$ has non-zero measure in $\mathbb{R}^t$

Description of Input-Output

Let $\boldsymbol{f} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ $\quad$ $\boldsymbol{x} = (x_1, \ldots, x_n)$, $\boldsymbol{y} = (y_1, \ldots, y_t)$

$\mathcal{V} = \{(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{C}^{n+t} \mid f_1 = \ldots = f_s = 0\}$ $\quad$ $\pi : (\boldsymbol{x}, \boldsymbol{y}) \mapsto \boldsymbol{y}$

Regularity assumptions

- $\boldsymbol{f}$ generates a radical ideal in $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$
- $\mathcal{V}$ is smooth and equi-dimensional
- $\pi(\mathcal{V} \cap \mathbb{R}^{n+t})$ has non-zero measure in $\mathbb{R}^t$

Our main problem $\longrightarrow$ Weaker variant of one block QE

Compute a semi-algebraic formula defining a **dense** subset
in the **interior** of $\pi(\mathcal{V} \cap \mathbb{R}^{n+t})$

Description of Input-Output

Let $\boldsymbol{f} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ $\quad \boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_t)$

$\mathcal{V} = \{(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{C}^{n+t} \mid f_1 = \ldots = f_s = 0\}$ $\quad \pi : (\boldsymbol{x}, \boldsymbol{y}) \mapsto \boldsymbol{y}$

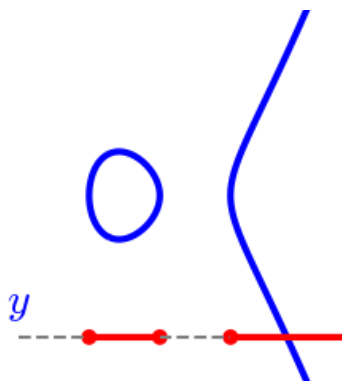
Regularity assumptions

- $\boldsymbol{f}$ generates a radical ideal in $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$
- $\mathcal{V}$ is smooth and equi-dimensional
- $\pi(\mathcal{V} \cap \mathbb{R}^{n+t})$ has non-zero measure in $\mathbb{R}^t$

Our main problem $\longrightarrow$ Weaker variant of one block QE

Compute a semi-algebraic formula defining a **dense** subset
in the **interior** of $\pi(\mathcal{V} \cap \mathbb{R}^{n+t})$

$$(\exists\, x : x^2 = y^3 - y) \;\Leftrightarrow\; (y^3 - y \geq 0)$$



Description of Input-Output

Let $\boldsymbol{f} = \{f_1, \ldots, f_s\} \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ $\quad \boldsymbol{x} = (x_1, \ldots, x_n), \boldsymbol{y} = (y_1, \ldots, y_t)$

$\mathcal{V} = \{(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{C}^{n+t} \mid f_1 = \ldots = f_s = 0\}$ $\quad \pi : (\boldsymbol{x}, \boldsymbol{y}) \mapsto \boldsymbol{y}$

Regularity assumptions

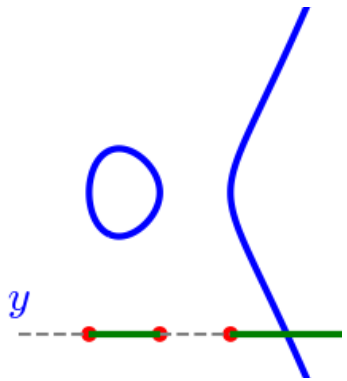
- $\boldsymbol{f}$ generates a radical ideal in $\mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$
- $\mathcal{V}$ is smooth and equi-dimensional
- $\pi(\mathcal{V} \cap \mathbb{R}^{n+t})$ has non-zero measure in $\mathbb{R}^t$

Our main problem $\longrightarrow$ Weaker variant of one block QE

Compute a semi-algebraic formula defining a **dense** subset
in the **interior** of $\pi(\mathcal{V} \cap \mathbb{R}^{n+t})$

$$(\exists\, x : x^2 = y^3 - y) \;\Leftrightarrow\; (y^3 - y \geq 0)$$

Weaker output: $(y^3 - y > 0)$
(*almost* equivalent)



Main results

New algorithm for our variant of one block QE

- In: f satisfies *regularity assumptions*
- Out: A formula Φ defining a *dense* subset of the *interior* of $\pi(\mathcal{V} \cap \mathbb{R}^{n+t})$

Solve examples that are out of reach of the state-of-the-art software.

Main results

New algorithm for our variant of one block QE

- In: f satisfies *regularity assumptions*
- Out: A formula Φ defining a *dense* subset of the *interior* of $\pi(\mathcal{V} \cap \mathbb{R}^{n+t})$

Solve examples that are out of reach of the state-of-the-art software.

t	n	s	NEW QE	MAPLE	MATHEMATICA
2	3	2	**7 s**	$>$ 120 h	$>$ 120 h
2	4	2	**2 m**	$>$ 120 h	$>$ 120 h
2	5	2	**20 m**	$>$ 120 h	$>$ 120 h
2	6	2	**3 h**	$>$ 120 h	$>$ 120 h
2	7	2	**8 h**	$>$ 120 h	$>$ 120 h
3	3	2	**2 m**	$>$ 120 h	$>$ 120 h
3	4	2	**25 m**	$>$ 120 h	$>$ 120 h
3	5	2	**10 h**	$>$ 120 h	$>$ 120 h
4	3	2	**30 m**	$>$ 120 h	$>$ 120 h

Random dense systems with $D = 2$

Main results

New algorithm for our variant of one block QE

- In: f satisfies *regularity assumptions*
- Out: A formula Φ defining a *dense* subset of the *interior* of $\pi(\mathcal{V} \cap \mathbb{R}^{n+t})$

Solve examples that are out of reach of the state-of-the-art software.

t	n	s	NEW QE	MAPLE	MATHEMATICA
2	3	2	**7 s**	$>$ 120 h	$>$ 120 h
2	4	2	**2 m**	$>$ 120 h	$>$ 120 h
2	5	2	**20 m**	$>$ 120 h	$>$ 120 h
2	6	2	**3 h**	$>$ 120 h	$>$ 120 h
2	7	2	**8 h**	$>$ 120 h	$>$ 120 h
3	3	2	**2 m**	$>$ 120 h	$>$ 120 h
3	4	2	**25 m**	$>$ 120 h	$>$ 120 h
3	5	2	**10 h**	$>$ 120 h	$>$ 120 h
4	3	2	**30 m**	$>$ 120 h	$>$ 120 h

Random dense systems with $D = 2$

New algorithm for real root classification

- Construct a matrix $\boldsymbol{H}$ with entries in $\mathbb{Q}(\boldsymbol{y})$.
- Get semi-algebraic formulas as minors of $\boldsymbol{H}$.
- Evaluate the formulas using $\boldsymbol{H}$ (fast).

Main results

New algorithm for our variant of one block QE

- In: f satisfies *regularity assumptions*
- Out: A formula Φ defining a *dense* subset of the *interior* of $\pi(\mathcal{V} \cap \mathbb{R}^{n+t})$

Solve examples that are out of reach of the state-of-the-art software.

t	n	s	NEW QE	MAPLE	MATHEMATICA
2	3	2	**7 s**	$>$ 120 h	$>$ 120 h
2	4	2	**2 m**	$>$ 120 h	$>$ 120 h
2	5	2	**20 m**	$>$ 120 h	$>$ 120 h
2	6	2	**3 h**	$>$ 120 h	$>$ 120 h
2	7	2	**8 h**	$>$ 120 h	$>$ 120 h
3	3	2	**2 m**	$>$ 120 h	$>$ 120 h
3	4	2	**25 m**	$>$ 120 h	$>$ 120 h
3	5	2	**10 h**	$>$ 120 h	$>$ 120 h
4	3	2	**30 m**	$>$ 120 h	$>$ 120 h

Random dense systems with $D = 2$

New algorithm for real root classification

- Construct a matrix $\boldsymbol{H}$ with entries in $\mathbb{Q}(\boldsymbol{y})$.
- Get semi-algebraic formulas as minors of $\boldsymbol{H}$.
- Evaluate the formulas using $\boldsymbol{H}$ (fast).

t	D	NEW RRC	MAPLE[RF]	MAPLE[RC]
2	[3, 2]	**5 s**	1 m	12 s
2	[2, 2, 2]	**34 s**	17m	2 m
2	[3, 3]	**3 m**	2 h	5 m
3	[2, 2]	**27 s**	36 s	12 m
3	[3, 2]	**3 h**	86 h	37 h
3	[2, 2, 2]	**32 h**	$>$ 120 h	$>$ 120 h
3	[4, 2]	**90 h**	$>$ 120 h	$>$ 120 h
4	[2, 2]	**8 m**	$>$ 120 h	$>$ 120 h

Random dense systems

RF: RootFinding RC: RegularChains

Complexity results

Generic input $f = (f_1, \ldots, f_s) \subset \mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_t]$ with $\deg(f_i) \leq D$

Complexity results

Generic input $f = (f_1, \ldots, f_s) \subset \mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_t]$ with $\deg(f_i) \leq D$

Degree bound of polynomials in the output Φ

$$\mathfrak{B} = 2nD^s(D-1)^{n-s+1}\binom{n}{s-1} \qquad \in O\left(nD^n\binom{n}{s-1}\right)$$

Complexity results

Generic input $f = (f_1, \ldots, f_s) \subset \mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_t]$ with $\deg(f_i) \leq D$

Degree bound of polynomials in the output Φ

$$\mathfrak{B} = 2nD^s(D-1)^{n-s+1}\binom{n}{s-1} \qquad \in O\left(nD^n\binom{n}{s-1}\right)$$

Arithmetic complexity for one block QE

$$O^{\sim}\left(8^t\,\mathfrak{B}^{3t}\binom{t+\mathfrak{B}}{t}\right)$$

Complexity results

Generic input $f = (f_1, \ldots, f_s) \subset \mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_t]$ with $\deg(f_i) \leq D$

Degree bound of polynomials in the output Φ

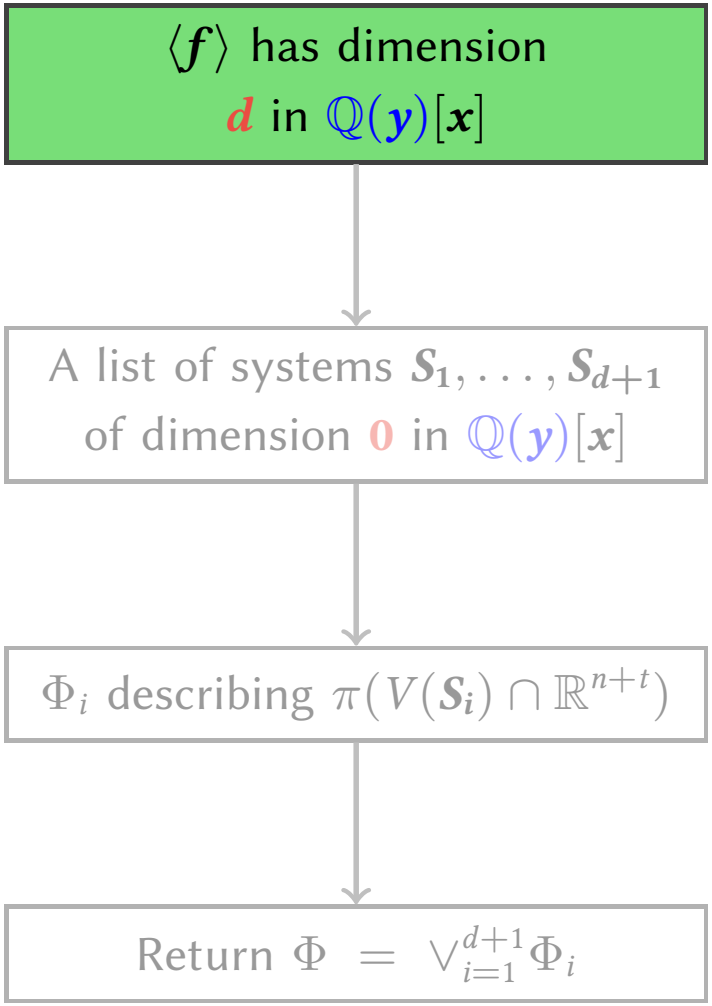
$$\mathfrak{B} = 2nD^s(D-1)^{n-s+1}\binom{n}{s-1} \qquad \in O\left(nD^n\binom{n}{s-1}\right)$$

Arithmetic complexity for one block QE

$$O^{\sim}\left(8^t\,\mathfrak{B}^{3t}\binom{t+\mathfrak{B}}{t}\right)$$

- Explicit constant in the exponent
- For $D = 2$ and s is fixed: $\mathfrak{B}$ is polynomial in n

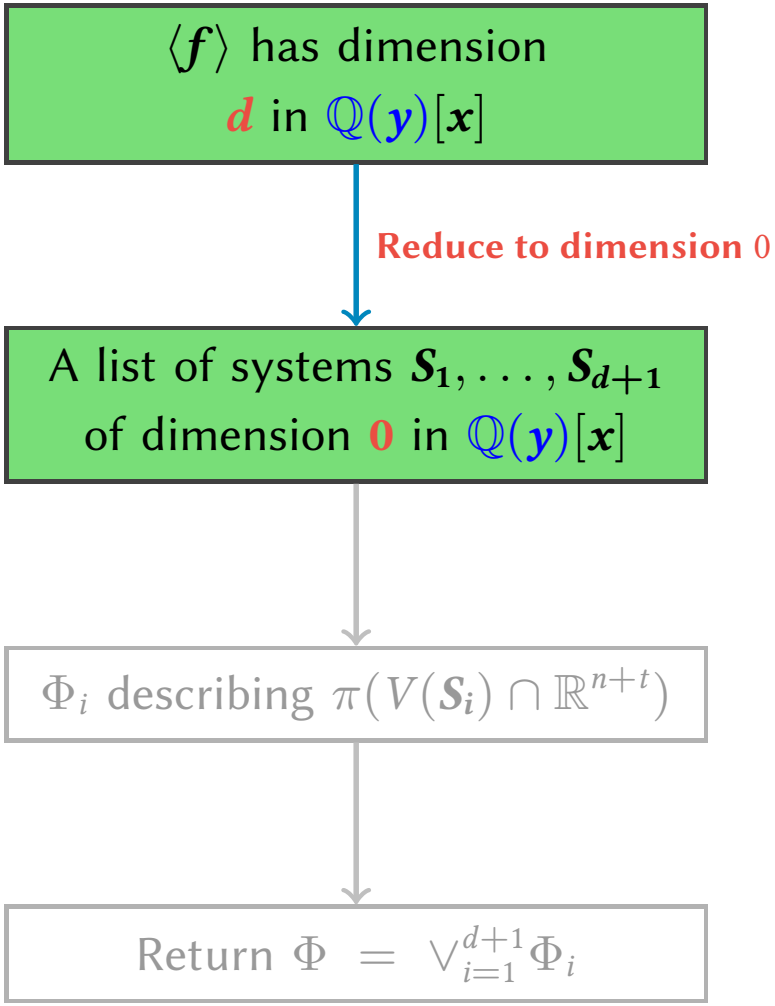
First step: Reduction to dimension zero



Input: $f \subset \mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_t]$

- f generates a radical ideal in $\mathbb{Q}[x, y]$
- $\mathcal{V}$ is smooth and equi-dimensional
- $\pi(\mathcal{V} \cap \mathbb{R}^{n+t})$ has non-zero measure in $\mathbb{R}^t$

First step: Reduction to dimension zero



Input: $f \subset \mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_t]$

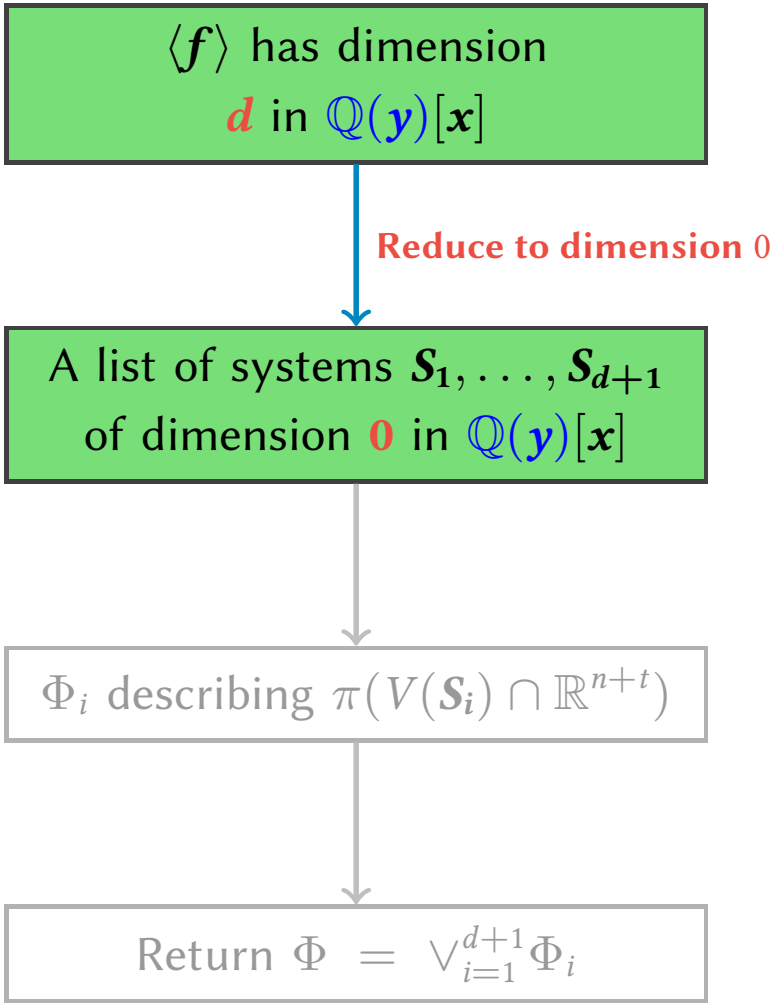
- f generates a radical ideal in $\mathbb{Q}[x, y]$
- $\mathcal{V}$ is smooth and equi-dimensional
- $\pi(\mathcal{V} \cap \mathbb{R}^{n+t})$ has non-zero measure in $\mathbb{R}^t$

Output: $S_1, \ldots, S_{d+1} \subset \mathbb{Q}[x, y]$

For almost every $\eta \in \mathbb{C}^t$:

- The sets of complex solutions of $S_i(x, \eta)$ are finite.
- If $\eta \in \mathbb{R}^t$, their union intersects every component of $V(f(x, \eta)) \cap \mathbb{R}^n$.

First step: Reduction to dimension zero



Input: $f \subset \mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_t]$

- f generates a radical ideal in $\mathbb{Q}[x, y]$
- $\mathcal{V}$ is smooth and equi-dimensional
- $\pi(\mathcal{V} \cap \mathbb{R}^{n+t})$ has non-zero measure in $\mathbb{R}^t$

Output: $S_1, \ldots, S_{d+1} \subset \mathbb{Q}[x, y]$

For almost every $\eta \in \mathbb{C}^t$:

- The sets of complex solutions of $S_i(x, \eta)$ are finite.
- If $\eta \in \mathbb{R}^t$, their union intersects every component of $V(f(x, \eta)) \cap \mathbb{R}^n$.

Real root finding algorithm

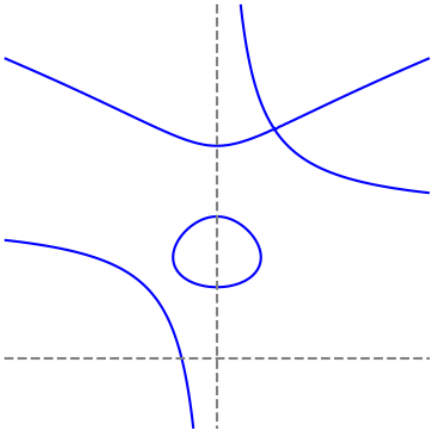
[Safey El Din - Schost '03]

Safey El Din - Schost algorithm

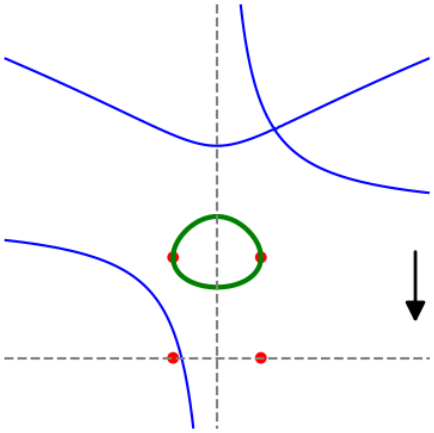
Compute points per connected components

Safey El Din - Schost algorithm

Compute points per connected components

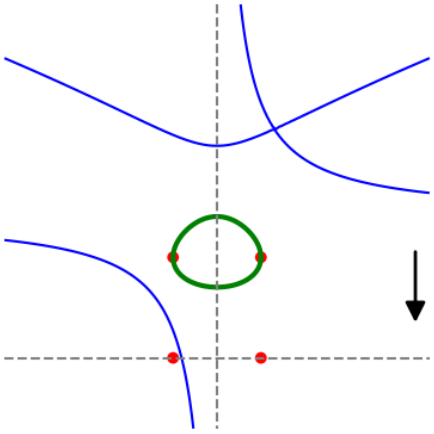


Compute points per connected components

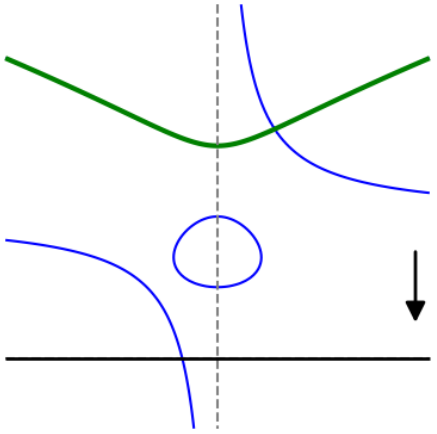


Bounded components

Compute points per connected components

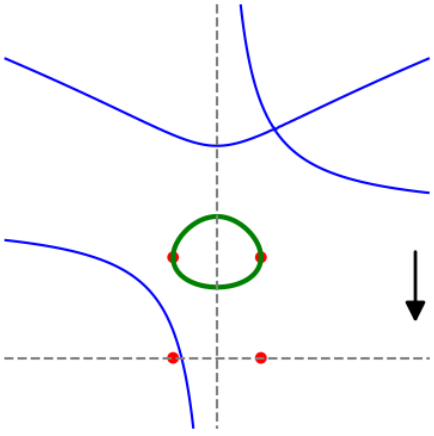


Bounded components

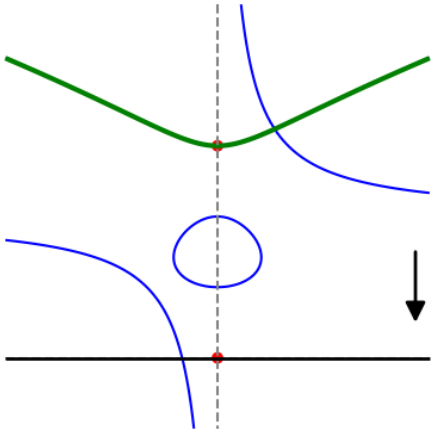


Unbounded components

Compute points per connected components

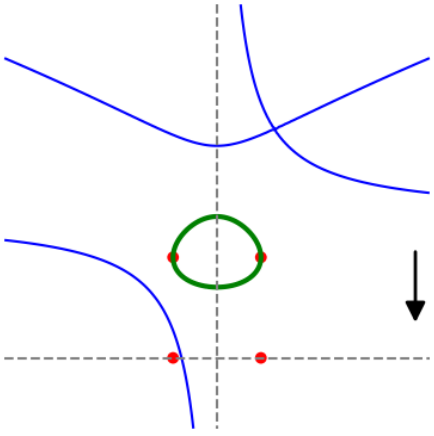


Bounded components

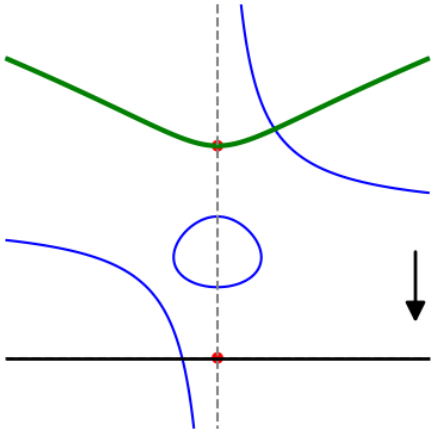


Unbounded components

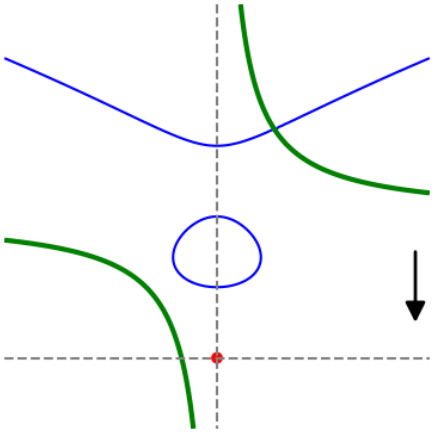
Compute points per connected components



Bounded components

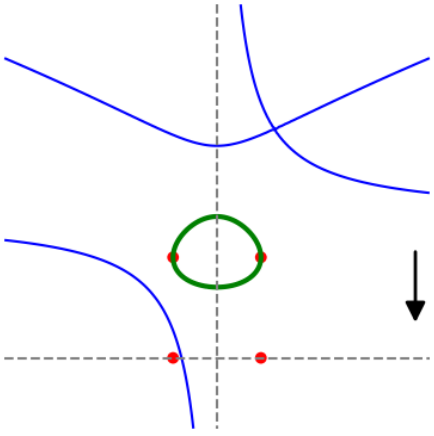


Unbounded components

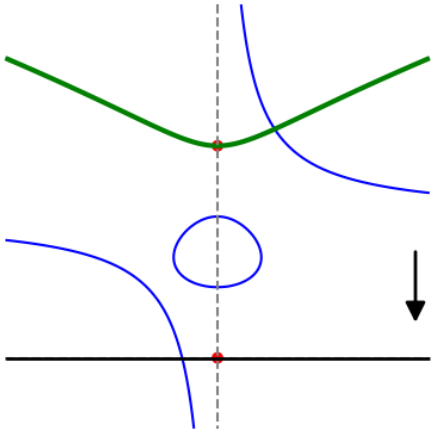


Non-proper points

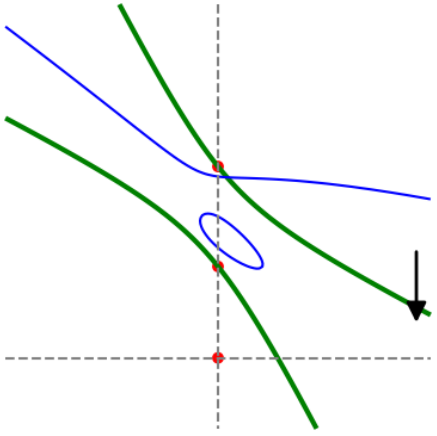
Compute points per connected components



Bounded components

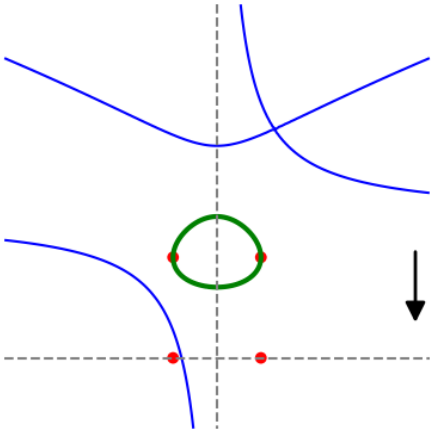


Unbounded components

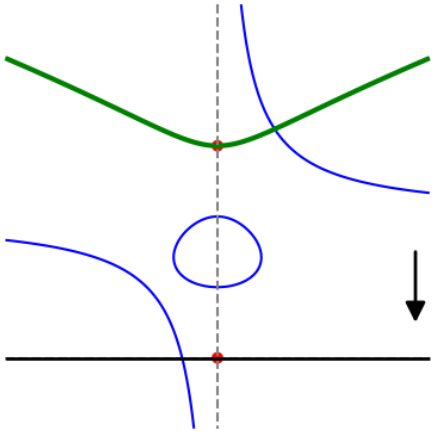


Non-proper points

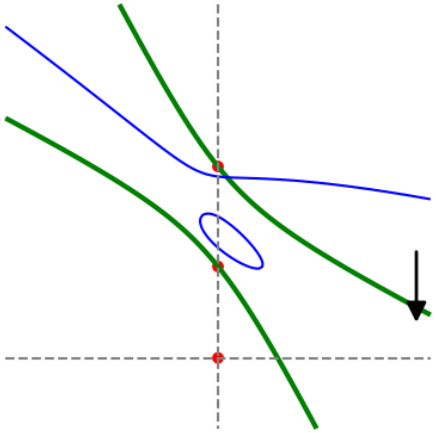
Compute points per connected components



Bounded components



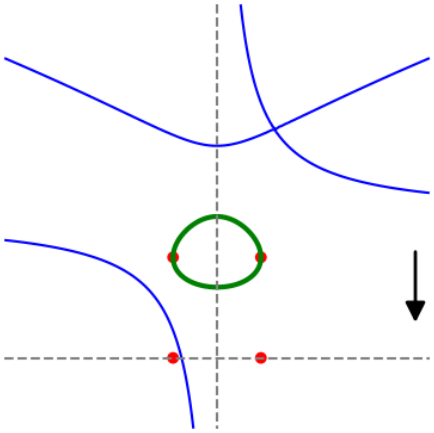
Unbounded components



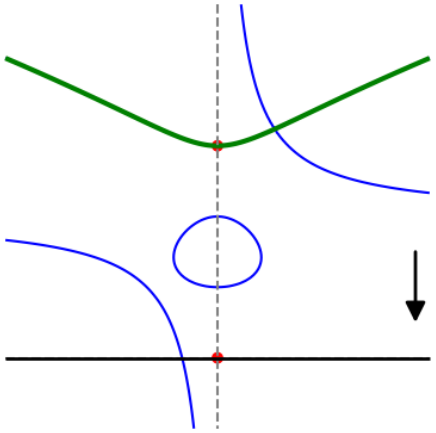
Non-proper points

Consider y as parameters

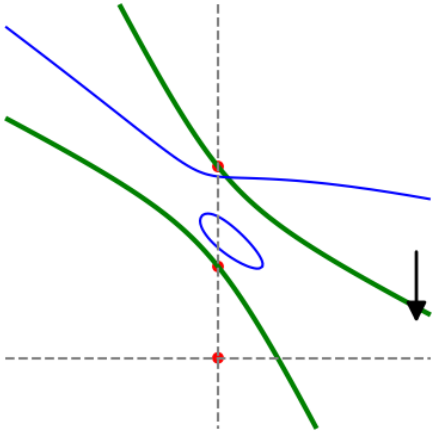
Compute points per connected components



Bounded components



Unbounded components



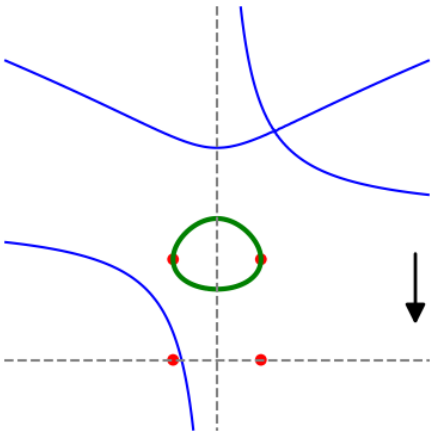
Non-proper points

Consider y as parameters

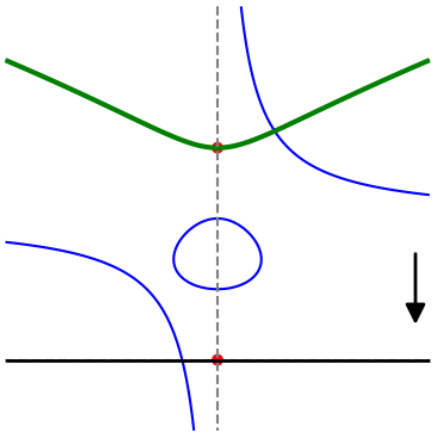
Generic $A \in \mathrm{GL}(n, \mathbb{Q})$

$f \mapsto f^A = f(A \cdot x, y)$: **ensure properness**

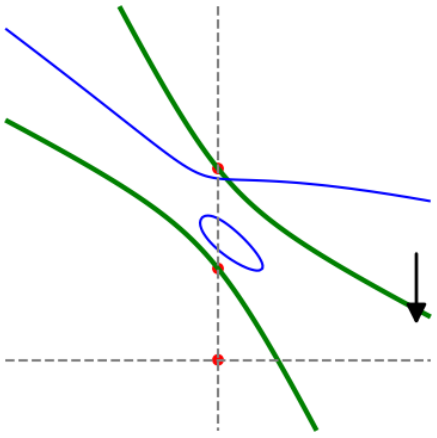
Compute points per connected components



Bounded components



Unbounded components



Non-proper points

Consider y as parameters

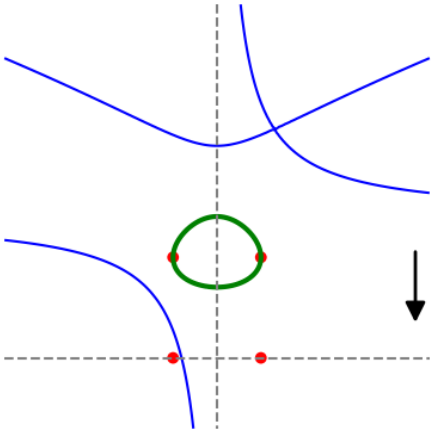
Generic $A \in \mathrm{GL}(n, \mathbb{Q})$

$f \mapsto f^A = f(A \cdot x, y)$: **ensure properness**

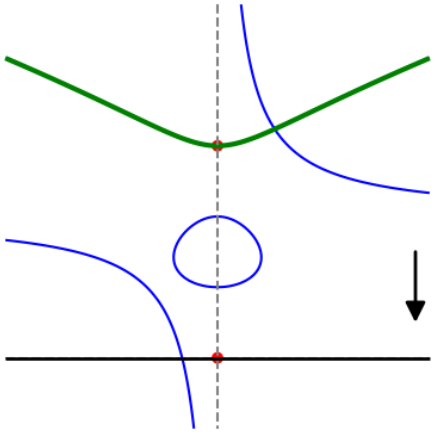
$\pi_i : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_i)$

$\mathbf{crit}(\pi_i, f^A)$: critical locus of π_i on $V(f^A)$

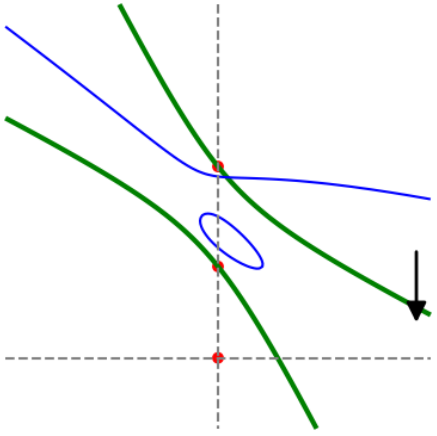
Compute points per connected components



Bounded components



Unbounded components



Non-proper points

Consider y as parameters

Generic $A \in \mathrm{GL}(n, \mathbb{Q})$ $\qquad$ $f \mapsto f^A = f(A \cdot x, y)$: **ensure properness**

$\pi_i : (x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_i)$ $\qquad$ $\mathbf{crit}(\pi_i, f^A)$: critical locus of π_i on $V(f^A)$

S_i defines $\mathbf{crit}(\pi_i, f^A) \cap \pi_{i-1}^{-1}(0, \ldots, 0)$

Safey El Din - Schost algorithm

Jacobian criterion

$$S_i = \underbrace{\left\{ f^A,\ (n-d)\text{-minors of } \left[\frac{\partial f^A}{\partial x_{i+1}}, \ldots, \frac{\partial f^A}{\partial x_n} \right] \right\}}_{\mathrm{crit}(\pi_i, f^A)} \cup \underbrace{\{x_1, \ldots, x_{i-1}\}}_{\pi_{i-1}^{-1}(0,\ldots,0)}$$

Safey El Din - Schost algorithm

Jacobian criterion

$$S_i = \underbrace{\left\{ f^A,\ (n-d)\text{-minors of } \left[\frac{\partial f^A}{\partial x_{i+1}}, \ldots, \frac{\partial f^A}{\partial x_n} \right] \right\}}_{\mathrm{crit}(\pi_i, f^A)} \cup \underbrace{\{x_1, \ldots, x_{i-1}\}}_{\pi_{i-1}^{-1}(0,\ldots,0)}$$

Geometric results

For generic A, S_i generates a radical zero-dimensional ideal in $\mathbb{Q}(y)[x]$.

For almost every $\eta \in \mathbb{C}^t$:

- The vanishing set of each $S_i(x, \eta)$ is finite.
- If $\eta \in \mathbb{R}^t$, their union intersects every component of $V(f(x, \eta)) \cap \mathbb{R}^n$.

Safey El Din - Schost algorithm

Jacobian criterion

$$S_i = \underbrace{\left\{ f^A,\ (n-d)\text{-minors of } \left[\frac{\partial f^A}{\partial x_{i+1}}, \ldots, \frac{\partial f^A}{\partial x_n} \right] \right\}}_{\mathrm{crit}(\pi_i, f^A)} \cup \underbrace{\{x_1, \ldots, x_{i-1}\}}_{\pi_{i-1}^{-1}(0,\ldots,0)}$$

Geometric results

For generic A, S_i generates a radical zero-dimensional ideal in $\mathbb{Q}(y)[x]$.

For almost every $\eta \in \mathbb{C}^t$:

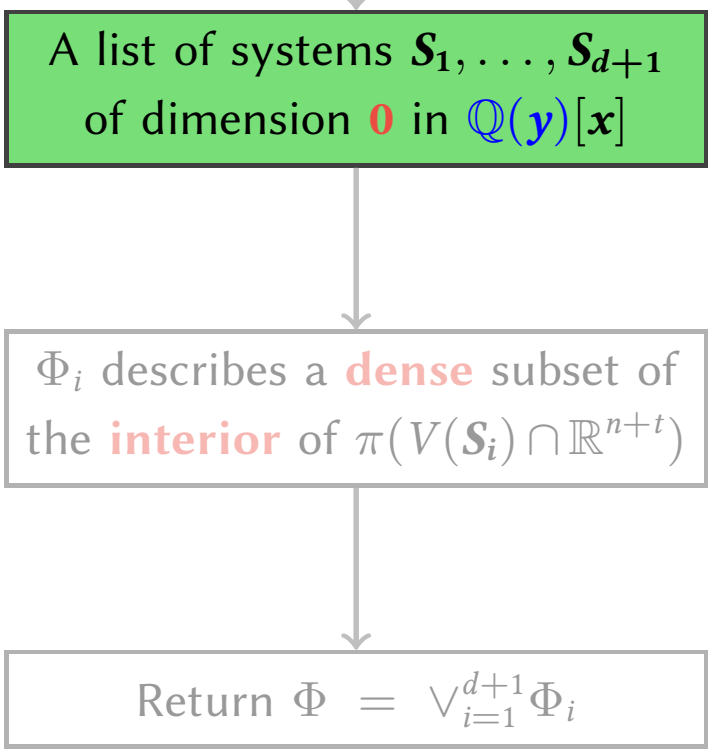
- The vanishing set of each $S_i(x, \eta)$ is finite.
- If $\eta \in \mathbb{R}^t$, their union intersects every component of $V(f(x, \eta)) \cap \mathbb{R}^n$.

S_i is a determinantal system: Useful for complexity analysis!

Second step: Classify real roots of S_i

S_i generates a radical zero-dimensional ideal in $\mathbb{Q}(y)[x]$

$\langle f \rangle$ has dimension d in $\mathbb{Q}(y)[x]$



Second step: Classify real roots of S_i

S_i generates a radical zero-dimensional ideal in $\mathbb{Q}(y)[x]$

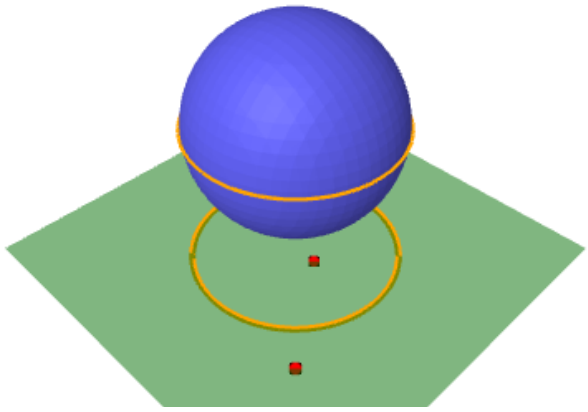
$\langle f \rangle$ has dimension d in $\mathbb{Q}(y)[x]$

A list of systems $S_1, \ldots, S_{d+1}$ of dimension 0 in $\mathbb{Q}(y)[x]$

Classify real roots of S_i

Φ_i describes a dense subset of the interior of $\pi(V(S_i) \cap \mathbb{R}^{n+t})$

Return $\Phi = \vee_{i=1}^{d+1} \Phi_i$



Real root classification

$$x^2 + {y_1}^2 + {y_2}^2 = 1$$

Output:
$$\begin{cases} {y_1}^2 + {y_2}^2 < 1 & : \text{ 2 solutions} \\ {y_1}^2 + {y_2}^2 > 1 & : \text{ 0 solution} \\ {y_1}^2 + {y_2}^2 = 1 & : \text{ 1 solution} \end{cases}$$

Omit the index i: $S_i \to S$

Classic algorithms and drawbacks

- Sturm-based algorithms: Univariate polynomials with parameters
  [González-Vega, Recio, Lombardi, Roy '98; Liang, Jeffrey, Moreno Maza '08]

Classic algorithms and drawbacks

- Sturm-based algorithms: Univariate polynomials with parameters
  [González-Vega, Recio, Lombardi, Roy '98; Liang, Jeffrey, Moreno Maza '08]

$$V(\boldsymbol{S}) = \left\{ q(x_n) = 0, x_1 = \frac{v_1(x_n)}{q'(x_n)}, \ldots, x_{n-1} = \frac{v_1(x_n)}{q'(x_n)} \right\}$$

  where $q, v_1, \ldots, v_{n-1} \in \mathbb{Q}[\boldsymbol{y}][x_n]$

Classic algorithms and drawbacks

- Sturm-based algorithms: Univariate polynomials with parameters
  [González-Vega, Recio, Lombardi, Roy '98; Liang, Jeffrey, Moreno Maza '08]

$$V(\boldsymbol{S}) = \left\{ q(x_n) = 0, x_1 = \frac{v_1(x_n)}{q'(x_n)}, \ldots, x_{n-1} = \frac{v_1(x_n)}{q'(x_n)} \right\}$$

  where $q, v_1, \ldots, v_{n-1} \in \mathbb{Q}[\boldsymbol{y}][x_n]$

  Classify real roots of $q(x_n)$: Sturm's sequence.

Classic algorithms and drawbacks

- Sturm-based algorithms: Univariate polynomials with parameters
  [González-Vega, Recio, Lombardi, Roy '98; Liang, Jeffrey, Moreno Maza '08]

$$V(\boldsymbol{S}) = \left\{ q(x_n) = 0, x_1 = \frac{v_1(x_n)}{q'(x_n)}, \ldots, x_{n-1} = \frac{v_1(x_n)}{q'(x_n)} \right\}$$

  where $q, v_1, \ldots, v_{n-1} \in \mathbb{Q}[\boldsymbol{y}][x_n]$

  Classify real roots of $q(x_n)$: Sturm's sequence.

Degree overhead

Classic algorithms and drawbacks

- Sturm-based algorithms: Univariate polynomials with parameters
  [González-Vega, Recio, Lombardi, Roy '98; Liang, Jeffrey, Moreno Maza '08]

$$V(\boldsymbol{S}) = \left\{ q(x_n) = 0, x_1 = \frac{v_1(x_n)}{q'(x_n)}, \ldots, x_{n-1} = \frac{v_1(x_n)}{q'(x_n)} \right\}$$

  where $q, v_1, \ldots, v_{n-1} \in \mathbb{Q}[\boldsymbol{y}][x_n]$

  Classify real roots of $q(x_n)$: Sturm's sequence.

  Degree overhead

- Border polynomials and Discriminant variety:
  [Yang, Xia '05; Lazard, Rouillier '07]

Classic algorithms and drawbacks

- Sturm-based algorithms: Univariate polynomials with parameters
  [González-Vega, Recio, Lombardi, Roy '98; Liang, Jeffrey, Moreno Maza '08]

$$V(\boldsymbol{S}) = \left\{ q(x_n) = 0, x_1 = \frac{v_1(x_n)}{q'(x_n)}, \ldots, x_{n-1} = \frac{v_1(x_n)}{q'(x_n)} \right\}$$

  where $q, v_1, \ldots, v_{n-1} \in \mathbb{Q}[\boldsymbol{y}][x_n]$

  Classify real roots of $q(x_n)$: Sturm's sequence.

  Degree overhead

- Border polynomials and Discriminant variety:
  [Yang, Xia '05; Lazard, Rouillier '07]

Compute $w \in \mathbb{Q}[\boldsymbol{y}]$ s.t. the number of real roots of $\boldsymbol{S}(\boldsymbol{x}, \eta)$ is invariant over each connected component of $\mathbb{R}^t \setminus V(w)$.

Classic algorithms and drawbacks

- Sturm-based algorithms: Univariate polynomials with parameters
  [González-Vega, Recio, Lombardi, Roy '98; Liang, Jeffrey, Moreno Maza '08]

$$V(\boldsymbol{S}) = \left\{ q(x_n) = 0, x_1 = \frac{v_1(x_n)}{q'(x_n)}, \ldots, x_{n-1} = \frac{v_1(x_n)}{q'(x_n)} \right\}$$

  where $q, v_1, \ldots, v_{n-1} \in \mathbb{Q}[\boldsymbol{y}][x_n]$

  Classify real roots of $q(x_n)$: Sturm's sequence. **Degree overhead**

- Border polynomials and Discriminant variety:
  [Yang, Xia '05; Lazard, Rouillier '07]

  Compute $w \in \mathbb{Q}[\boldsymbol{y}]$ s.t. the number of real roots of $\boldsymbol{S}(\boldsymbol{x}, \eta)$ is invariant over each connected component of $\mathbb{R}^t \setminus V(w)$.

  - No intermediate projection.
  - Obtain formulas by **CAD** of $\mathbb{R}^t \setminus V(w)$.

Classic algorithms and drawbacks

- Sturm-based algorithms: Univariate polynomials with parameters
  [González-Vega, Recio, Lombardi, Roy '98; Liang, Jeffrey, Moreno Maza '08]

$$V(\boldsymbol{S}) = \left\{ q(x_n) = 0, x_1 = \frac{v_1(x_n)}{q'(x_n)}, \ldots, x_{n-1} = \frac{v_1(x_n)}{q'(x_n)} \right\}$$

  where $q, v_1, \ldots, v_{n-1} \in \mathbb{Q}[\boldsymbol{y}][x_n]$

  Classify real roots of $q(x_n)$: Sturm's sequence. **Degree overhead**

- Border polynomials and Discriminant variety:
  [Yang, Xia '05; Lazard, Rouillier '07]

  Compute $w \in \mathbb{Q}[\boldsymbol{y}]$ s.t. the number of real roots of $\boldsymbol{S}(\boldsymbol{x}, \eta)$ is invariant over each connected component of $\mathbb{R}^t \setminus V(w)$.

  - No intermediate projection.
  - Obtain formulas by **CAD** of $\mathbb{R}^t \setminus V(w)$. **Doubly exponential in t**

Classic algorithms and drawbacks

- Sturm-based algorithms: Univariate polynomials with parameters
  [González-Vega, Recio, Lombardi, Roy '98; Liang, Jeffrey, Moreno Maza '08]

$$V(\boldsymbol{S}) = \left\{ q(x_n) = 0, x_1 = \frac{v_1(x_n)}{q'(x_n)}, \ldots, x_{n-1} = \frac{v_1(x_n)}{q'(x_n)} \right\}$$

  where $q, v_1, \ldots, v_{n-1} \in \mathbb{Q}[\boldsymbol{y}][x_n]$

  Classify real roots of $q(x_n)$: Sturm's sequence. **Degree overhead**

- Border polynomials and Discriminant variety:
  [Yang, Xia '05; Lazard, Rouillier '07]

Compute $w \in \mathbb{Q}[\boldsymbol{y}]$ s.t. the number of real roots of $\boldsymbol{S}(\boldsymbol{x}, \eta)$ is invariant over each connected component of $\mathbb{R}^t \setminus V(w)$.

- No intermediate projection.
- Obtain formulas by **CAD** of $\mathbb{R}^t \setminus V(w)$. **Doubly exponential in t**

An alternative to Sturm's theorem: **Hermite's quadratic forms**

Hermite's matrices

Ch. Hermite

Root counting using quadratic forms [Hermite 1856]
Multivariate Hermite's quadratic forms:
[Pedersen '91; Pedersen, Roy, Szpirglas '93; Rouillier '99; Basu, Pollack, Roy '06]

Use Hermite matrices for parametric systems:

[Henrion '10; Netzer, Plaumann, Thom '11; L. and Safey El Din '20]

Hermite's matrices

Ch. Hermite

Root counting using quadratic forms [Hermite 1856]
Multivariate Hermite's quadratic forms:
[Pedersen '91; Pedersen, Roy, Szpirglas '93; Rouillier '99; Basu, Pollack, Roy '06]

Use Hermite matrices for parametric systems:

[Henrion '10; Netzer, Plaumann, Thom '11; L. and Safey El Din '20]

Given a field $\mathbb{K}$, $S \subset \mathbb{K}[x]$ of dimension 0

$\mathbb{K}[x]/\langle S \rangle$ is a vector space of finite dimension δ

Hermite's matrices

Ch. Hermite

Root counting using quadratic forms [Hermite 1856]
Multivariate Hermite's quadratic forms:
[Pedersen '91; Pedersen, Roy, Szpirglas '93; Rouillier '99; Basu, Pollack, Roy '06]

Use Hermite matrices for parametric systems:

[Henrion '10; Netzer, Plaumann, Thom '11; L. and Safey El Din '20]

Given a field $\mathbb{K}$, $S \subset \mathbb{K}[x]$ of dimension 0

$\mathbb{K}[x]/\langle S \rangle$ is a vector space of finite dimension δ

Multiplication linear map $\mathcal{L}_p$

$$\mathbb{K}[x]/\langle S \rangle \to \mathbb{K}[x]/\langle S \rangle,$$
$$q \mapsto p \cdot q$$

Hermite's matrices

Ch. Hermite

Root counting using quadratic forms [Hermite 1856]
Multivariate Hermite's quadratic forms:
[Pedersen '91; Pedersen, Roy, Szpirglas '93; Rouillier '99; Basu, Pollack, Roy '06]

Use Hermite matrices for parametric systems:

[Henrion '10; Netzer, Plaumann, Thom '11; L. and Safey El Din '20]

Given a field $\mathbb{K}$, $S \subset \mathbb{K}[x]$ of dimension 0

$\mathbb{K}[x]/\langle S \rangle$ is a vector space of finite dimension δ

Multiplication linear map $\mathcal{L}_p$

$$\mathbb{K}[x]/\langle S \rangle \to \mathbb{K}[x]/\langle S \rangle,$$
$$q \mapsto p \cdot q$$

Hermite's quadratic form of S

$$p, q \in \mathbb{K}[x]/\langle S \rangle,$$
$$(p, q) \mapsto \mathrm{trace}(\mathcal{L}_{p \cdot q})$$

Hermite's matrices

Ch. Hermite

Root counting using quadratic forms [Hermite 1856]
Multivariate Hermite's quadratic forms:
[Pedersen '91; Pedersen, Roy, Szpirglas '93; Rouillier '99; Basu, Pollack, Roy '06]

Use Hermite matrices for parametric systems:

[Henrion '10; Netzer, Plaumann, Thom '11; L. and Safey El Din '20]

Given a field $\mathbb{K}$, $S \subset \mathbb{K}[x]$ of dimension 0

$\mathbb{K}[x]/\langle S \rangle$ is a vector space of finite dimension δ

Multiplication linear map $\mathcal{L}_p$

$$\mathbb{K}[x]/\langle S \rangle \to \mathbb{K}[x]/\langle S \rangle,$$
$$q \mapsto p \cdot q$$

Hermite's quadratic form of S

$$p, q \in \mathbb{K}[x]/\langle S \rangle,$$
$$(p, q) \mapsto \operatorname{trace}(\mathcal{L}_{p \cdot q})$$

Fix a basis $M = \{m_1, \ldots, m_\delta\}$. The **Hermite matrix** of S w.r.t. M is

$$H = (\underbrace{\operatorname{trace}(\mathcal{L}_{m_k \cdot m_\ell})}_{\in \mathbb{K}})_{1 \le k, \ell \le \delta}.$$

Parametric Hermite matrices

Take $\mathbb{K} = \mathbb{Q}(\boldsymbol{y})$ as coefficient field, $\boldsymbol{S}$ is zero-dimensional in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$

Fix some basis $\boldsymbol{M} = \{m_1, \ldots, m_\delta\}$ of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/\langle \boldsymbol{S} \rangle$

$$\boldsymbol{H} = \left(\operatorname{trace}\left(\mathcal{L}_{m_k \cdot m_\ell}\right)\right)_{1 \leq k, \ell \leq \delta}$$

Parametric Hermite matrices

Take $\mathbb{K} = \mathbb{Q}(\boldsymbol{y})$ as coefficient field, $\boldsymbol{S}$ is zero-dimensional in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$

Fix some basis $\boldsymbol{M} = \{m_1, \ldots, m_\delta\}$ of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/\langle \boldsymbol{S} \rangle$

$$\boldsymbol{H} = \left(\operatorname{trace}\left(\mathcal{L}_{m_k \cdot m_\ell}\right)\right)_{1 \le k, \ell \le \delta}$$

Choose a basis $\boldsymbol{M}$ of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/\langle \boldsymbol{S} \rangle$?

$\boldsymbol{G} \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$: the reduced Gröbner basis of $\boldsymbol{S}$ w.r.t. $\mathbf{grevlex}(\boldsymbol{x}) \succ \mathbf{grevlex}(\boldsymbol{y})$

$$\boldsymbol{M} = \{\text{monomials in } \boldsymbol{x} \text{ that are irreducible by } \boldsymbol{G}\}$$

Parametric Hermite matrices

Take $\mathbb{K} = \mathbb{Q}(\boldsymbol{y})$ as coefficient field, $\boldsymbol{S}$ is zero-dimensional in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$

Fix some basis $\boldsymbol{M} = \{m_1, \ldots, m_\delta\}$ of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/\langle \boldsymbol{S} \rangle$

$$\boldsymbol{H} = \left(\operatorname{trace}\left(\mathcal{L}_{m_k \cdot m_\ell}\right)\right)_{1 \leq k, \ell \leq \delta}$$

Choose a basis $\boldsymbol{M}$ of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/\langle \boldsymbol{S} \rangle$?

$\boldsymbol{G} \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$: the reduced Gröbner basis of $\boldsymbol{S}$ w.r.t. $\mathbf{grevlex}(\boldsymbol{x}) \succ \mathbf{grevlex}(\boldsymbol{y})$

$$\boldsymbol{M} = \{\text{monomials in } \boldsymbol{x} \text{ that are irreducible by } \boldsymbol{G}\}$$

Specialization property

Parametric Hermite matrices

Take $\mathbb{K} = \mathbb{Q}(\boldsymbol{y})$ as coefficient field, $\boldsymbol{S}$ is zero-dimensional in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$

Fix some basis $\boldsymbol{M} = \{m_1, \ldots, m_\delta\}$ of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/\langle \boldsymbol{S} \rangle$

$$\boldsymbol{H} = \left(\operatorname{trace}\left(\mathcal{L}_{m_k \cdot m_\ell}\right)\right)_{1 \le k,\ell \le \delta}$$

Choose a basis $\boldsymbol{M}$ of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/\langle \boldsymbol{S} \rangle$?

$\boldsymbol{G} \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$: the reduced Gröbner basis of $\boldsymbol{S}$ w.r.t. $\mathbf{grevlex}(\boldsymbol{x}) \succ \mathbf{grevlex}(\boldsymbol{y})$

$$\boldsymbol{M} = \{\text{monomials in } \boldsymbol{x} \text{ that are irreducible by } \boldsymbol{G}\}$$

Specialization property

$$w_\infty = \prod_{g \in \boldsymbol{G}} \operatorname{leadingcoeff}(g, \boldsymbol{x}) \in \mathbb{Q}[\boldsymbol{y}]$$

$\boldsymbol{H}$ specializes well if $w_\infty(\eta) \neq 0$

Parametric Hermite matrices

Take $\mathbb{K} = \mathbb{Q}(\boldsymbol{y})$ as coefficient field, $\boldsymbol{S}$ is zero-dimensional in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$

Fix some basis $\boldsymbol{M} = \{m_1, \ldots, m_\delta\}$ of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/\langle \boldsymbol{S} \rangle$

$$\boldsymbol{H} = \left(\operatorname{trace}\left(\mathcal{L}_{m_k \cdot m_\ell}\right)\right)_{1 \le k, \ell \le \delta}$$

Choose a basis $\boldsymbol{M}$ of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/\langle \boldsymbol{S} \rangle$?

$\boldsymbol{G} \subset \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$: the reduced Gröbner basis of $\boldsymbol{S}$ w.r.t. $\mathbf{grevlex}(\boldsymbol{x}) \succ \mathbf{grevlex}(\boldsymbol{y})$

$$\boldsymbol{M} = \{\text{monomials in } \boldsymbol{x} \text{ that are irreducible by } \boldsymbol{G}\}$$

Specialization property

$$w_\infty = \prod_{g \in \boldsymbol{G}} \operatorname{leadingcoeff}(g, \boldsymbol{x}) \in \mathbb{Q}[\boldsymbol{y}]$$

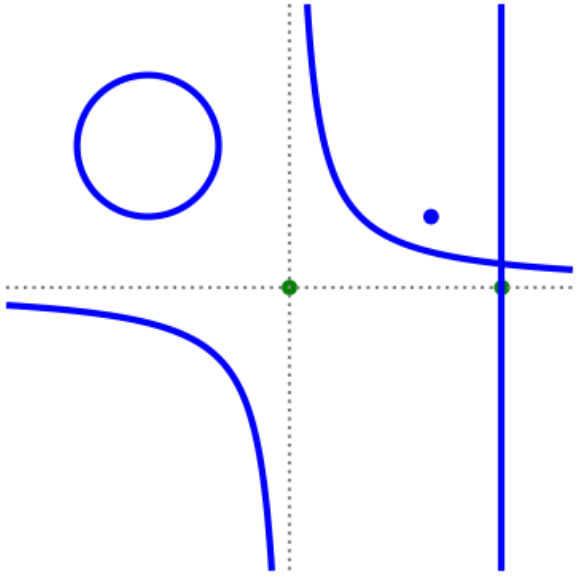
$\boldsymbol{H}$ specializes well if $w_\infty(\eta) \neq 0$

Number of complex roots of $\boldsymbol{S}(\boldsymbol{x}, \eta)$	$=$	Rank of $\boldsymbol{H}(\eta)$
Number of real roots of $\boldsymbol{S}(\boldsymbol{x}, \eta)$	$=$	Signature of $\boldsymbol{H}(\eta)$

A better way to obtain the boundary!

$V(\boldsymbol{w}_\infty) \in \mathbb{C}^t$ contains:

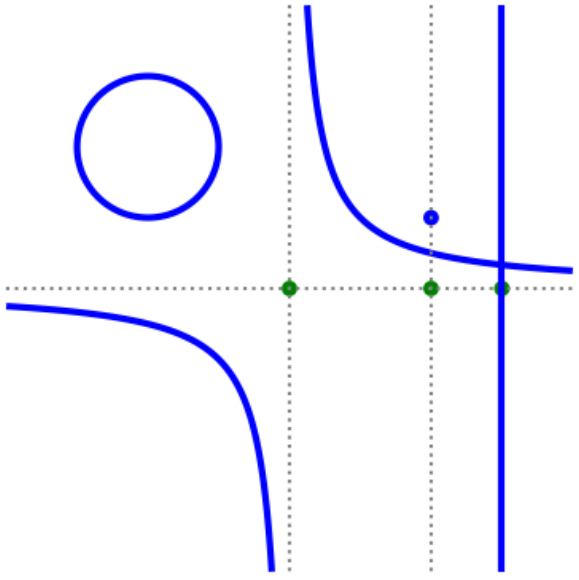
- Non-proper points.



A better way to obtain the boundary!

$V(\boldsymbol{w_\infty}) \in \mathbb{C}^t$ contains:

- Non-proper points.
- Projection of components of dimension $< t$.



A better way to obtain the boundary!

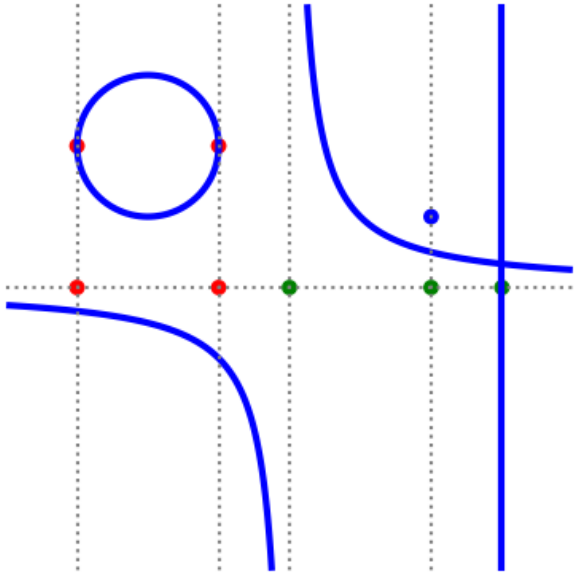
$V(\boldsymbol{w}_\infty) \in \mathbb{C}^t$ contains:

- Non-proper points.
- Projection of components of dimension $< t$.

$\det \boldsymbol{H}(\eta) = 0$ and $\boldsymbol{w}_\infty(\eta) \neq 0$

- rank $\boldsymbol{H}(\eta) < \delta = \dim \mathbb{C}[\boldsymbol{x}]/\langle \boldsymbol{S}(\boldsymbol{x}, \eta)\rangle$

$\rightsquigarrow$ Roots with multiplicities appear.



A better way to obtain the boundary!

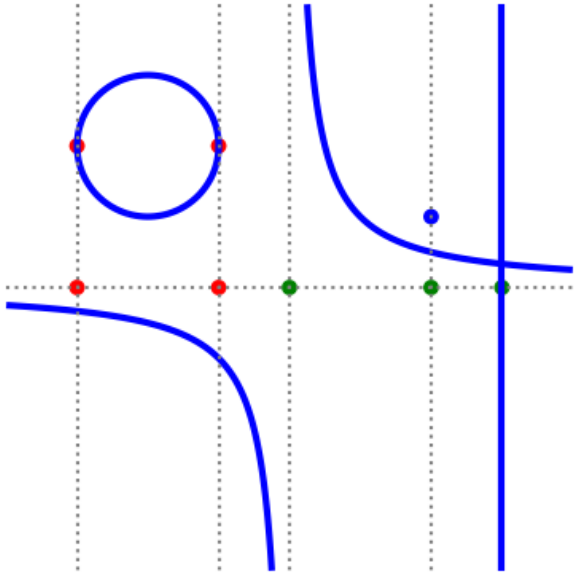
$V(\boldsymbol{w}_\infty) \in \mathbb{C}^t$ contains:

- Non-proper points.
- Projection of components of dimension $< t$.

$\det \boldsymbol{H}(\eta) = 0$ and $\boldsymbol{w}_\infty(\eta) \neq 0$

- rank $\boldsymbol{H}(\eta) < \delta = \dim \mathbb{C}[\boldsymbol{x}]/\langle \boldsymbol{S}(\boldsymbol{x}, \eta)\rangle$

$\rightsquigarrow$ Roots with multiplicities appear.



Theorem Proof uses Thom's isotopy lemma

Number of real roots of $\boldsymbol{S}(\boldsymbol{x}, \eta)$ is invariant over each connected component of the set defined by $\boldsymbol{w}_\infty \neq 0$ and $\det \boldsymbol{H} \neq 0$.

A better way to obtain the boundary!

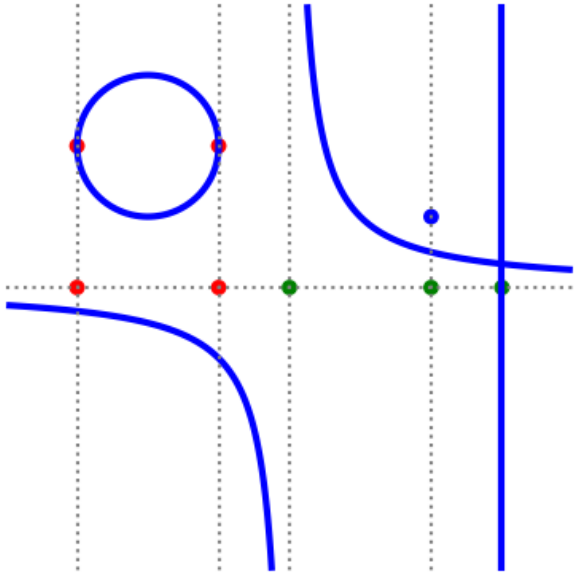
$V(\boldsymbol{w}_\infty) \in \mathbb{C}^t$ contains:

- Non-proper points.
- Projection of components of dimension $< t$.

$\det \boldsymbol{H}(\eta) = 0$ and $\boldsymbol{w}_\infty(\eta) \neq 0$

- rank $\boldsymbol{H}(\eta) < \delta = \dim \mathbb{C}[\boldsymbol{x}]/\langle \boldsymbol{S}(\boldsymbol{x}, \eta)\rangle$

$\rightsquigarrow$ Roots with multiplicities appear.



Theorem Proof uses Thom's isotopy lemma

Number of real roots of $\boldsymbol{S}(\boldsymbol{x}, \eta)$ is invariant over each connected component of the set defined by $\boldsymbol{w}_\infty \neq 0$ and $\det \boldsymbol{H} \neq 0$.

Compare with Maple:

- **Discriminant variety** (DV)
- **Border polynomial** (BP)

A better way to obtain the boundary!

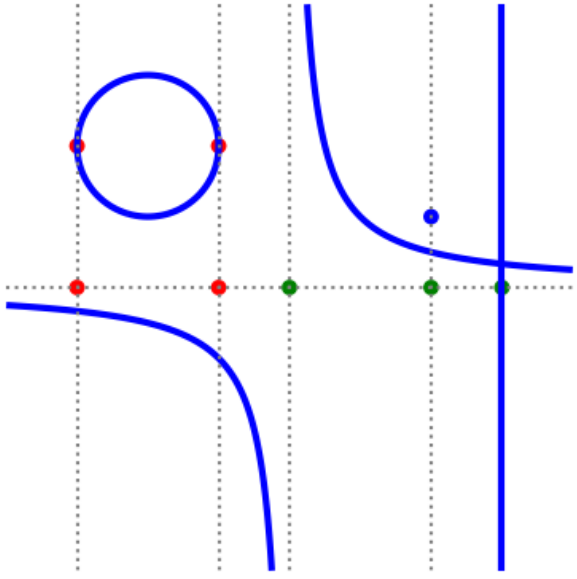
$V(\boldsymbol{w}_\infty) \in \mathbb{C}^t$ contains:

- Non-proper points.
- Projection of components of dimension $< t$.

$\det \boldsymbol{H}(\eta) = 0$ and $\boldsymbol{w}_\infty(\eta) \neq 0$

- rank $\boldsymbol{H}(\eta) < \delta = \dim \mathbb{C}[\boldsymbol{x}]/\langle \boldsymbol{S}(\boldsymbol{x}, \eta)\rangle$

$\rightsquigarrow$ Roots with multiplicities appear.



Theorem — Proof uses Thom's isotopy lemma

Number of real roots of $\boldsymbol{S}(\boldsymbol{x}, \eta)$ is invariant over each connected component of the set defined by $\boldsymbol{w}_\infty \neq 0$ and $\det \boldsymbol{H} \neq 0$.

Compare with Maple:

- **Discriminant variety** (DV)
- **Border polynomial** (BP)

Random dense systems $\longrightarrow$

t	D	HERMITE	MAPLE[DV]	MAPLE[BP]
2	$[2,2,2]$	**.6 s**	17 m	23 s
2	$[3,3]$	**1.1 s**	2 h	8 s
3	$[3,2]$	**.4 s**	2 h	3 s
3	$[2,2,2]$	**8 s**	$>$ 120 h	20 m
3	$[4,2]$	**12 s**	$>$ 120 h	15 m

Algorithm for classifying real roots

For $\eta \in \mathbb{R}^t$ s.t. $\boldsymbol{w}_{\infty}(\eta) \neq 0$:

$$\text{Number of real roots of } \boldsymbol{S}(\boldsymbol{x}, \eta) \quad = \quad \underbrace{\text{Signature of } \boldsymbol{H}(\eta)}_{\text{signs of principal minors } M_1, \ldots, M_\delta \text{ of } \boldsymbol{H}}$$

Algorithm for classifying real roots

For $\eta \in \mathbb{R}^t$ s.t. $\boldsymbol{w}_\infty(\eta) \neq 0$:

$$\text{Number of real roots of } \boldsymbol{S}(\boldsymbol{x}, \eta) \quad = \quad \underbrace{\text{Signature of } \boldsymbol{H}(\eta)}_{\text{signs of principal minors } M_1, \ldots, M_\delta \text{ of } \boldsymbol{H}}$$

Algorithm

1. Compute points per connected components of the set defined by

$$M_1 \neq 0 \wedge \ldots \wedge M_\delta \neq 0 \wedge \boldsymbol{w}_\infty \neq 0.$$

Algorithm for classifying real roots

For $\eta \in \mathbb{R}^t$ s.t. $\boldsymbol{w_\infty}(\eta) \neq 0$:

$$\text{Number of real roots of } \boldsymbol{S}(\boldsymbol{x}, \eta) \quad = \quad \underbrace{\text{Signature of } \boldsymbol{H}(\eta)}_{\text{signs of principal minors } M_1, \ldots, M_\delta \text{ of } \boldsymbol{H}}$$

Algorithm

1. Compute points per connected components of the set defined by

$$M_1 \neq 0 \wedge \ldots \wedge M_\delta \neq 0 \wedge \boldsymbol{w_\infty} \neq 0.$$

2. Evaluate the signs of $M_1, \ldots, M_\delta$ and the signature of $\boldsymbol{H}$ at those points.

Algorithm for classifying real roots

For $\eta \in \mathbb{R}^t$ s.t. $\boldsymbol{w_\infty}(\eta) \neq 0$:

$$\text{Number of real roots of } \boldsymbol{S}(\boldsymbol{x}, \eta) \quad = \quad \underbrace{\text{Signature of } \boldsymbol{H}(\eta)}_{\text{signs of principal minors } M_1, \ldots, M_\delta \text{ of } \boldsymbol{H}}$$

Algorithm

1. Compute points per connected components of the set defined by
$$M_1 \neq 0 \wedge \ldots \wedge M_\delta \neq 0 \wedge \boldsymbol{w_\infty} \neq 0.$$
2. Evaluate the signs of $M_1, \ldots, M_\delta$ and the signature of $\boldsymbol{H}$ at those points.
3. Return the sign conditions that yield positive signature for $\boldsymbol{H}$.

Output for one block QE!

Algorithm for classifying real roots

For $\eta \in \mathbb{R}^t$ s.t. $\boldsymbol{w_\infty}(\eta) \neq 0$:

$$\text{Number of real roots of } \boldsymbol{S}(\boldsymbol{x}, \eta) \quad = \quad \underbrace{\text{Signature of } \boldsymbol{H}(\eta)}_{\text{signs of principal minors } M_1, \ldots, M_\delta \text{ of } \boldsymbol{H}}$$

Algorithm

1. Compute points per connected components of the set defined by
$$M_1 \neq 0 \wedge \ldots \wedge M_\delta \neq 0 \wedge \boldsymbol{w_\infty} \neq 0.$$
2. Evaluate the signs of $M_1, \ldots, M_\delta$ and the signature of $\boldsymbol{H}$ at those points.
3. Return the sign conditions that yield positive signature for $\boldsymbol{H}$.

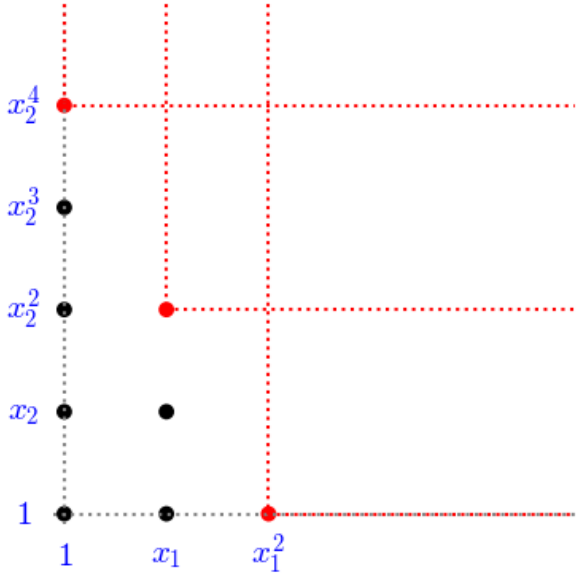
Output for one block QE!

If we want also the real root classification:

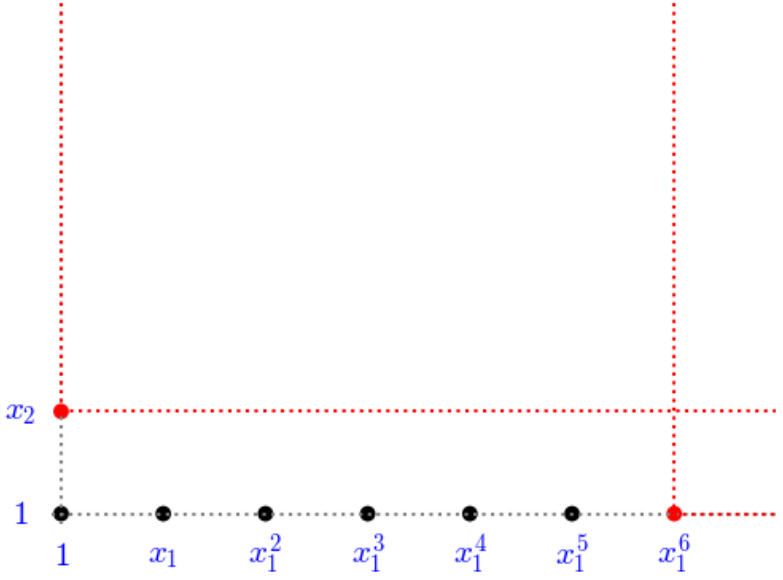
3'. Return all the sign conditions and the corresponding number of real solutions.

Choice of bases for quotient rings

Monomial order over $\boldsymbol{x}$ → Gröbner bases → Basis of quotient rings



grevlex staircase



lex staircase

Choice of bases for quotient rings

Monomial order over $\boldsymbol{x}$  Gröbner bases  Basis of quotient rings

- Gröbner bases of **grevlex** have lower degree than **lex**
- The generic staircase for **grevlex** is known [Moreno-Socías '03]

Choice of bases for quotient rings

Monomial order over $\boldsymbol{x}$ → Gröbner bases → Basis of quotient rings

- Gröbner bases of **grevlex** have lower degree than **lex**
- The generic staircase for **grevlex** is known [Moreno-Socías '03]

$(g_1, g_2) \subset \mathbb{Q}[x_1, x_2, \boldsymbol{y}]$: random dense polynomials of total degree 2

Degree in $\boldsymbol{y}$ of entries in Hermite matrices:

grevlex $\boldsymbol{H}_1$:
$$\begin{bmatrix} 0 & 1 & 1 & 2 \\ 1 & 2 & 2 & 3 \\ 1 & 2 & 2 & 3 \\ 2 & 3 & 3 & 4 \end{bmatrix}$$

lex $\boldsymbol{H}_2$:
$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 \end{bmatrix}$$

Change basis of $\mathbb{Q}(\boldsymbol{y})/\langle g_1, g_2 \rangle$: $\boldsymbol{H}_2 = P^T \cdot \boldsymbol{H}_1 \cdot P$

$$\det \boldsymbol{H}_2 = \det \boldsymbol{H}_1 \cdot (\det P)^2$$

Choice of bases for quotient rings

Monomial order over $\boldsymbol{x}$ → Gröbner bases → Basis of quotient rings

- Gröbner bases of **grevlex** have lower degree than **lex**
- The generic staircase for **grevlex** is known [Moreno-Socías '03]

$(g_1, g_2) \subset \mathbb{Q}[x_1, x_2, \boldsymbol{y}]$: random dense polynomials of total degree 2

Degree in $\boldsymbol{y}$ of entries in Hermite matrices:

$$\textbf{grevlex } \boldsymbol{H}_1: \begin{bmatrix} 0 & 1 & 1 & 2 \\ 1 & 2 & 2 & 3 \\ 1 & 2 & 2 & 3 \\ 2 & 3 & 3 & 4 \end{bmatrix} \qquad \textbf{lex } \boldsymbol{H}_2: \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 \end{bmatrix}$$

Change basis of $\mathbb{Q}(\boldsymbol{y})/\langle g_1, g_2 \rangle$: $\boldsymbol{H}_2 = P^T \cdot \boldsymbol{H}_1 \cdot P$

$$\det \boldsymbol{H}_2 = \det \boldsymbol{H}_1 \cdot (\det P)^2$$

We use **grevlex** Gröbner bases for constructing Hermite matrices

Degree bound & Complexity

Complexity? Calls to RRC are the **main cost** ⇝ Computing sample points?

⇝ **Degree bound** for minors of Hermite matrices?

Degree bound & Complexity

Complexity? Calls to RRC are the **main cost** ⇝ Computing sample points?

⇝ **Degree bound** for minors of Hermite matrices?

Generic input: $f = (f_1, \ldots, f_s) \subset \mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_t]$ $(\deg(f_i) \leq D)$

Degree bound & Complexity

Complexity? Calls to RRC are the **main cost** ⇝ Computing sample points?

⇝ **Degree bound** for minors of Hermite matrices?

Generic input: $\boldsymbol{f} = (f_1, \ldots, f_s) \subset \mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_t]$ $(\deg(f_i) \leq D)$

Classifying real roots of $\boldsymbol{S}$ (a determinantal system)

- $\boldsymbol{M} = \{m_1, \ldots, m_\delta\}$: **grevlex** basis of $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]/\langle \boldsymbol{S} \rangle$
- $\boldsymbol{H} = (\boldsymbol{h_{k,\ell}})_{1 \leq k,\ell \leq \delta}$ $\quad h_{k,\ell} = \operatorname{trace}(\mathcal{L}_{m_k \cdot m_\ell})$

Degree bound & Complexity

Complexity? Calls to RRC are the **main cost** ⇝ Computing sample points?

⇝ **Degree bound** for minors of Hermite matrices?

Generic input: $f = (f_1, \ldots, f_s) \subset \mathbb{Q}[x_1, \ldots, x_n, y_1, \ldots, y_t]$ $(\deg(f_i) \leq D)$

Classifying real roots of S (a determinantal system)

- $M = \{m_1, \ldots, m_\delta\}$: **grevlex** basis of $\mathbb{Q}(y)[x]/\langle S \rangle$
- $H = (h_{k,\ell})_{1 \leq k,\ell \leq \delta}$ $\quad h_{k,\ell} = \operatorname{trace}(\mathcal{L}_{m_k \cdot m_\ell})$

Complexity for one block QE

- **Sharp** degree bound for the minors of H:

$$\mathfrak{B} = D^s(D-1)^{n-s}\left(2(n-s)(D-1)\binom{n-1}{s-2} + (n(D-2)+s)\binom{n-1}{s-1}\right)$$

- Arithmetic complexity [L. , Safey El Din '20]

$$O^{\sim}\left(8^t \mathfrak{B}^{3t}\binom{t+\mathfrak{B}}{t}\right)$$

Sketch of the proof

1. Generic f
   $\rightsquigarrow$ S in **Noether position**

$\longrightarrow$

Entries of H are in $\mathbb{Q}[y]$
$\deg(h_{k,\ell}) \leq \deg(m_k) + \deg(m_\ell)$

Sketch of the proof

1. Generic f $\rightsquigarrow$ S in **Noether position** $\longrightarrow$ Entries of H are in $\mathbb{Q}[y]$, $\deg(h_{k,\ell}) \leq \deg(m_k) + \deg(m_\ell)$

$$\deg(\det(H)) \leq 2 \sum_{m \in M} \deg(m)$$

Sketch of the proof

1. Generic $\boldsymbol{f}$ $\rightsquigarrow$ $\boldsymbol{S}$ in **Noether position** $\longrightarrow$ Entries of $\boldsymbol{H}$ are in $\mathbb{Q}[\boldsymbol{y}]$, $\deg(\boldsymbol{h_{k,\ell}}) \leq \deg(m_k) + \deg(m_\ell)$

$$\deg(\det(\boldsymbol{H})) \quad \leq \quad 2 \sum_{m \in \boldsymbol{M}} \deg(m)$$

2. Hilbert series of $\langle \boldsymbol{S} \rangle$ in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$: $\mathrm{HS}(z) = \sum_{i=0}^{\infty} c_i \cdot z^i$

Sketch of the proof

1. Generic $\boldsymbol{f}$ $\rightsquigarrow$ $\boldsymbol{S}$ in **Noether position** $\longrightarrow$ Entries of $\boldsymbol{H}$ are in $\mathbb{Q}[\boldsymbol{y}]$, $\deg(\boldsymbol{h}_{k,\ell}) \leq \deg(m_k) + \deg(m_\ell)$

$$\deg(\det(\boldsymbol{H})) \quad \leq \quad 2 \sum_{m \in \boldsymbol{M}} \deg(m)$$

2. Hilbert series of $\langle \boldsymbol{S} \rangle$ in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$: $\mathrm{HS}(z) = \sum_{i=0}^{\infty} c_i \cdot z^i$

   $\boldsymbol{M}$ from **grevlex**: $c_i = |\{m \in \boldsymbol{M} \mid \deg(m) = i\}|$

Sketch of the proof

1. Generic $\boldsymbol{f}$ $\rightsquigarrow$ $\boldsymbol{S}$ in **Noether position** $\longrightarrow$ Entries of $\boldsymbol{H}$ are in $\mathbb{Q}[\boldsymbol{y}]$, $\deg(\boldsymbol{h}_{k,\ell}) \leq \deg(m_k) + \deg(m_\ell)$

$$\deg(\det(\boldsymbol{H})) \quad \leq \quad 2 \sum_{m \in \boldsymbol{M}} \deg(m)$$

2. Hilbert series of $\langle \boldsymbol{S} \rangle$ in $\mathbb{Q}(\boldsymbol{y})[\boldsymbol{x}]$: $\mathrm{HS}(z) = \sum_{i=0}^{\infty} c_i \cdot z^i$

$\boldsymbol{M}$ from **grevlex**: $c_i = |\{m \in \boldsymbol{M} \mid \deg(m) = i\}|$

$$\mathrm{HS}'(1) \; = \sum_i i \cdot c_i = \sum_{m \in \boldsymbol{M}} \deg(m)$$

Sketch of the proof

1. Generic f $\rightsquigarrow$ S in **Noether position** $\longrightarrow$ Entries of H are in $\mathbb{Q}[y]$, $\deg(h_{k,\ell}) \leq \deg(m_k) + \deg(m_\ell)$

$$\deg(\det(H)) \leq 2 \sum_{m \in M} \deg(m)$$

2. Hilbert series of $\langle S \rangle$ in $\mathbb{Q}(y)[x]$: $\mathrm{HS}(z) = \sum_{i=0}^{\infty} c_i \cdot z^i$

M from **grevlex**: $c_i = |\{m \in M \mid \deg(m) = i\}|$

$$\mathrm{HS}'(1) = \sum_i i \cdot c_i = \sum_{m \in M} \deg(m)$$

$$\deg(\det H) \leq 2\ \mathrm{HS}'(1)$$

Degree bound & Complexity

[Faugère, Safey El Din, Spaenlehauer '13]

$$\mathrm{HS}(z) = \frac{\det(A(z^{D-1}))}{z^{(D-1)\binom{s-1}{2}}} \frac{(1-z^D)^s(1-z^{D-1})^{n-s}}{(1-z)^n}$$

where $A(z)$ is the $(s-1)\times(s-1)$ matrix whose (i,j)-th entry is $\sum_k \binom{s-i}{k}\binom{n-1-j}{k} z^k$

Degree bound & Complexity

[Faugère, Safey El Din, Spaenlehauer '13]

$$\mathrm{HS}(z) = \frac{\det(A(z^{D-1}))}{z^{(D-1)\binom{s-1}{2}}} \frac{(1-z^D)^s(1-z^{D-1})^{n-s}}{(1-z)^n}$$

where $A(z)$ is the $(s-1)\times(s-1)$ matrix whose (i,j)-th entry is $\sum_k \binom{s-i}{k}\binom{n-1-j}{k} z^k$

Simplification [Berthomieu, Bostan, Ferguson, Safey El Din '21]

$$\mathrm{HS}(z) = (1+\ldots+z^{D-1})^s(1+\ldots+z^{D-2})^{n-s}\sum_{k=0}^{s-1}\binom{n-s-1+k}{k} z^{(D-1)k}$$

Degree bound & Complexity

[Faugère, Safey El Din, Spaenlehauer '13]

$$\mathrm{HS}(z) = \frac{\det(A(z^{D-1}))}{z^{(D-1)\binom{s-1}{2}}} \frac{(1-z^D)^s(1-z^{D-1})^{n-s}}{(1-z)^n}$$

where $A(z)$ is the $(s-1)\times(s-1)$ matrix whose (i,j)-th entry is $\sum_k \binom{s-i}{k}\binom{n-1-j}{k} z^k$

Simplification [Berthomieu, Bostan, Ferguson, Safey El Din '21]

$$\mathrm{HS}(z) = (1+\ldots+z^{D-1})^s(1+\ldots+z^{D-2})^{n-s}\sum_{k=0}^{s-1}\binom{n-s-1+k}{k} z^{(D-1)k}$$

$$\mathrm{HS}'(1) = D^s(D-1)^{n-s}\left((n-s)(D-1)\binom{n-1}{s-2} + \frac{1}{2}(n(D-2)+s)\binom{n-1}{s-1}\right)$$

Experiments

Implemented in Maple with FGb, RAGLib, msolve

Intel Xeon Gold 6244 3.6GHz + 754GB RAM

∞: stopped after 5 days

t	D	HERMITE					MAPLE[RF]			MAPLE[RC]		
		MAT	DET	SP	**total**	DEG	DV	CAD	**total**	BP	RRC	**total**
2	$[2,2]$	.07 s	.01 s	.3 s	**.4 s**	8	.1 s	.3 s	.4 s	.1 s	1 s	1.1 s
2	$[3,2]$	.1 s	.2 s	4.8 s	**5 s**	18	1 m	5 s	1 m	.3 s	12 s	12 s
2	$[2,2,2]$	.3 s	.3 s	33 s	**34 s**	24	17m	32 s	17m	23 s	2 m	2 m
2	$[3,3]$	.3 s	.8 s	3 m	**3 m**	36	2 h	4 m	2 h	8 s	4 m	4 m
3	$[2,2]$	.1 s	.02 s	26 s	**27 s**	8	1 s	35 s	36 s	.2 s	12m	12m
3	$[3,2]$	.2 s	.2 s	3 h	**3 h**	18	2 h	84 h	86 h	3 s	37 h	37 h
3	$[2,2,2]$	.5 s	7 s	32 h	**32 h**	24	∞	∞	∞	20m	∞	∞
3	$[4,2]$	.6 s	12 s	90 h	**90 h**	32	∞	∞	∞	12m	∞	∞
4	$[2,2]$	.2 s	.1 s	8 m	**8 m**	8	4 s	∞	∞	1 s	∞	∞

Random dense systems with $n = s$ (RRC)

t	n	s	MAT+DET	SP	**TOTAL**	DEG	MAPLE[RF]	MAPLE[RC]
3	6	6	1 h.	85 h.	**86 h**	48	∞	∞

Kuramoto model for 4 oscillators

MAT: compute Hermite matrices

DET: compute the minors

SP: compute sample points

DEG: highest degree in the output

RF[DV]: RootFinding[DiscriminantVariety]

RF[CAD]: RootFinding[RRC]

RC[BP]: RegularChains[BorderPolynomial]

RC[RRC]: RegularChains[RRC]

Experiments

t	n	s	MAT+DET	SP	TOTAL	DEG	MAPLE	MATHEMATICA
2	3	2	1 s	6 s	**7 s**	24	∞	∞
2	4	2	9 s	2 m	**2 m**	40	∞	∞
2	5	2	2 m	18 m	**20 m**	56	∞	∞
2	6	2	20 m	2.5 h	**3 h**	72	∞	∞
2	7	2	1.5 h	6.5 h	**8 h**	88	∞	∞
3	3	2	6 s.	2 m.	**2 m**	24	∞	∞
3	4	2	5 m.	20 m.	**25 m**	40	∞	∞
3	5	2	2 h.	8 h.	**10 h**	56	∞	∞
4	3	2	40 s.	30 m.	**30 m**	24	∞	∞
4	4	2	5 h.	45 h.	**50 h**	40	∞	∞

Random dense systems with $D = 2$

D	t	n	s	MAT+DET	SP	TOTAL	DEG	MAPLE	MATHEMATICA
2	3	3	2	3 s.	37 s.	**40 s**	22	∞	∞
2	3	4	2	2 m.	10 m.	**12 m**	34	∞	∞
2	3	5	2	2 m.	10 m.	**12 m**	32	∞	∞
[3, 2]	3	3	2	15 m.	2 h.	**2 h**	48	∞	∞
2	4	3	2	20 s.	20 m.	**21 m**	22	∞	∞
2	4	4	2	15 s.	18 m.	**19 m**	20	∞	∞

Random sparse systems

Conclusions & Perspectives

Conclusions

- New **practical** algorithms for RRC and one-block QE
- **Better** degree bound and complexity results for **generic** inputs
- **Easier evaluation** of formulas using the matrices
- Solve **applications**: Kuramoto model with 4 oscillators

[Kuramoto '75; Harris and Hauenstein '20]

Conclusions & Perspectives

Conclusions

- New **practical** algorithms for RRC and one-block QE
- **Better** degree bound and complexity results for **generic** inputs
- **Easier evaluation** of formulas using the matrices
- Solve **applications**: Kuramoto model with 4 oscillators

[Kuramoto '75; Harris and Hauenstein '20]

Perspectives

- Hermite matrices for computing **totally real hyperplane section**
- Work on the **implementation** to tackle **applications**
- Control the degree of denominators in non-generic case
- Exploit the **structure** of Hermite matrices
- Handle **inequalities**