Computing at least one point per connected components of semi-algebraic sets defined by a single inequality

Edern Gillot

SIAM AG25 – Computational Real Algebraic Geometry

Joint work with Jérémy Berthomieu and Mohab Safey El Din

11 July 2025

Problem Description

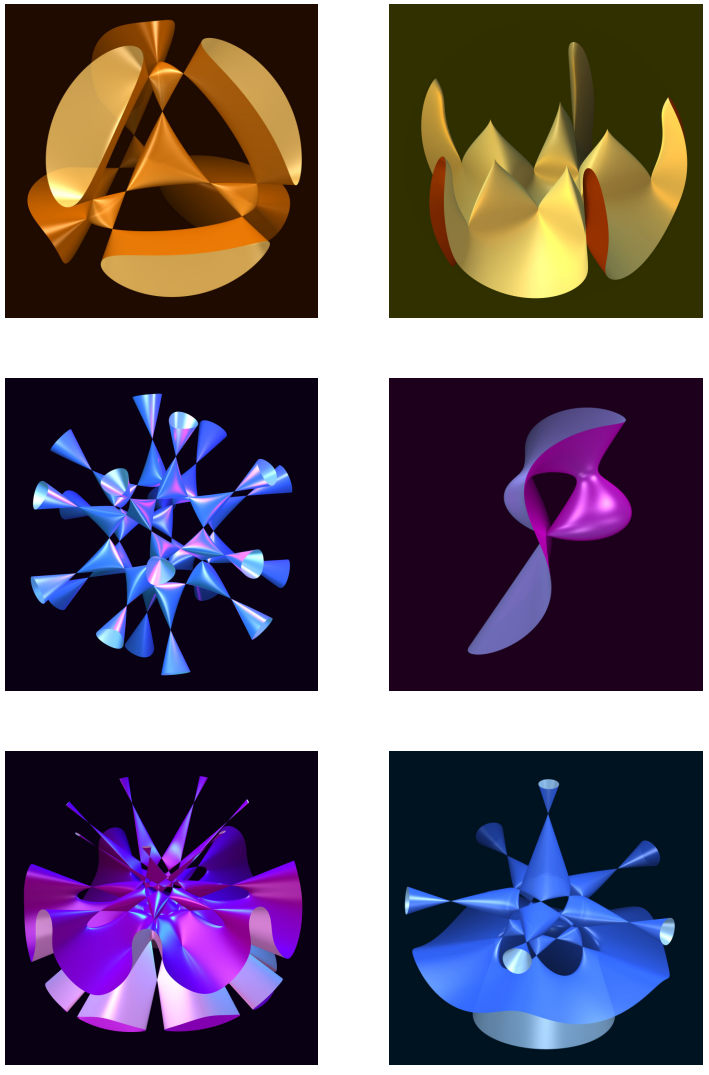
Real polynomial systems
with **constraints**

$$\{\boldsymbol{x} \in \mathbb{R}^n : f_1(\boldsymbol{x}) = \cdots = f_r(\boldsymbol{x}) = 0,$$
$$g_1(\boldsymbol{x}) > 0, \cdots, g_s(\boldsymbol{x}) > 0\}, f_i, g_j \in \mathbb{R}[\boldsymbol{X}]$$

Problem Description

Real polynomial systems
with **constraints**

$$\{\boldsymbol{x} \in \mathbb{R}^n : f_1(\boldsymbol{x}) = \cdots = f_r(\boldsymbol{x}) = 0,$$
$$g_1(\boldsymbol{x}) > 0, \cdots, g_s(\boldsymbol{x}) > 0\}, f_i, g_j \in \mathbb{R}[\boldsymbol{X}]$$



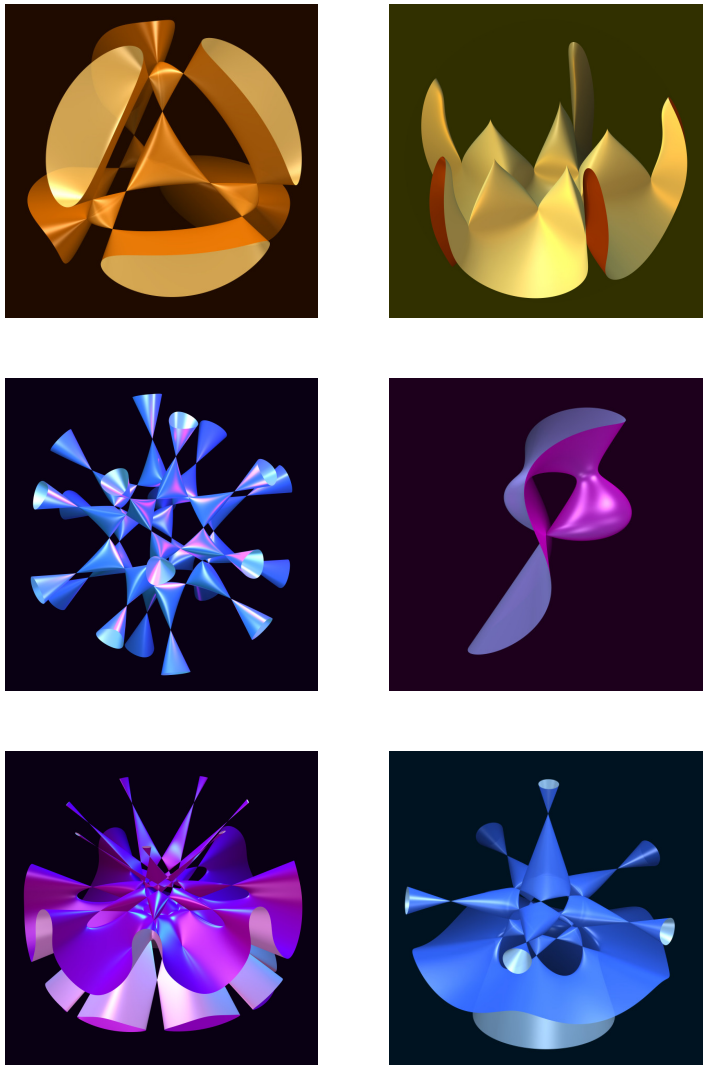
Source: **[IMAGINARY–Labs]**

Problem Description

Real polynomial systems
with **constraints**

$$\{\boldsymbol{x} \in \mathbb{R}^n : f_1(\boldsymbol{x}) = \cdots = f_r(\boldsymbol{x}) = 0,$$
$$g_1(\boldsymbol{x}) > 0, \cdots, g_s(\boldsymbol{x}) > 0\}, f_i, g_j \in \mathbb{R}[\boldsymbol{X}]$$

Existence of solutions?



Source: **[IMAGINARY–Labs]**

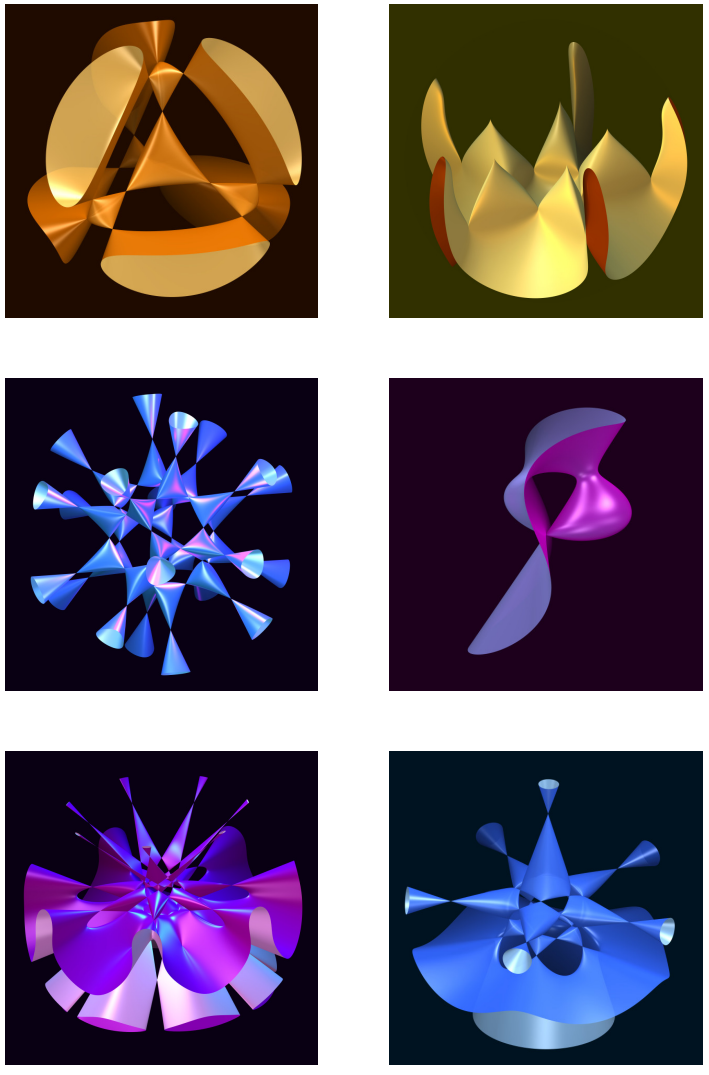
Problem Description

Real polynomial systems with **constraints**

$$\{\boldsymbol{x} \in \mathbb{R}^n : f_1(\boldsymbol{x}) = \cdots = f_r(\boldsymbol{x}) = 0,$$
$$g_1(\boldsymbol{x}) > 0, \cdots, g_s(\boldsymbol{x}) > 0\}, f_i, g_j \in \mathbb{R}[\boldsymbol{X}]$$

Existence of solutions?

NP Hard! [Garey–Johnson 1979]



Source: [IMAGINARY–Labs]

Problem Description

Real polynomial systems with **constraints**

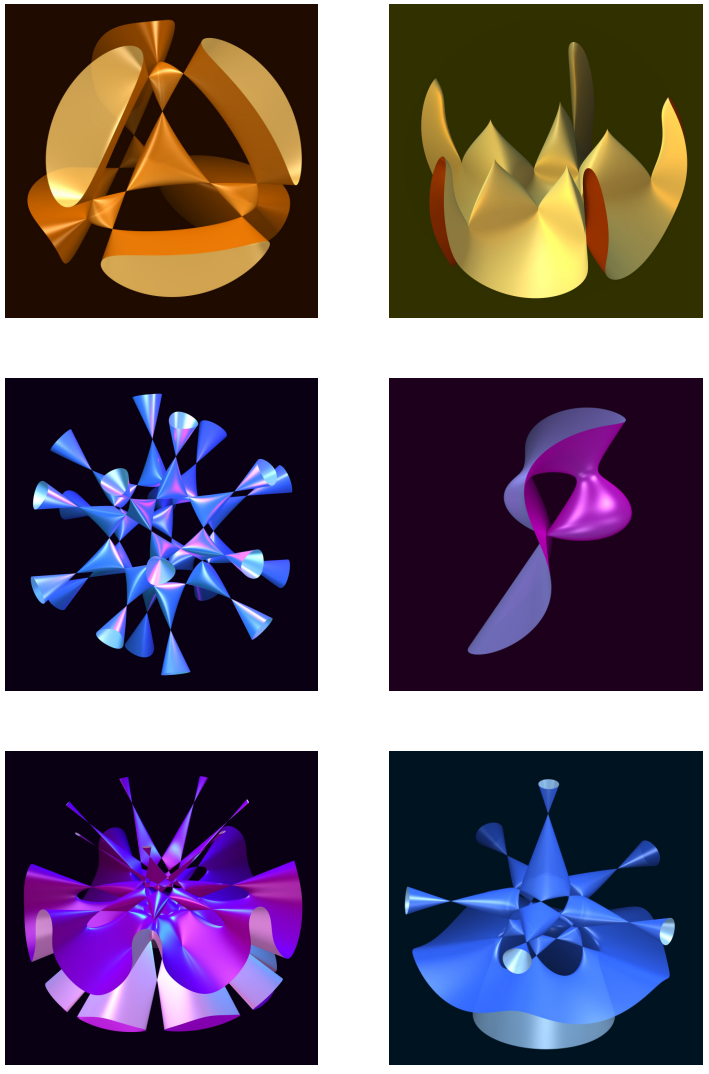
$$\{\boldsymbol{x} \in \mathbb{R}^n : f_1(\boldsymbol{x}) = \cdots = f_r(\boldsymbol{x}) = 0,$$
$$g_1(\boldsymbol{x}) > 0, \cdots, g_s(\boldsymbol{x}) > 0\}, f_i, g_j \in \mathbb{R}[\boldsymbol{X}]$$

Existence of solutions?

NP Hard! [Garey–Johnson 1979]

Finite # of **connected components**

[Tarski 1929, Whitney 1957, Łojasiewicz 1964]



Source: [IMAGINARY–Labs]

Problem Description

Real polynomial systems with **constraints**

$$\{\boldsymbol{x} \in \mathbb{R}^n : f_1(\boldsymbol{x}) = \cdots = f_r(\boldsymbol{x}) = 0,$$
$$g_1(\boldsymbol{x}) > 0, \cdots, g_s(\boldsymbol{x}) > 0\}, f_i, g_j \in \mathbb{R}[\boldsymbol{X}]$$

Existence of solutions?

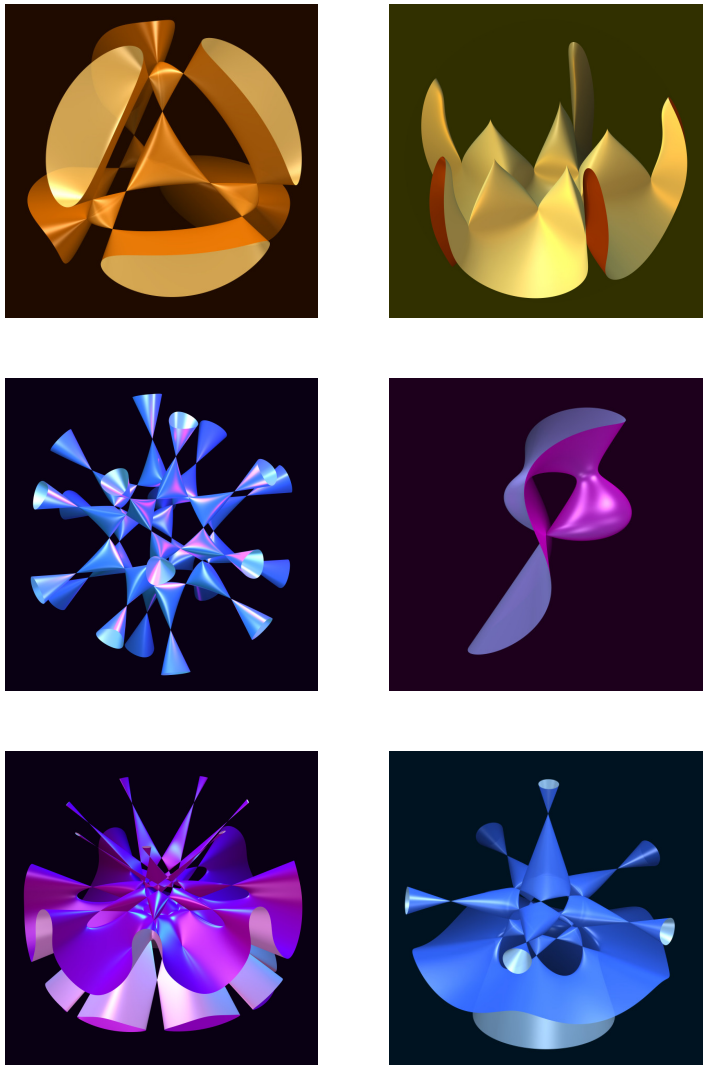
NP Hard! [Garey–Johnson 1979]

Finite # of **connected components**

[Tarski 1929, Whitney 1957, Łojasiewicz 1964]

$\boldsymbol{s^n O(d)^n}$ [Oleinik–Petrovski 1949, Milnor 1964, Thom 1965]

$\boldsymbol{n}$ variables, max degree $\boldsymbol{d}$, $\boldsymbol{s}$ inequalities



Source: [IMAGINARY–Labs]

Problem Description

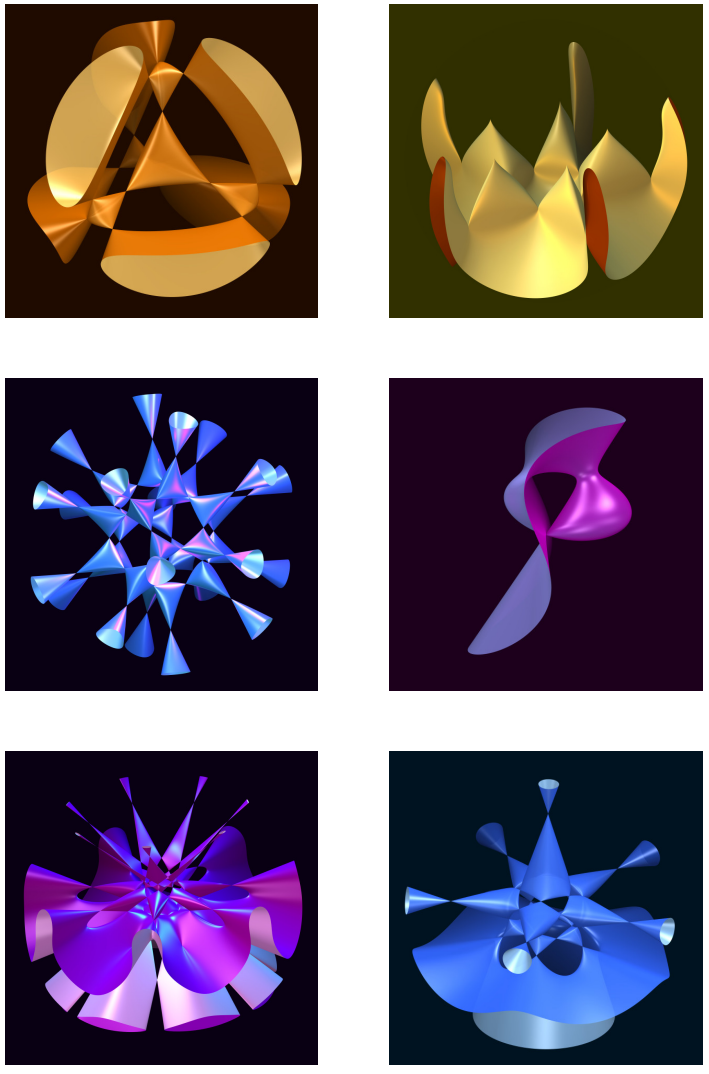
Real polynomial systems with **constraints**

$$\{\boldsymbol{x} \in \mathbb{R}^n : f_1(\boldsymbol{x}) = \cdots = f_r(\boldsymbol{x}) = 0,$$
$$g_1(\boldsymbol{x}) > 0, \cdots, g_s(\boldsymbol{x}) > 0\}, f_i, g_j \in \mathbb{R}[\boldsymbol{X}]$$

Given f_i's, g_j's $\in \mathbb{Q}[x_1, \ldots, x_n]$, $\rightarrow$ **at least** one point per **connected component**

$\boldsymbol{s^n O(d)^n}$ [Oleinik–Petrovski 1949, Milnor 1964, Thom 1965]

$\boldsymbol{n}$ variables, max degree $\boldsymbol{d}$, $\boldsymbol{s}$ inequalities



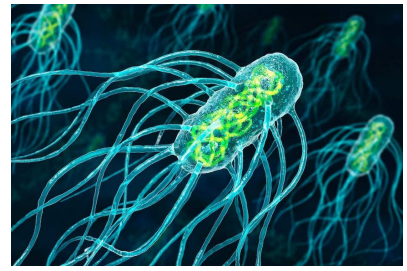
Source: [IMAGINARY–Labs]

Problem Description

Given f_i's, g_j's $\in \mathbb{Q}[x_1, \ldots, x_n]$, $\rightarrow$ **at least** one point per **connected component**

Problem Description

Given f_i's, g_j's $\in \mathbb{Q}[x_1, \ldots, x_n]$, $\rightarrow$ **at least** one point per **connected component**



Applications:

Robotics [Chablat–Prébet–Safey El Din–Salunkhe–Wenger 2022]

[Capco–Safey El Din–Schicho 2023]

Biology [Feliu–Sadeghimanesh 2022]

[Yabo–Safey El Din–Caillau–Gouzé 2023]

Optimisation [Greuet–Safey El Din 2014] [Ferguson 2022]

Program Verification

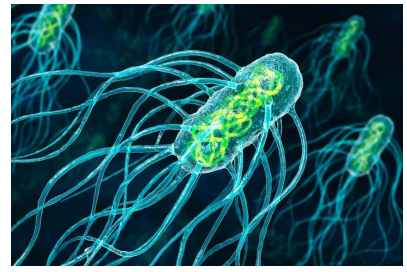
[Goharshady–Hitarth–Mohammadi–Motwani 2023]

[Bayarmagnai–Mohammadi–Prébet 2024] [Maaz–Strzeboński 2025]

Combinatorics [Kauers–Pillwein 2010] [Ibrahim–Salvy 2024]

Problem Description

Given f_i's, g_j's $\in \mathbb{Q}[x_1, \ldots, x_n]$, $\rightarrow$ **at least** one point per **connected component**



Applications:

Robotics [Chablat–Prébet–Safey El Din–Salunkhe–Wenger 2022]

[Capco–Safey El Din–Schicho 2023]

Biology [Feliu–Sadeghimanesh 2022]

[Yabo–Safey El Din–Caillau–Gouzé 2023]

Optimisation [Greuet–Safey El Din 2014] [Ferguson 2022]

Program Verification

[Goharshady–Hitarth–Mohammadi–Motwani 2023]

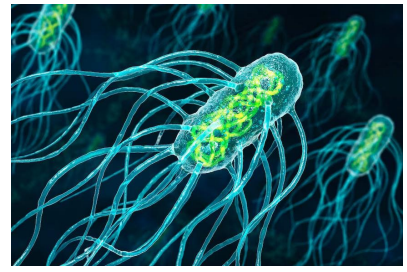
[Bayarmagnai–Mohammadi–Prébet 2024] [Maaz–Strzeboński 2025]

Combinatorics [Kauers–Pillwein 2010] [Ibrahim–Salvy 2024]

Make use of **inherent structure**

Problem Description

Given f_i's, g_j's $\in \mathbb{Q}[x_1, \ldots, x_n]$, $\rightarrow$ **at least** one point per **connected component**



Applications:

Robotics [Chablat–Prébet–Safey El Din–Salunkhe–Wenger 2022]

[Capco–Safey El Din–Schicho 2023]

Biology [Feliu–Sadeghimanesh 2022]

[Yabo–Safey El Din–Caillau–Gouzé 2023]

Optimisation [Greuet–Safey El Din 2014] [Ferguson 2022]

Program Verification

[Goharshady–Hitarth–Mohammadi–Motwani 2023]

[Bayarmagnai–Mohammadi–Prébet 2024] [Maaz–Strzeboński 2025]

Combinatorics [Kauers–Pillwein 2010] [Ibrahim–Salvy 2024]

Make use of **inherent structure**

Single inequality:

$$S = \{\boldsymbol{x} \in \mathbb{R}^n : f(\boldsymbol{x}) \neq 0\}$$

State-of-the-Art

n variables, degree d, bitsize τ, Thom–Milnor bound $O(d)^n$

First algorithm: [Tarski 1951] not elementary recursive

State-of-the-Art

n variables, degree d, bitsize τ, Thom–Milnor bound $O(d)^n$

First algorithm: [Tarski 1951] not elementary recursive

CAD [Collins 1975]

State-of-the-Art

n variables, degree d, bitsize τ, Thom–Milnor bound $O(d)^n$

First algorithm: [Tarski 1951] not elementary recursive

$n \leq 4$ ← **CAD** [Collins 1975]

Bit complexity: $\tau d^{2^{O(n)}}$

State-of-the-Art

n variables, degree d, bitsize τ, Thom–Milnor bound $O(d)^n$

First algorithm: [Tarski 1951] not elementary recursive

$n \leq 4$ ← **CAD** [Collins 1975]

Bit complexity: $\tau d^{2^{O(n)}}$

Deterministic algorithms

[Grigoriev–Vorobjov 1988] [Renegar 1992]
[Canny–Grigoriev–Vorobjov 1992]
[Heintz–Roy–Solernó 1994]
[Basu–Pollack–Roy 1996/2006]...

State-of-the-Art

n variables, degree d, bitsize τ, Thom–Milnor bound $O(d)^n$

First algorithm: [Tarski 1951] not elementary recursive

$n \leq 4$ ← **CAD** [Collins 1975]

Bit complexity: $\tau d^{2^{O(n)}}$

Deterministic algorithms

[Grigoriev–Vorobjov 1988] [Renegar 1992]
[Canny–Grigoriev–Vorobjov 1992]
[Heintz–Roy–Solernó 1994]
[Basu–Pollack–Roy 1996/2006]...

Bit complexity: $\tau d^{O(n)}$
Constant too large

Critical points & **Polar** varieties

State-of-the-Art

n variables, degree d, bitsize τ, Thom–Milnor bound $O(d)^n$

First algorithm: [Tarski 1951] not elementary recursive

$n \leq 4$ ← **CAD** [Collins 1975]

Bit complexity: $\tau d^{2^{O(n)}}$

Deterministic algorithms

[Grigoriev–Vorobjov 1988] [Renegar 1992]
[Canny–Grigoriev–Vorobjov 1992]
[Heintz–Roy–Solernó 1994]
[Basu–Pollack–Roy 1996/2006]...

Bit complexity: $\tau d^{O(n)}$
Constant too large

Critical points & **Polar** varieties

Probabilistic algorithms

[Bank–Giusti–Heintz–Mandel–Mbakop 1997] [Safey El Din–Schost 2003]
[Bank–Giusti–Heintz–Pardo 2004/2009]
[Bank–Giusti–Heintz–Safey El Din–Schost 2010]
[Bank–Gisuti–Heintz–Lecref–Matera–Solerno 2015] [Le–Safey El Din 2021]
[Elliott–Giesbrecht–Schost 2020/2023] [Harris–Hauenstein–Szanto 2023]...

State-of-the-Art

n variables, degree d, bitsize τ, Thom–Milnor bound $O(d)^n$

Current arithmetic complexity:

$$\widetilde{O}\Big(\mathcal{P}(n)d^2(d-1)^{2n}\Big)$$

[Le–Safey El Din 2021]

Current bit complexity:

$$\widetilde{O}\Big(\tau\mathcal{P}(n)d^{3n+4}\Big)$$

[Safey El Din–Schost 2003]
[Elliott–Giesbrecht–Schost 2023]

Do **not** involve degree structure of f, **general** bounds

State-of-the-Art

n variables, degree d, bitsize τ, Thom–Milnor bound $O(d)^n$

Current arithmetic complexity:

$$\widetilde{O}\Big(\mathcal{P}(n)d^2(d-1)^{2n}\Big)$$

[Le–Safey El Din 2021]

Current bit complexity:

$$\widetilde{O}\Big(\tau\mathcal{P}(n)d^{3n+4}\Big)$$

[Safey El Din–Schost 2003]
[Elliott–Giesbrecht–Schost 2023]

Do **not** involve degree structure of f, **general** bounds

Taking **structure** into account for **bit** complexity

[Labahn–Neiger–Vu–Zhou 2022] [Basu–Perrucci 2023]
[Faugère–Labahn–Safey El Din–Schost–Vu 2023]

State-of-the-Art

n variables, degree d, bitsize τ, Thom–Milnor bound $O(d)^n$

Current arithmetic complexity:
$\widetilde{O}\left(\mathcal{P}(n)d^2(d-1)^{2n}\right)$
[Le–Safey El Din 2021]

Current bit complexity:
$\widetilde{O}\left(\tau\mathcal{P}(n)d^{3n+4}\right)$
[Safey El Din–Schost 2003]
[Elliott–Giesbrecht–Schost 2023]

Do **not** involve degree structure of f, **general** bounds

Genericity assumptions on f

Taking **structure** into account for **bit** complexity

[Labahn–Neiger–Vu–Zhou 2022] [Basu–Perrucci 2023]
[Faugère–Labahn–Safey El Din–Schost–Vu 2023]

Algebraic to **semi-algebraic**
$f \neq 0 \to \lambda f - 1 = 0$

More variables & **breaks** structure

Contributions

Input: $f \in \mathbb{Q}[x_1, \ldots, x_n]$, $0 < \epsilon < 1$

Output: **parametrisation** of finite set of points with probability **at least** $1 - \epsilon$

Contributions

Input: $f \in \mathbb{Q}[x_1, \ldots, x_n]$, $0 < \epsilon < 1$

New Bit Complexity:

If $V(f)$ **smooth**:

$$\widetilde{O}\left(\tau \mathcal{P}(n, \log(1/\epsilon)) \mathfrak{D}^3\right)$$

If $V(f)$ **singular**:

$$\widetilde{O}\left(\tau \mathcal{P}(n, \log(1/\epsilon)) \mathfrak{D}^5\right)$$

$\mathfrak{D}$ encapsulates **degree structure**

Output: **parametrisation** of finite set of points with probability **at least** $1 - \epsilon$

$$\mathfrak{D} := \deg(f) \prod_{i=1}^{n} \deg\left(\frac{\partial f}{\partial X_i}\right)$$

$$\mathfrak{D} \leq d(d-1)^n$$

Contributions

Input: $f \in \mathbb{Q}[x_1, \ldots, x_n]$, $0 < \epsilon < 1$

Output: **parametrisation** of finite set of points with probability **at least** $1 - \epsilon$

New Bit Complexity:

If $V(f)$ **smooth**:

$$\widetilde{O}\left(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^3\right)$$

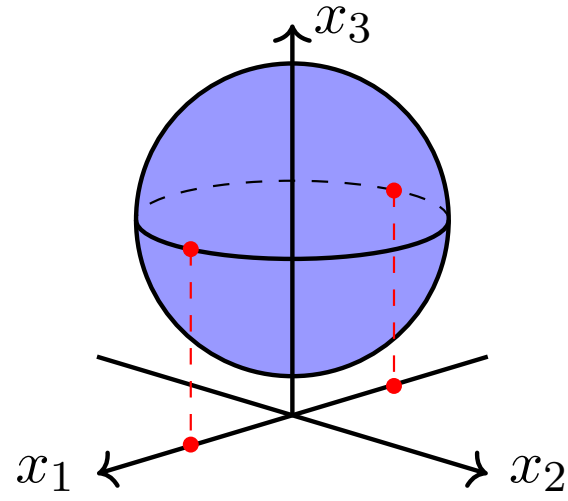
If $V(f)$ **singular**:

$$\widetilde{O}\left(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^5\right)$$

$$\mathfrak{D} := \deg(f) \prod_{i=1}^{n} \deg\left(\frac{\partial f}{\partial X_i}\right)$$

$$\mathfrak{D} \leq d(d-1)^n$$

$\mathfrak{D}$ encapsulates **degree structure**



Contributions

Input: $f \in \mathbb{Q}[x_1, \ldots, x_n]$, $0 < \epsilon < 1$

Output: **parametrisation** of finite set of points with probability **at least** $1 - \epsilon$

New Bit Complexity:

If $V(f)$ **smooth**:

$$\widetilde{O}\left(\tau \mathcal{P}(n, \log(1/\epsilon)) \mathfrak{D}^3\right)$$

If $V(f)$ **singular**:

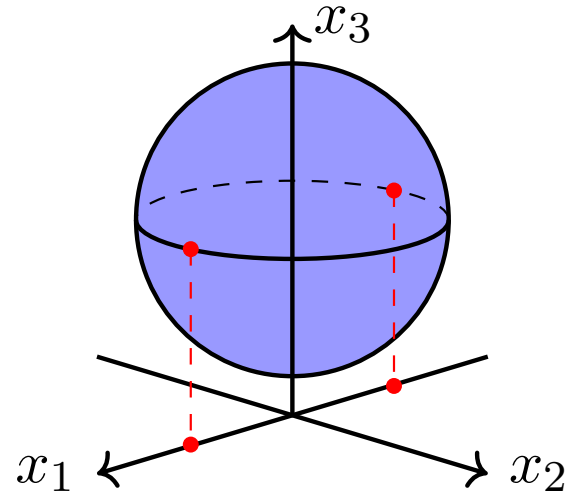
$$\widetilde{O}\left(\tau \mathcal{P}(n, \log(1/\epsilon)) \mathfrak{D}^5\right)$$

$$\mathfrak{D} := \deg(f) \prod_{i=1}^{n} \deg\left(\frac{\partial f}{\partial X_i}\right)$$

$$\mathfrak{D} \leq d(d-1)^n$$

$\mathfrak{D}$ encapsulates **degree structure**

Critical points are defined by **partial derivatives**



Singular points **always** satisfy critical point equations

Smooth Case — Change of Variables

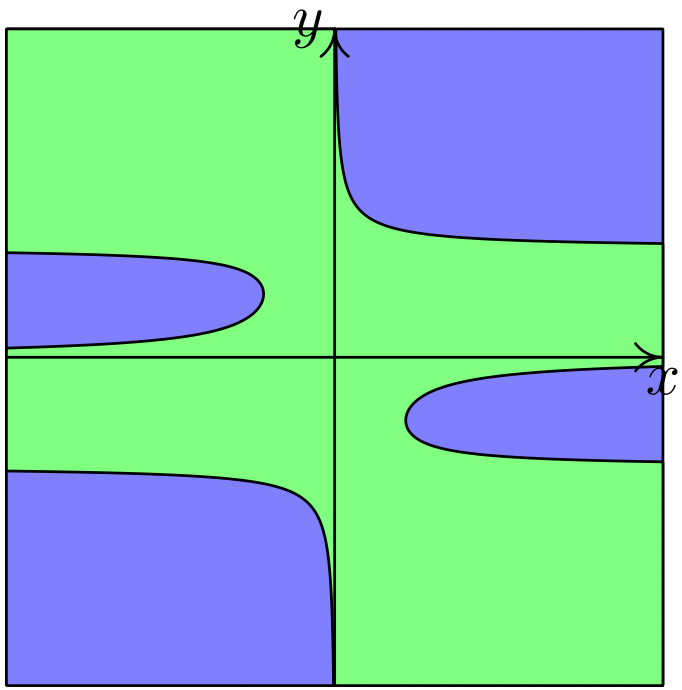
Random change of variables

Properness of projection on x-axis

Smooth Case — Change of Variables

Random change of variables

Properness of projection on x-axis

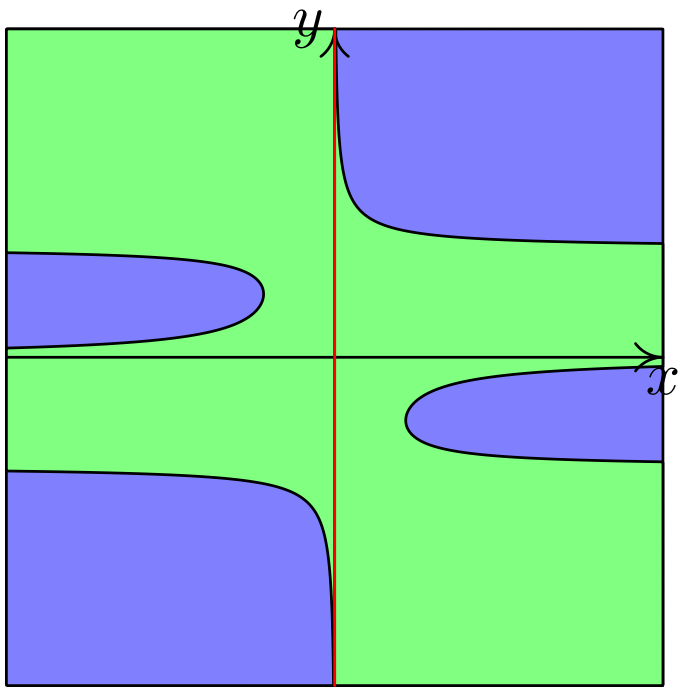


$$f = 4x(y^3 - y) - 1 \neq 0$$

Smooth Case — Change of Variables

Random change of variables

Properness of projection on x-axis

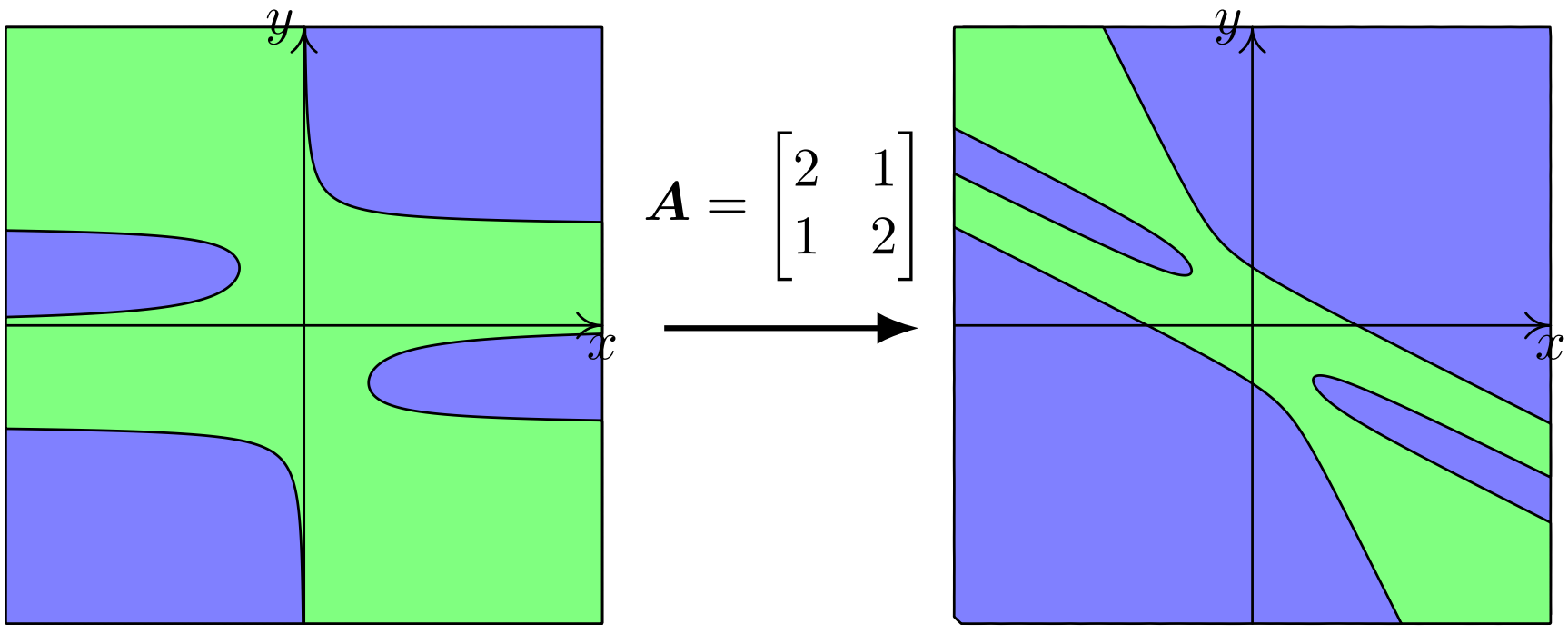


$$f = 4x(y^3 - y) - 1 \neq 0$$

Smooth Case — Change of Variables

Random change of variables

Properness of projection on x-axis



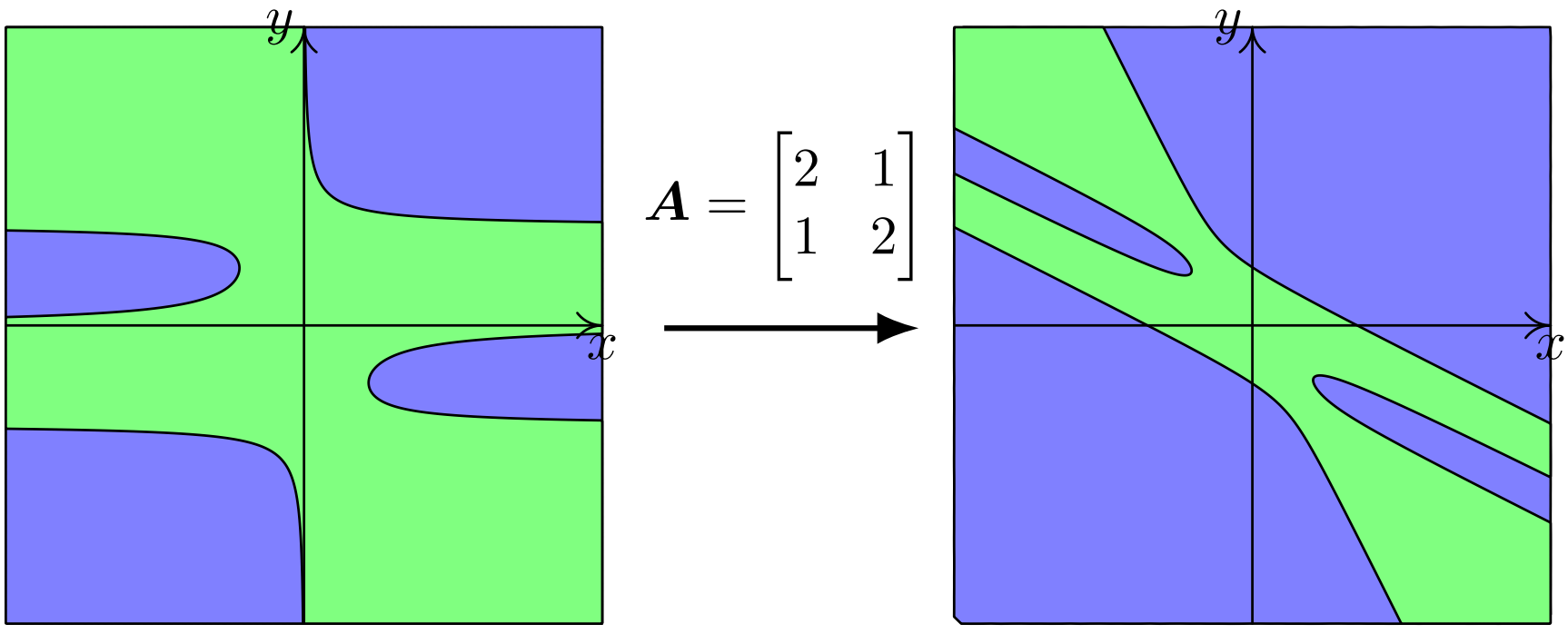
$f = 4x(y^3 - y) - 1 \neq 0$

$f^{\boldsymbol{A}} := f(\boldsymbol{A}(x, y)^T) \neq 0$

Smooth Case — Change of Variables

Random change of variables

Properness of projection on x-axis



$f = 4x(y^3 - y) - 1 \neq 0$

$f^{\boldsymbol{A}} := f(\boldsymbol{A}(x, y)^T) \neq 0$

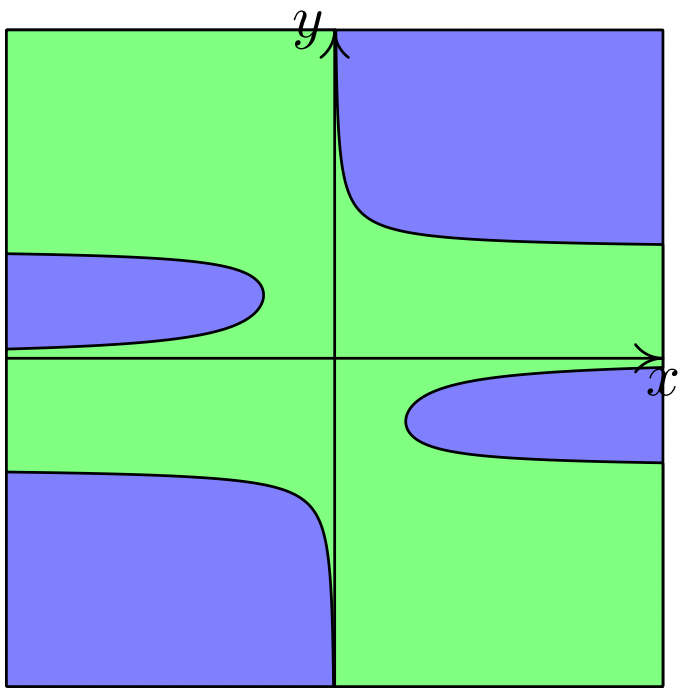
Generic $\boldsymbol{A} \implies$ projection of $V(f^{\boldsymbol{A}})$ on x-axis is **closed** and has **finite** fibres

[Safey El Din–Schost 2003]

Smooth Case — Change of Variables

Random change of variables

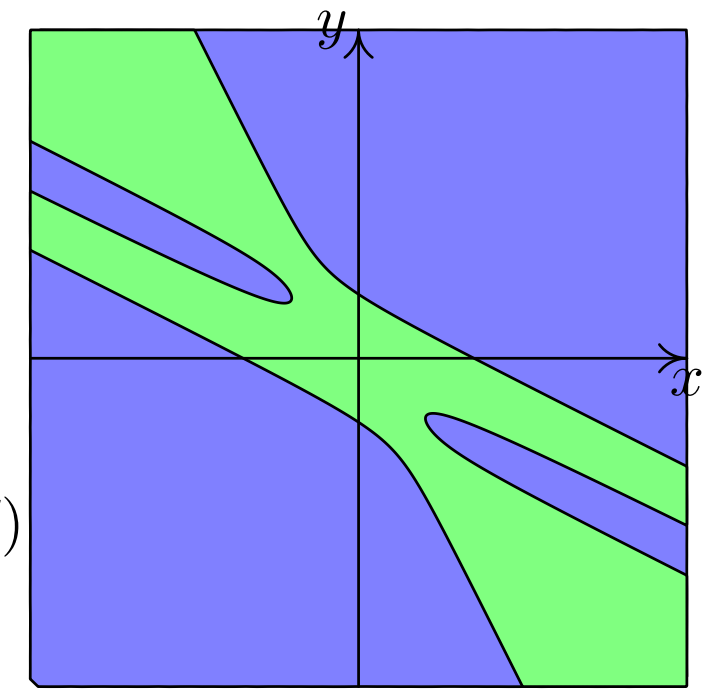
Properness of projection on x-axis



$$f = 4x(y^3 - y) - 1 \neq 0$$

$$\boldsymbol{A} = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

$$\log(\boldsymbol{A}_{ij}) \in \widetilde{O}(n + \log(d) + \log(1/\epsilon))$$



$$f^{\boldsymbol{A}} := f(\boldsymbol{A}(x, y)^T) \neq 0$$

Generic $\boldsymbol{A} \implies$ projection of $V(f^{\boldsymbol{A}})$ on x-axis is **closed** and has **finite** fibres

[Safey El Din–Schost 2003]

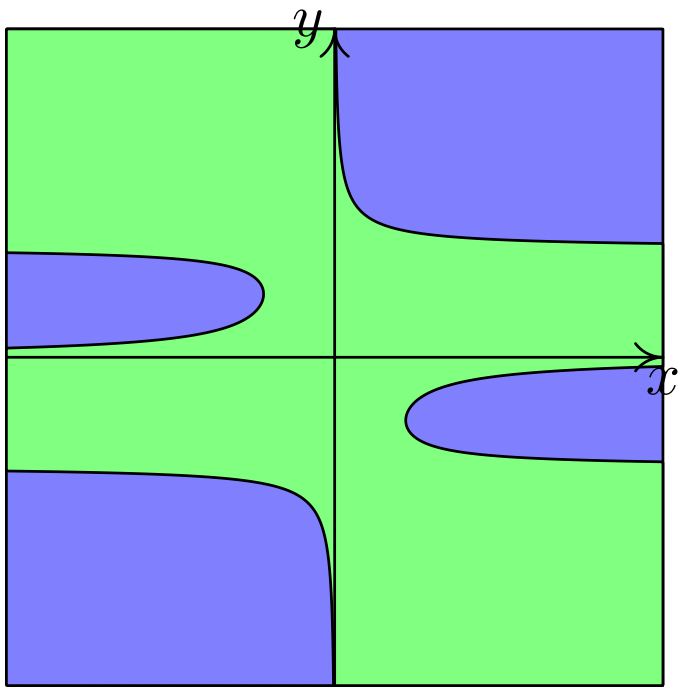
Probability of choosing a **good** $\boldsymbol{A}$: $\geq 1 - \epsilon/3$

[Elliott–Giesbrecht–Schost 2020/2023]

Smooth Case — Change of Variables

Random change of variables

Properness of projection on x-axis

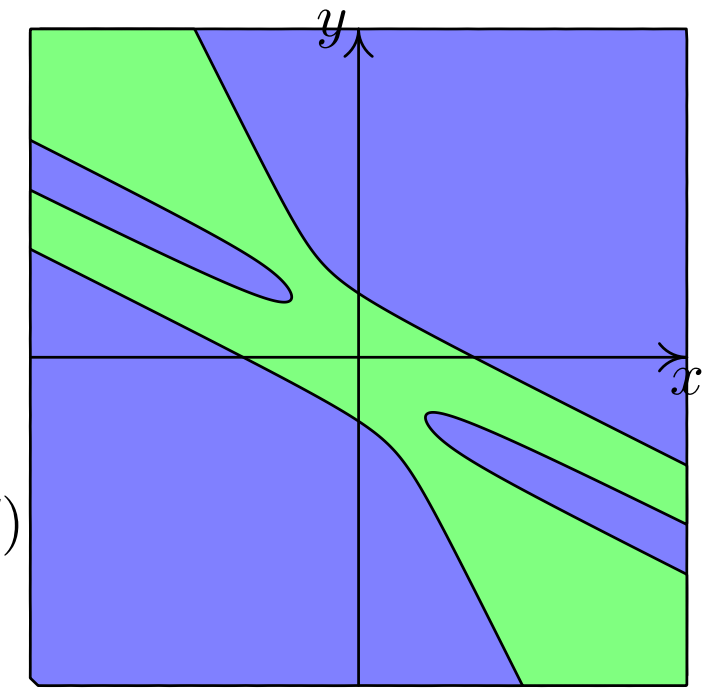


$$f = 4x(y^3 - y) - 1 \neq 0$$

$$\boldsymbol{A} = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

$$\log(\boldsymbol{A}_{ij}) \in \widetilde{O}(n + \log(d) + \log(1/\epsilon))$$

No τ



$$f^{\boldsymbol{A}} := f(\boldsymbol{A}(x, y)^T) \neq 0$$

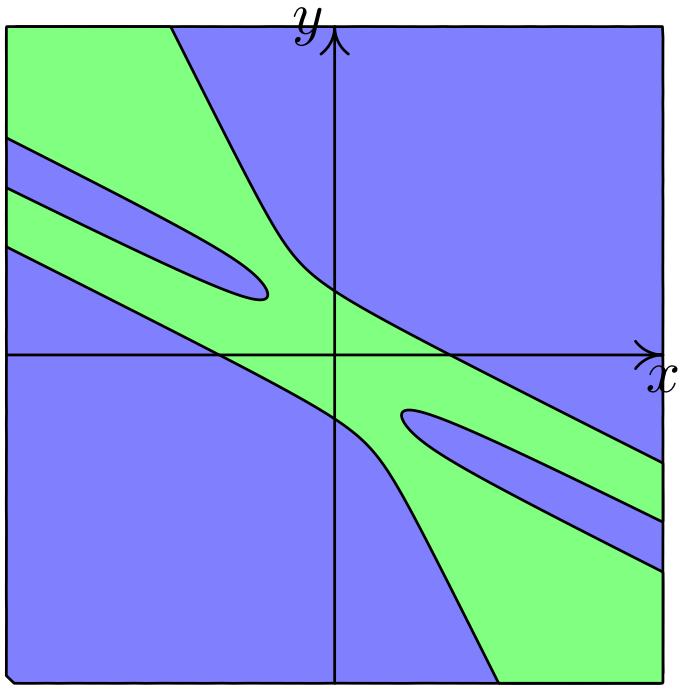
Generic $\boldsymbol{A}$ $\implies$ projection of $V(f^{\boldsymbol{A}})$ on x-axis is **closed** and has **finite** fibres

[Safey El Din–Schost 2003]

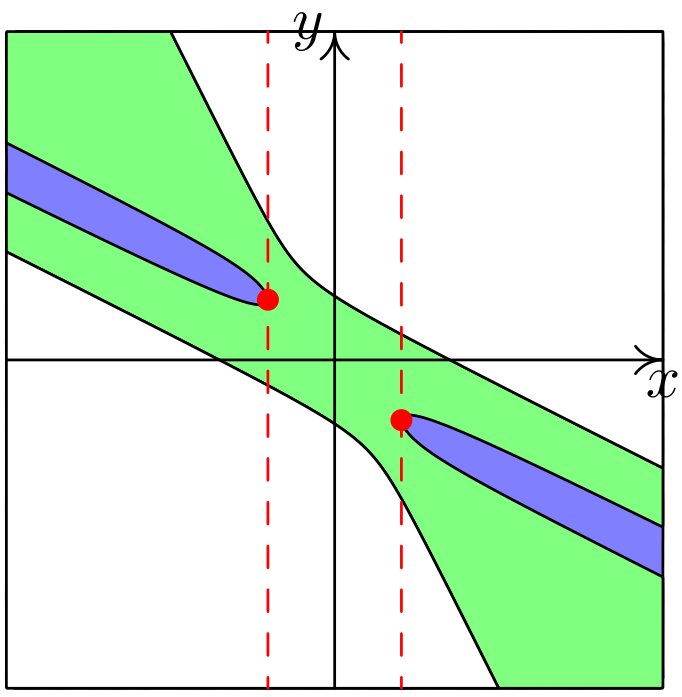
Probability of choosing a **good $\boldsymbol{A}$**: $\geq 1 - \epsilon/3$

[Elliott–Giesbrecht–Schost 2020/2023]

Smooth Case — Critical Points

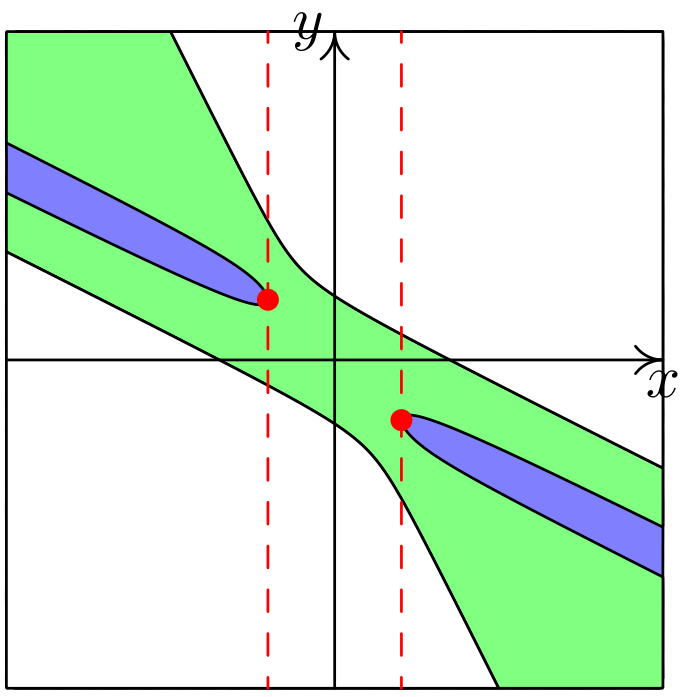


Smooth Case — Critical Points



$$f^{\boldsymbol{A}} = \frac{\partial f^{\boldsymbol{A}}}{\partial x_2} = \cdots = \frac{\partial f^{\boldsymbol{A}}}{\partial x_n} = 0$$

Smooth Case — Critical Points



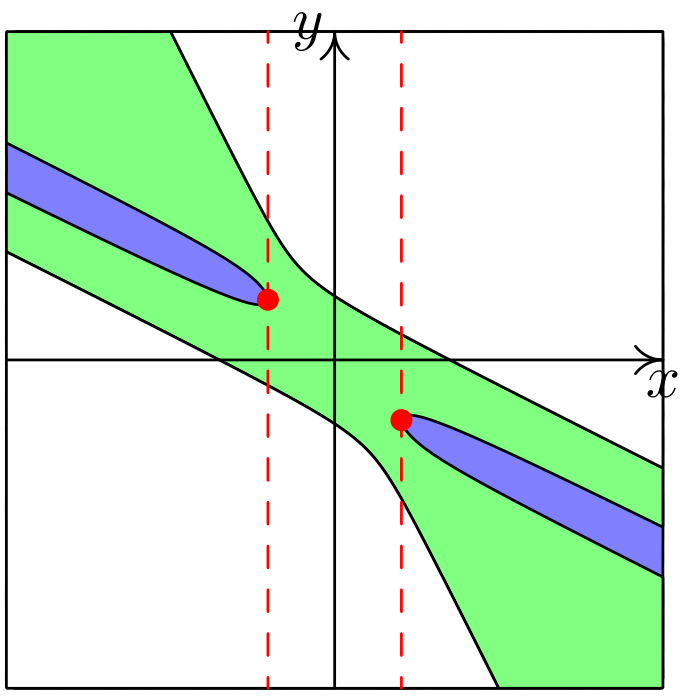
$$f^{\boldsymbol{A}} = \frac{\partial f^{\boldsymbol{A}}}{\partial x_2} = \cdots = \frac{\partial f^{\boldsymbol{A}}}{\partial x_n} = 0$$

Bit cost for computing **parametrisation** of solutions:

quadratic in $\deg(f^{\boldsymbol{A}}) \prod_{i=2}^{n} \deg\left(\frac{\partial f^{\boldsymbol{A}}}{\partial X_i}\right)$

[Safey El Din–Schost 2018]

Smooth Case — Critical Points



$$f^{\boldsymbol{A}} = \frac{\partial f^{\boldsymbol{A}}}{\partial x_2} = \cdots = \frac{\partial f^{\boldsymbol{A}}}{\partial x_n} = 0$$

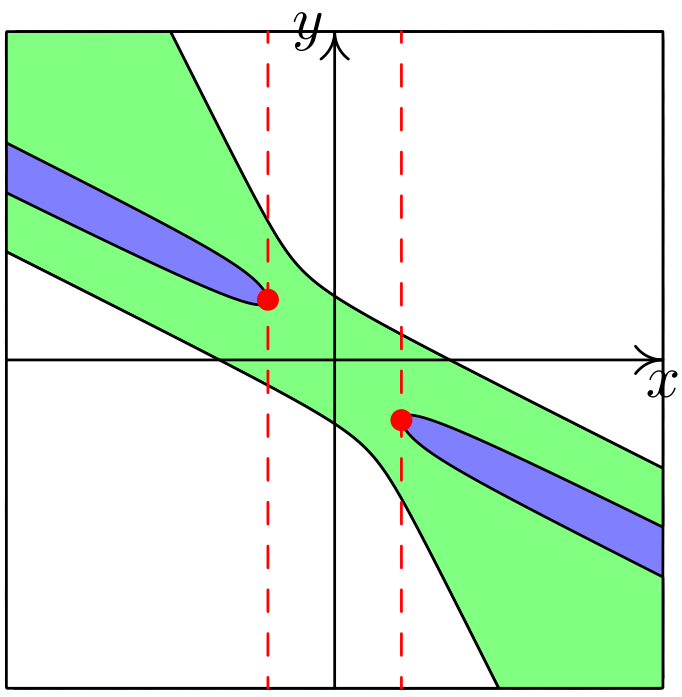
Bit cost for computing **parametrisation** of solutions:

quadratic in $\deg(f^{\boldsymbol{A}}) \prod_{i=2}^{n} \deg\left(\frac{\partial f^{\boldsymbol{A}}}{\partial X_i}\right)$

[Safey El Din–Schost 2018]

A breaks structure!

Smooth Case — Critical Points



$$f^{\boldsymbol{A}} = \frac{\partial f^{\boldsymbol{A}}}{\partial x_2} = \cdots = \frac{\partial f^{\boldsymbol{A}}}{\partial x_n} = 0$$

Bit cost for computing **parametrisation** of solutions:

quadratic in $\deg(f^{\boldsymbol{A}}) \prod_{i=2}^{n} \deg\left(\frac{\partial f^{\boldsymbol{A}}}{\partial X_i}\right)$

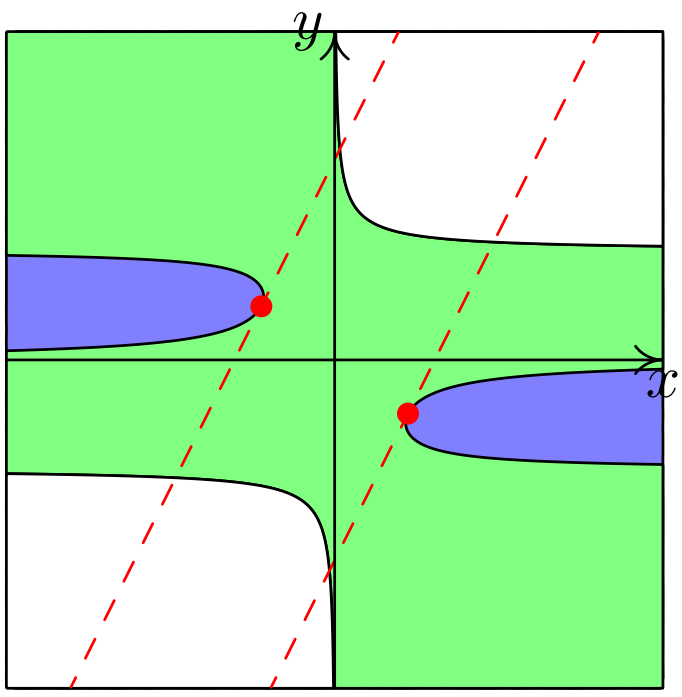
[Safey El Din–Schost 2018]

***A* breaks structure!**

$\exists g_2, \ldots, g_n \in \mathbb{Q}[x_1, \ldots, x_n] : \deg(g_i) = \deg\left(\frac{\partial f}{\partial X_i}\right)$ such that

$\boldsymbol{\xi}$ critical $\iff$ $\boldsymbol{A\xi} \in V(f, g_2, \ldots, g_n)$

Smooth Case — Critical Points



$$f^{\boldsymbol{A}} = \frac{\partial f^{\boldsymbol{A}}}{\partial x_2} = \cdots = \frac{\partial f^{\boldsymbol{A}}}{\partial x_n} = 0$$

Bit cost for computing **parametrisation** of solutions:

quadratic in $\deg(f^{\boldsymbol{A}}) \prod_{i=2}^{n} \deg\left(\frac{\partial f^{\boldsymbol{A}}}{\partial X_i}\right)$

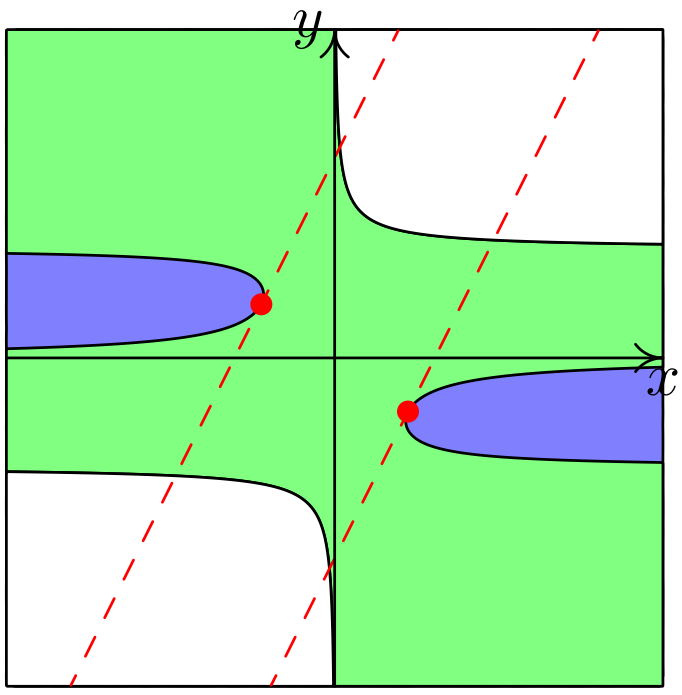
[Safey El Din–Schost 2018]

A breaks structure!

$\exists g_2, \ldots, g_n \in \mathbb{Q}[x_1, \ldots, x_n] : \deg(g_i) = \deg\left(\frac{\partial f}{\partial X_i}\right)$ such that

$\boldsymbol{\xi}$ critical $\iff$ $\boldsymbol{A\xi} \in V(f, g_2, \ldots, g_n)$

Smooth Case — Critical Points



$$f^{\boldsymbol{A}} = \frac{\partial f^{\boldsymbol{A}}}{\partial x_2} = \cdots = \frac{\partial f^{\boldsymbol{A}}}{\partial x_n} = 0$$

Bit cost for computing **parametrisation** of solutions:

quadratic in $\deg(f^{\boldsymbol{A}}) \prod_{i=2}^{n} \deg\left(\frac{\partial f^{\boldsymbol{A}}}{\partial X_i}\right)$

[Safey El Din–Schost 2018]

$\boldsymbol{A}$ **breaks structure!**

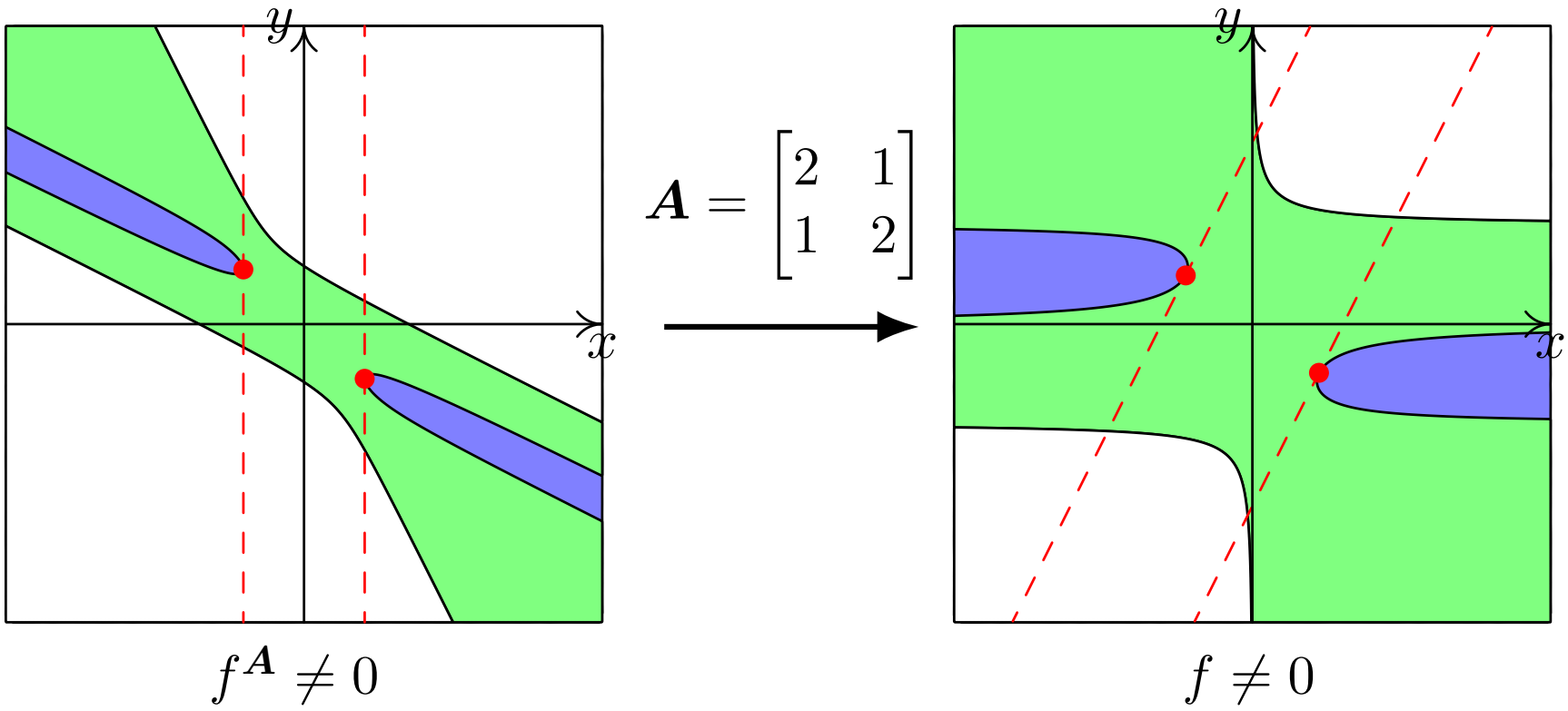
$\exists g_2, \ldots, g_n \in \mathbb{Q}[x_1, \ldots, x_n] : \deg(g_i) = \deg\left(\frac{\partial f}{\partial X_i}\right)$ such that

$\boldsymbol{\xi}$ critical $\iff$ $\boldsymbol{A\xi} \in V(f, g_2, \ldots, g_n)$

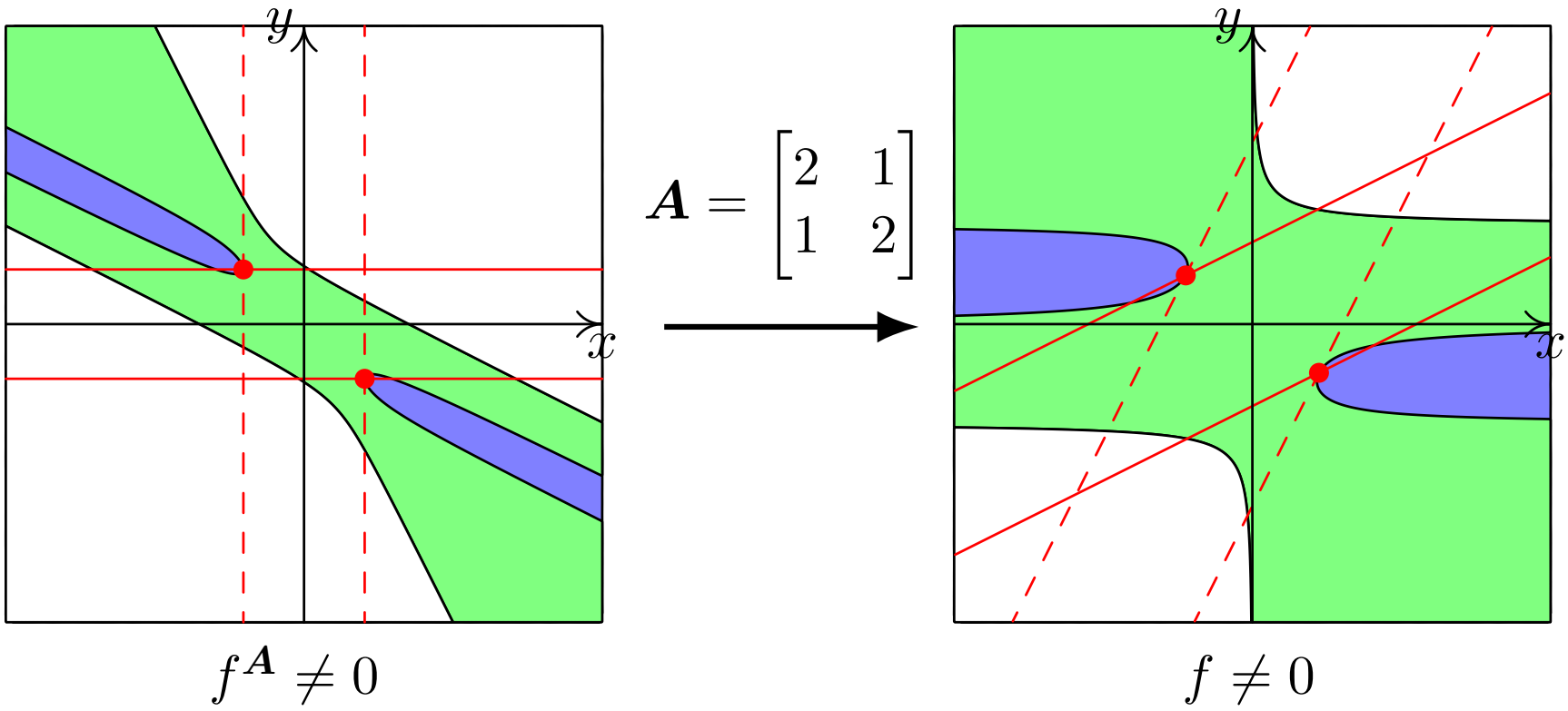
Bit cost for computing these points: $\widetilde{O}((\tau + \log(1/\epsilon))\mathcal{P}(n)\mathfrak{D}^2)$

Probability of success $\geq 1 - \epsilon/3$ after $O(\log(1/\epsilon))$ attempts

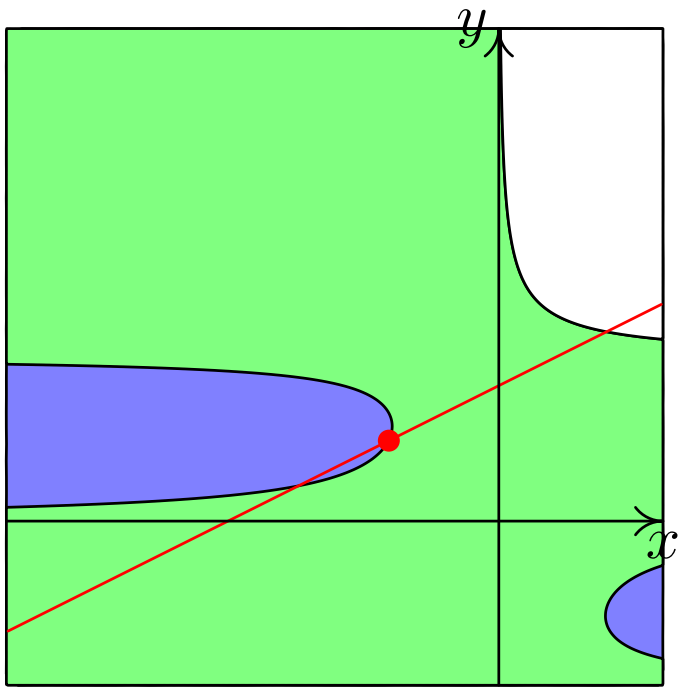
Smooth Case — Transverse Line



Smooth Case — Transverse Line

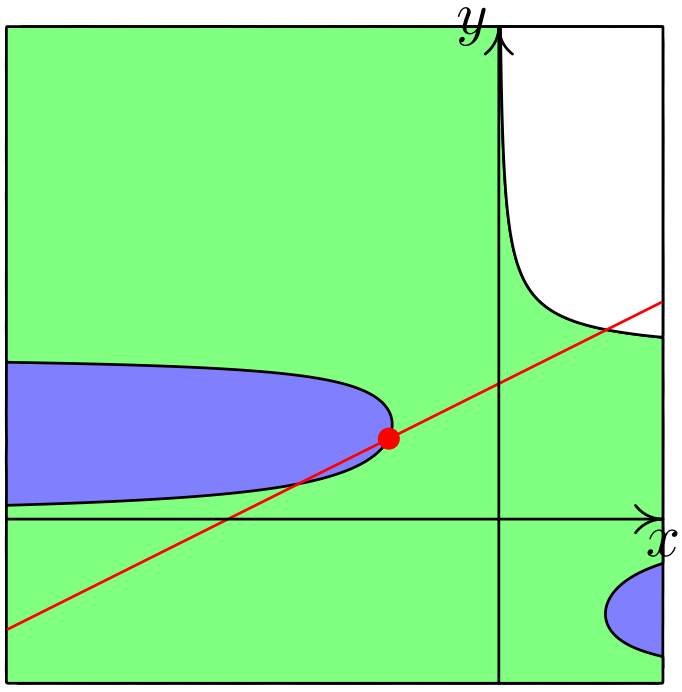


Smooth Case — Transverse Line



$f \neq 0$

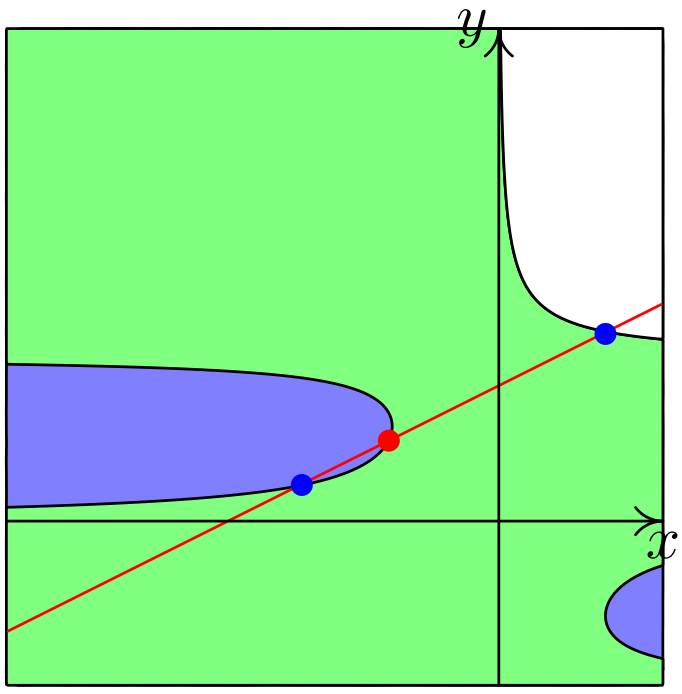
Smooth Case — Transverse Line



$f \neq 0$

Minimal distance between **computed solution point** and other **intersection points**

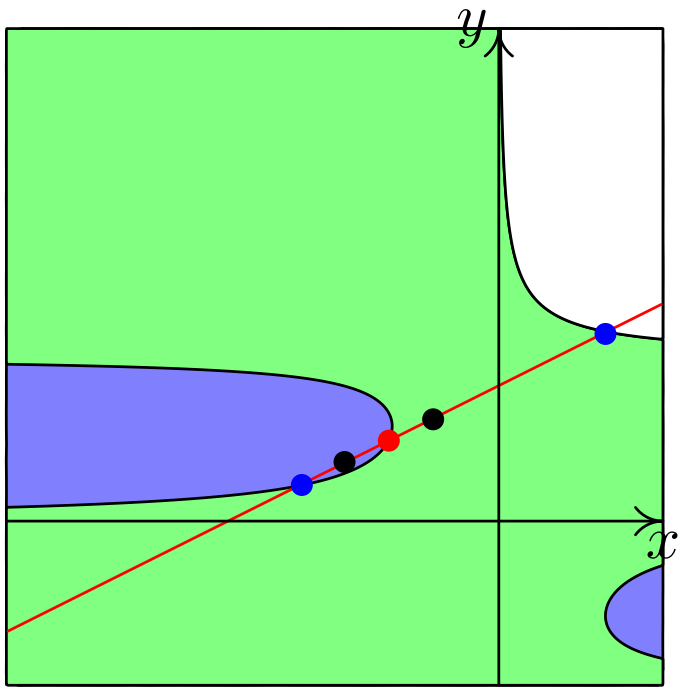
Smooth Case — Transverse Line



$f \neq 0$

Minimal distance between **computed solution point** and other **intersection points**

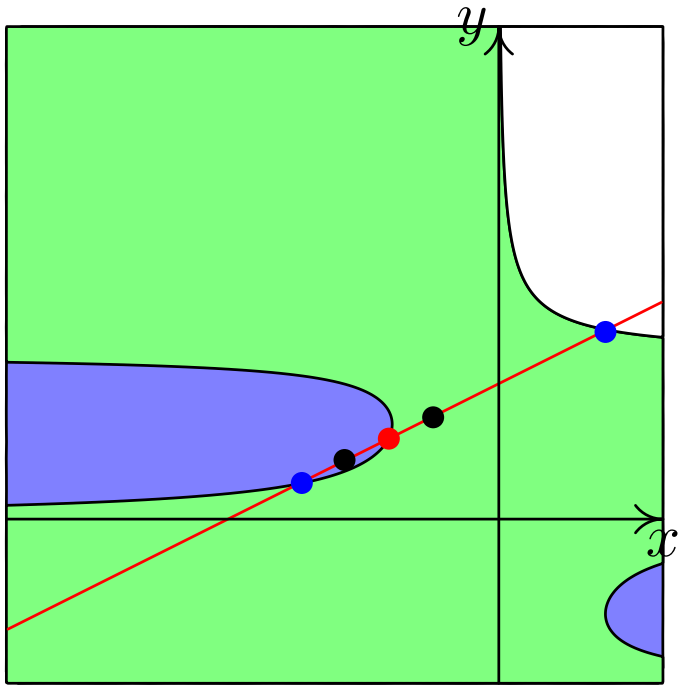
Smooth Case — Transverse Line



$f \neq 0$

Minimal distance between **computed solution point** and other **intersection points**

Smooth Case — Transverse Line



$f \neq 0$

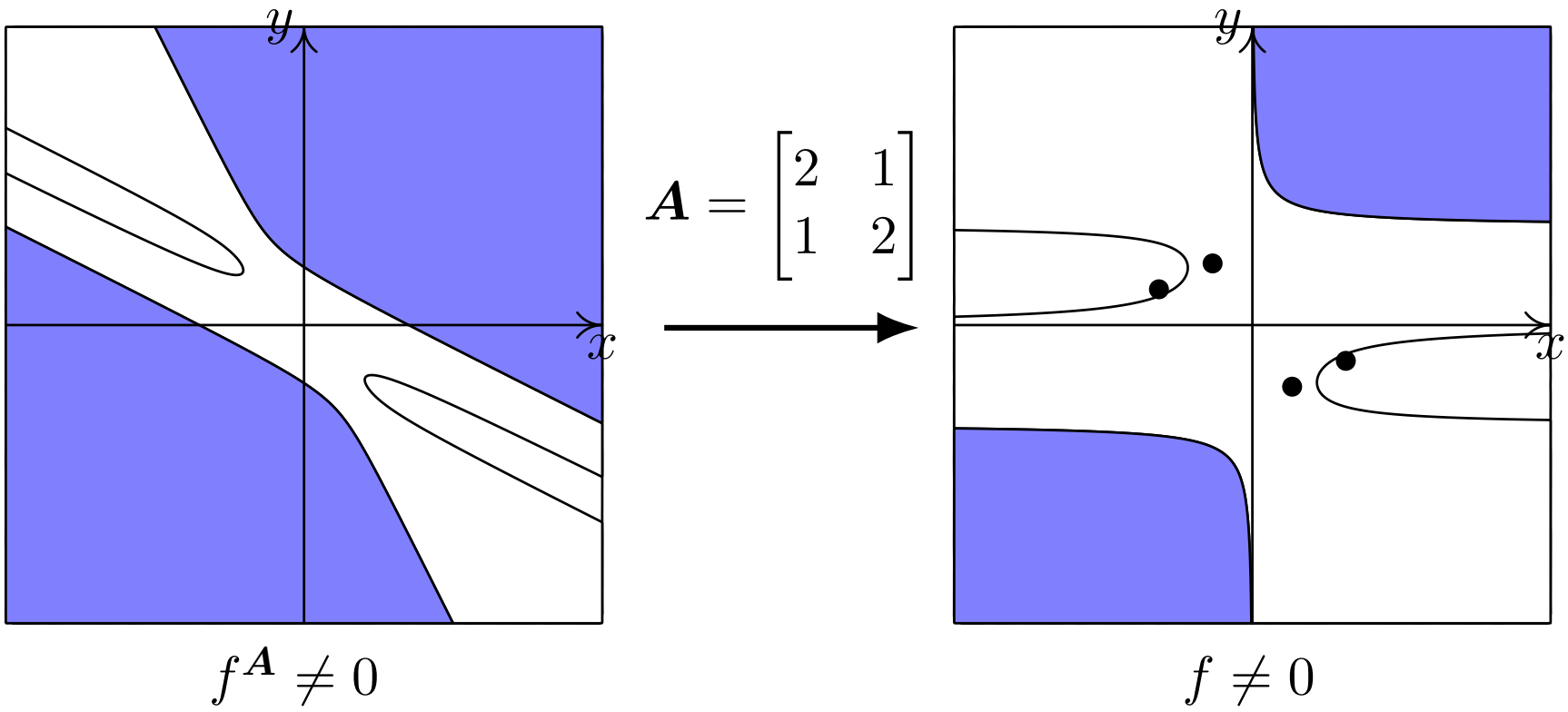
Minimal distance between **computed solution point** and other **intersection points**

Number of real critical points $\mathfrak{R} \leq \mathfrak{D}$

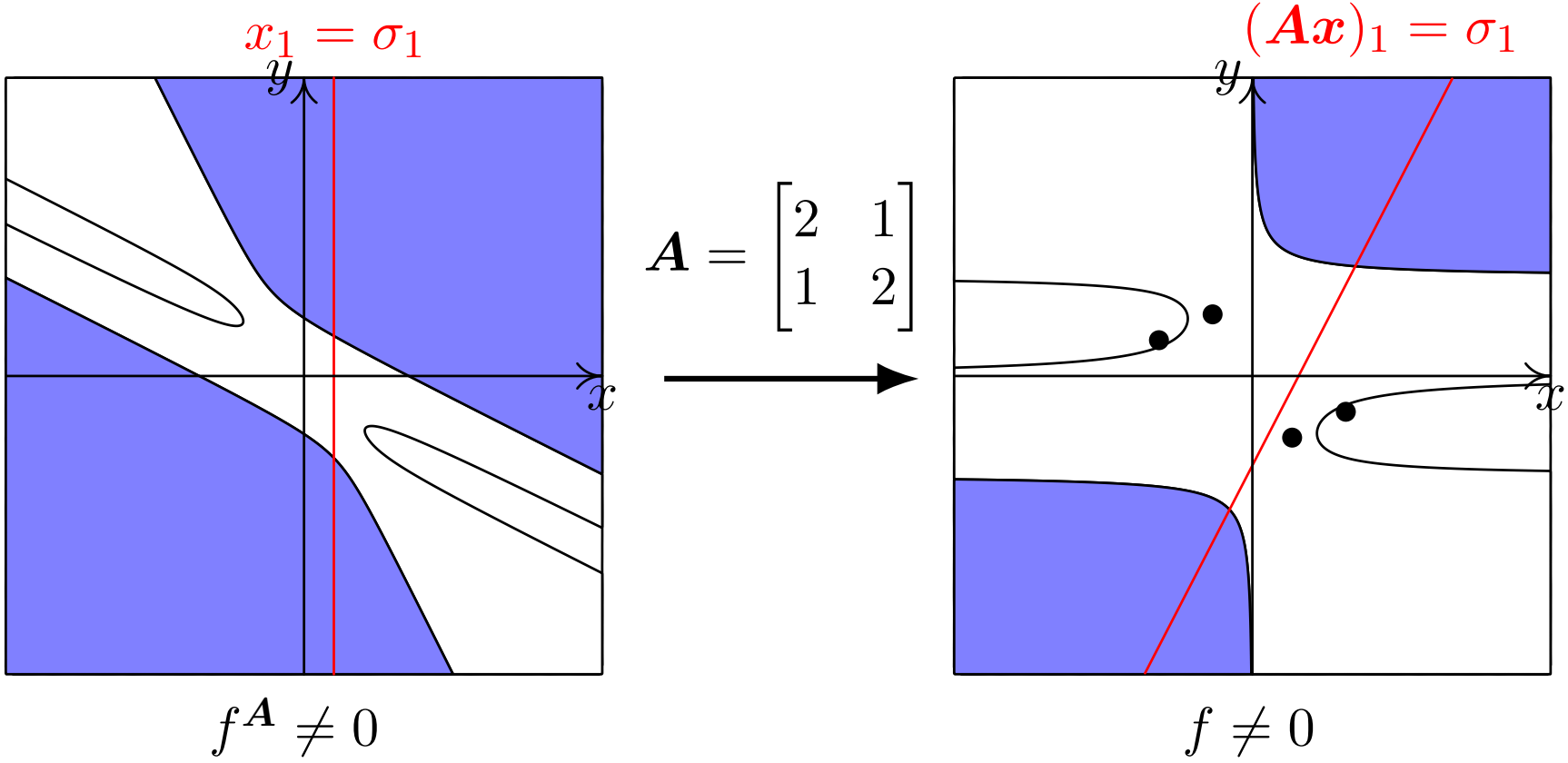
Bit cost of computing **minimal distance** and **parametrisations** of the **black points**: $\tilde{O}((\tau + \log(1/\epsilon))\mathcal{P}(n)\mathfrak{R}\mathfrak{D}^2)$

[Strzebonski–Tsigaridas 2019]

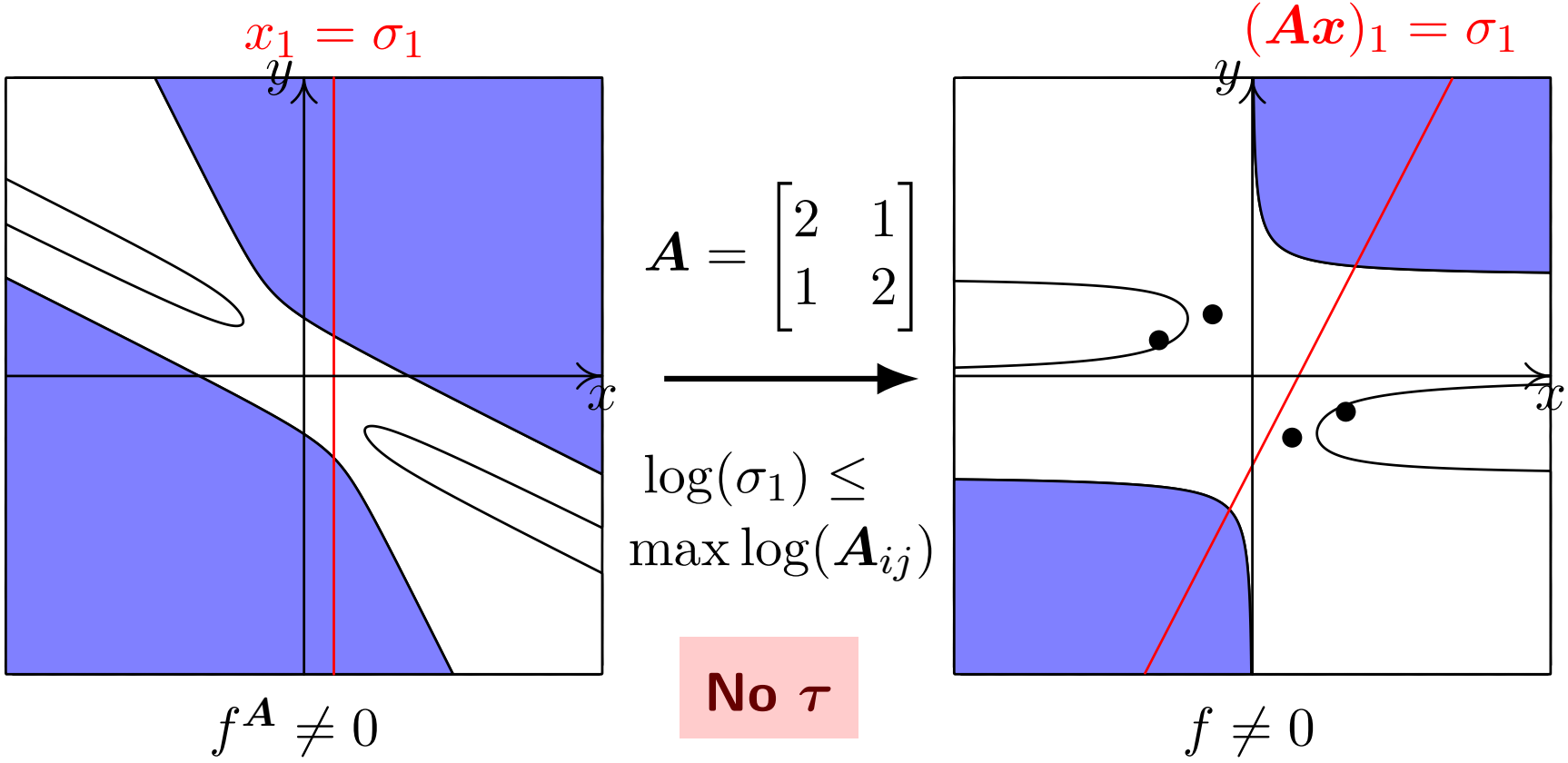
Smooth Case — Specification



Smooth Case — Specification



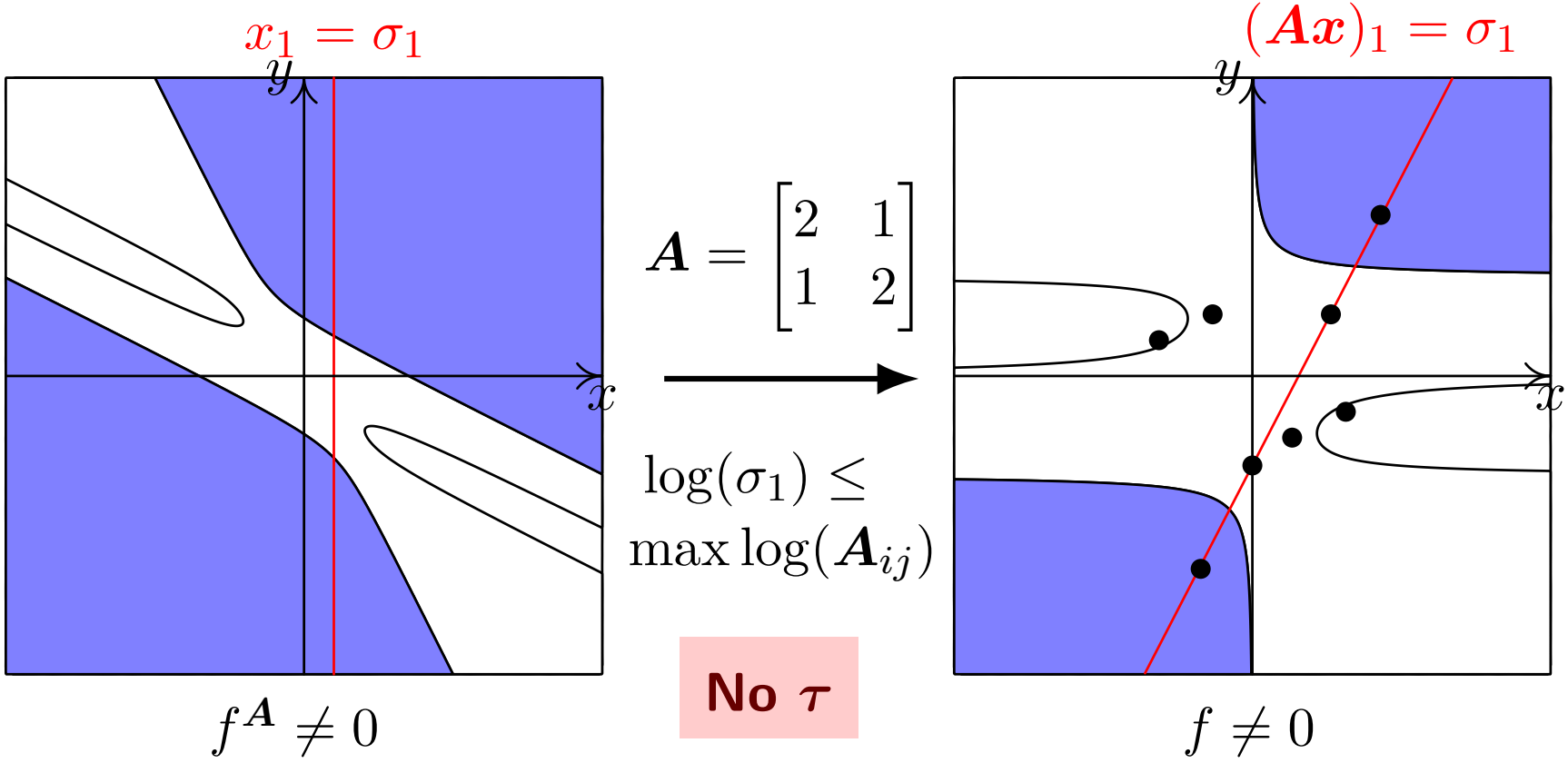
Smooth Case — Specification



Probability of choosing σ_1 such that $V((\boldsymbol{A}\boldsymbol{x})_1 - \sigma_1, f)$ is **smooth** is $\geq 1 - \epsilon/3$

[Elliott–Giesbrecht–Schost 2020/2023]

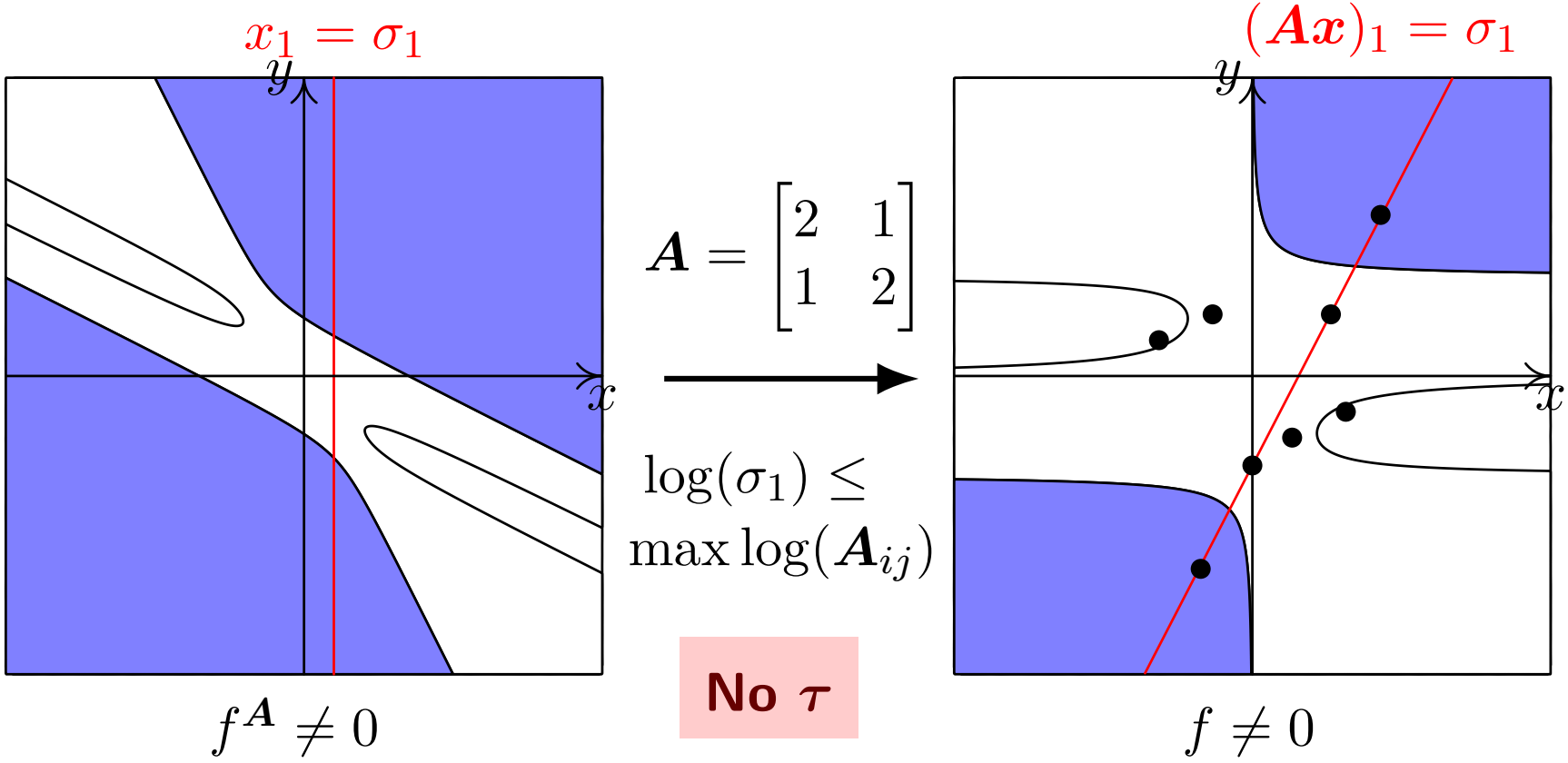
Smooth Case — Specification



Probability of choosing σ_1 such that $V((\boldsymbol{A}\boldsymbol{x})_1 - \sigma_1, f)$ is **smooth** is $\geq 1 - \epsilon/3$

[Elliott–Giesbrecht–Schost 2020/2023]

Smooth Case — Specification

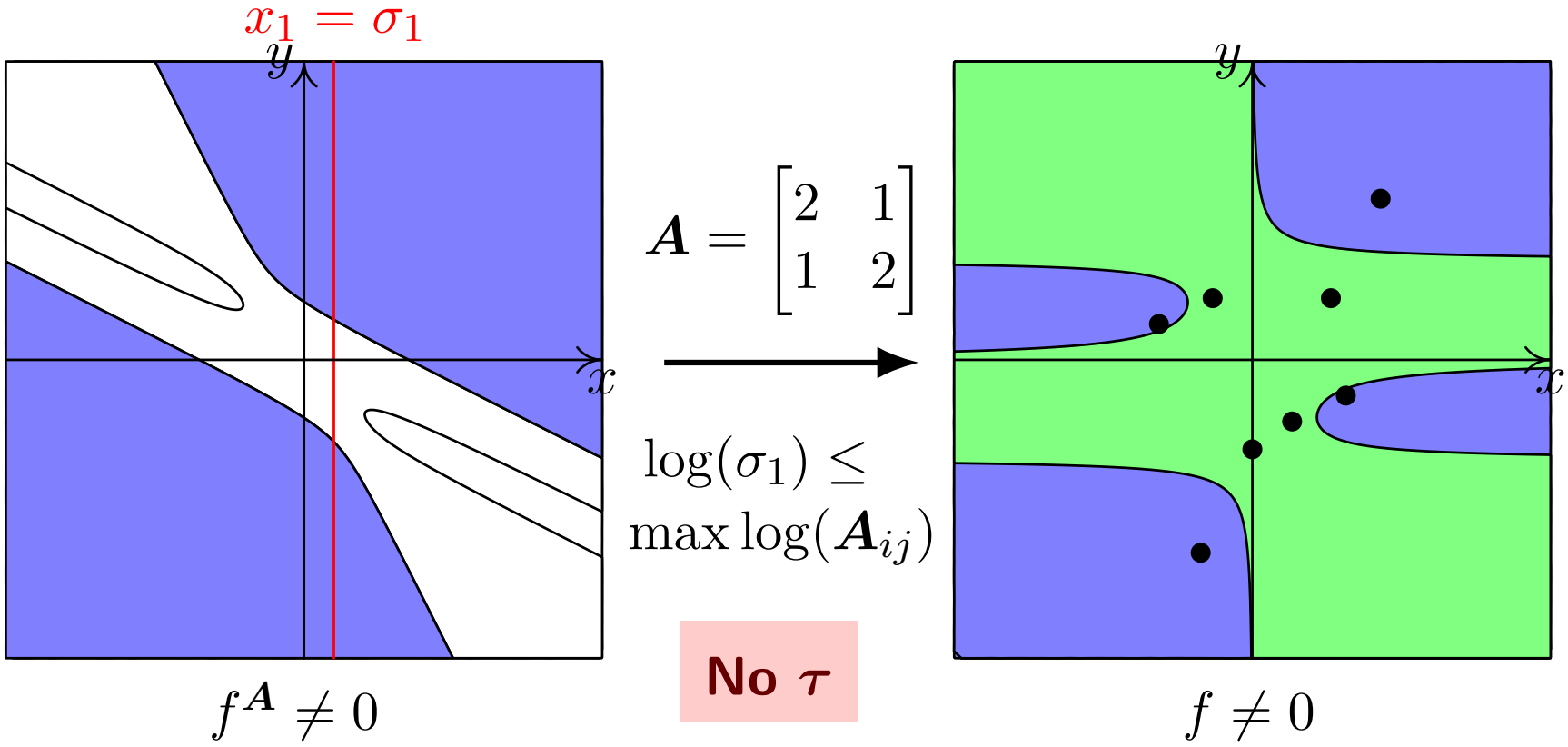


Probability of choosing σ_1 such that $V((\boldsymbol{A}\boldsymbol{x})_1 - \sigma_1, f)$ is **smooth** is $\geq 1 - \epsilon/3$

[Elliott–Giesbrecht–Schost 2020/2023]

Total bit complexity $\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^3)$; **Probability** $\geq 1 - \epsilon$

Smooth Case — Specification



No τ

Probability of choosing σ_1 such that $V((\boldsymbol{A}\boldsymbol{x})_1 - \sigma_1, f)$ is **smooth** is $\geq 1 - \epsilon/3$

[Elliott–Giesbrecht–Schost 2020/2023]

Total bit complexity $\tilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^3)$; **Probability** $\geq 1 - \epsilon$

Singular Case – Curve

No guarantee of
finiteness of solutions

$$f^{\boldsymbol{A}} = \frac{\partial f^{\boldsymbol{A}}}{\partial x_2} = \cdots = \frac{\partial f^{\boldsymbol{A}}}{\partial x_n} = 0$$

Singular Case – Curve

No guarantee of
finiteness of solutions

$$f^{\boldsymbol{A}} = \frac{\partial f^{\boldsymbol{A}}}{\partial x_2} = \cdots = \frac{\partial f^{\boldsymbol{A}}}{\partial x_n} = 0$$

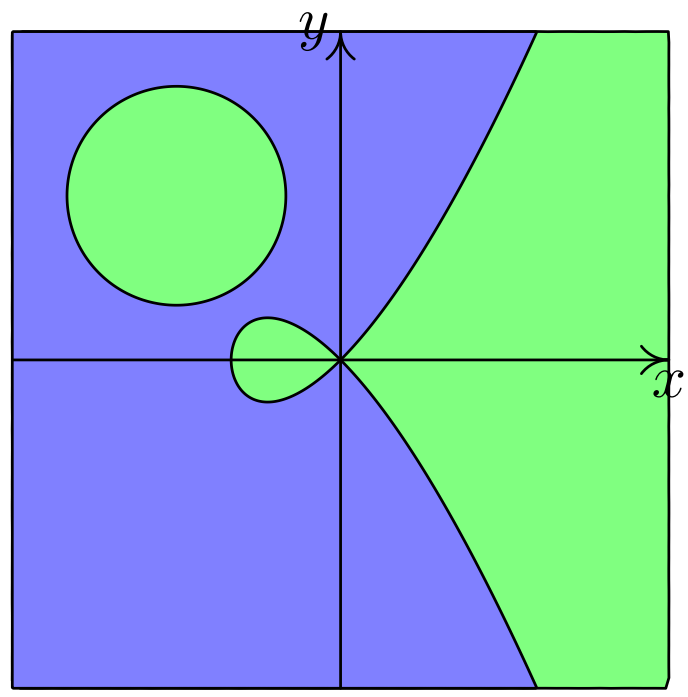
$$\mathcal{C}^{\boldsymbol{A}} := \overline{V\left(\frac{\partial f^{\boldsymbol{A}}}{\partial x_2}, \ldots, \frac{\partial f^{\boldsymbol{A}}}{\partial x_n}\right) \setminus V\left(\frac{\partial f^{\boldsymbol{A}}}{\partial x_1}\right)}^{\mathcal{Z}}$$

Singular Case – Curve

No guarantee of **finiteness** of solutions

$$f^{\boldsymbol{A}} = \frac{\partial f^{\boldsymbol{A}}}{\partial x_2} = \cdots = \frac{\partial f^{\boldsymbol{A}}}{\partial x_n} = 0$$

$$\mathcal{C}^{\boldsymbol{A}} := V\left(\frac{\partial f^{\boldsymbol{A}}}{\partial x_2}, \ldots, \frac{\partial f^{\boldsymbol{A}}}{\partial x_n}\right) \setminus V\left(\frac{\partial f^{\boldsymbol{A}}}{\partial x_1}\right) \overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}^{Z}$$



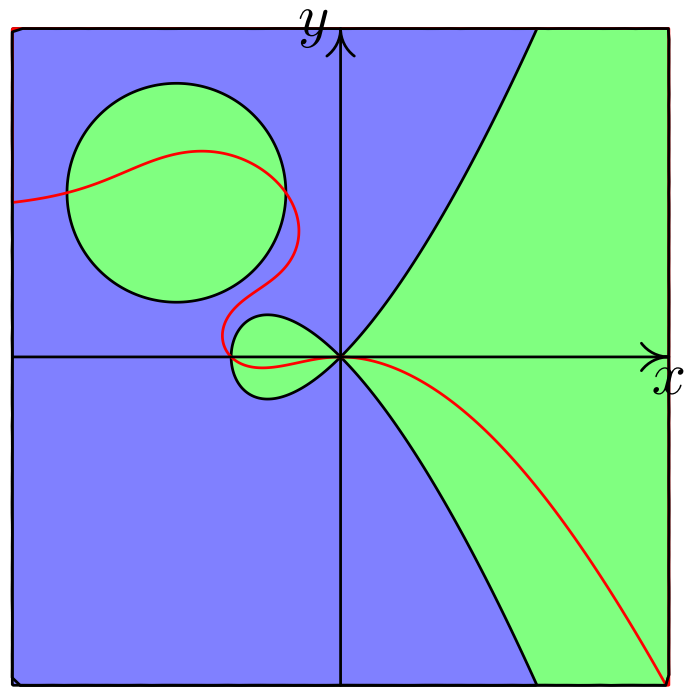
Singular $f^{\boldsymbol{A}} \neq 0$

Singular Case – Curve

No guarantee of **finiteness** of solutions

$$f^{\boldsymbol{A}} = \frac{\partial f^{\boldsymbol{A}}}{\partial x_2} = \cdots = \frac{\partial f^{\boldsymbol{A}}}{\partial x_n} = 0$$

$$\mathcal{C}^{\boldsymbol{A}} := V\left(\frac{\partial f^{\boldsymbol{A}}}{\partial x_2}, \ldots, \frac{\partial f^{\boldsymbol{A}}}{\partial x_n}\right) \setminus V\left(\frac{\partial f^{\boldsymbol{A}}}{\partial x_1}\right) \overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}^{Z}$$



Singular $f^{\boldsymbol{A}} \neq 0$

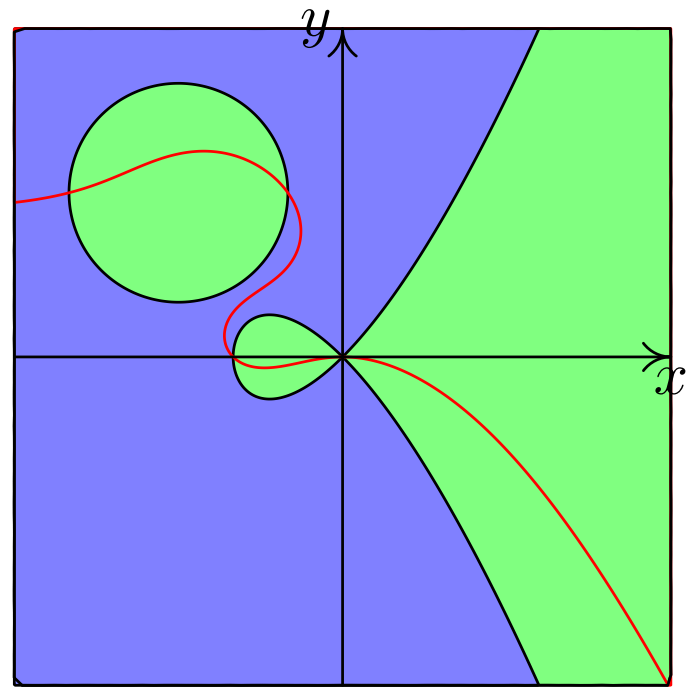
Singular Case – Curve

No guarantee of **finiteness** of solutions

$$f^{\boldsymbol{A}} = \frac{\partial f^{\boldsymbol{A}}}{\partial x_2} = \cdots = \frac{\partial f^{\boldsymbol{A}}}{\partial x_n} = 0$$

$$\mathcal{C}^{\boldsymbol{A}} := V\left(\frac{\partial f^{\boldsymbol{A}}}{\partial x_2}, \ldots, \frac{\partial f^{\boldsymbol{A}}}{\partial x_n}\right) \setminus V\left(\frac{\partial f^{\boldsymbol{A}}}{\partial x_1}\right) \overline{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad} z$$

Generic $A \implies \mathcal{C}^{\boldsymbol{A}}$ is a **curve**



Singular $f^{\boldsymbol{A}} \neq 0$

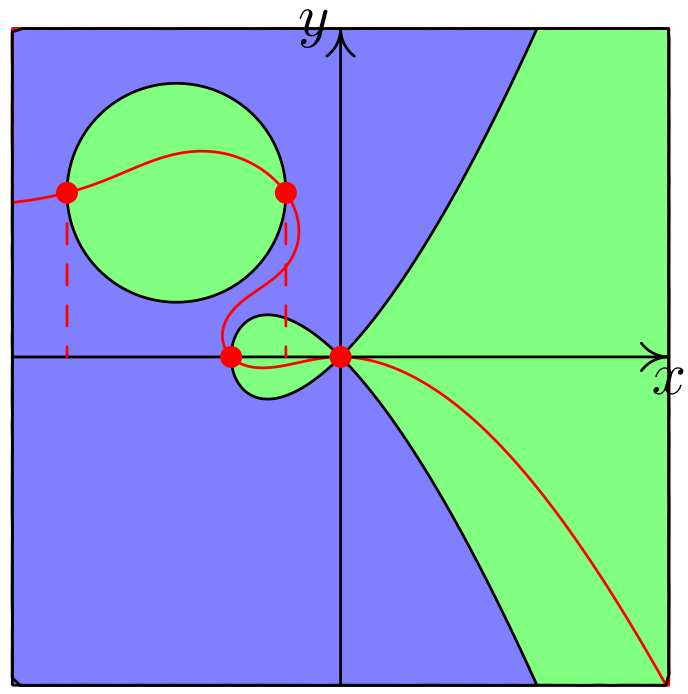
Singular Case – Curve

No guarantee of **finiteness** of solutions

$$f^{\boldsymbol{A}} = \frac{\partial f^{\boldsymbol{A}}}{\partial x_2} = \cdots = \frac{\partial f^{\boldsymbol{A}}}{\partial x_n} = 0$$

$$\mathcal{C}^{\boldsymbol{A}} := \overline{V\left(\frac{\partial f^{\boldsymbol{A}}}{\partial x_2}, \ldots, \frac{\partial f^{\boldsymbol{A}}}{\partial x_n}\right) \setminus V\left(\frac{\partial f^{\boldsymbol{A}}}{\partial x_1}\right)}^{Z}$$

Generic A $\implies$ $\mathcal{C}^{\boldsymbol{A}}$ is a **curve**



Singular $f^{\boldsymbol{A}} \neq 0$

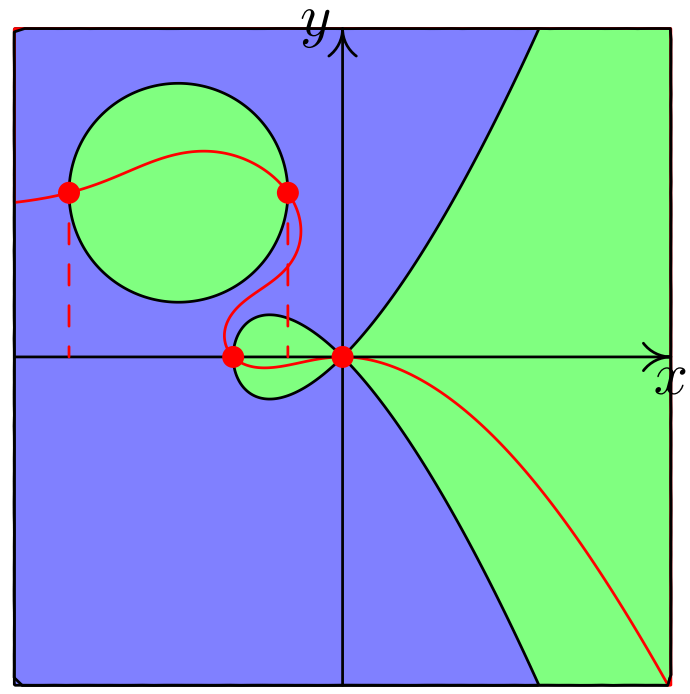
Singular Case – Curve

No guarantee of **finiteness** of solutions

$$f^{\boldsymbol{A}} = \frac{\partial f^{\boldsymbol{A}}}{\partial x_2} = \cdots = \frac{\partial f^{\boldsymbol{A}}}{\partial x_n} = 0$$

$$\mathcal{C}^{\boldsymbol{A}} := \overline{V\left(\frac{\partial f^{\boldsymbol{A}}}{\partial x_2}, \ldots, \frac{\partial f^{\boldsymbol{A}}}{\partial x_n}\right) \setminus V\left(\frac{\partial f^{\boldsymbol{A}}}{\partial x_1}\right)}^{Z}$$

Generic $A \implies \mathcal{C}^{\boldsymbol{A}}$ is a **curve**



Singular $f^{\boldsymbol{A}} \neq 0$

Probability $\geq 1 - \epsilon/3$; **equivalent** polynomials $g_1, \ldots, g_n$ defining $\mathcal{C}$

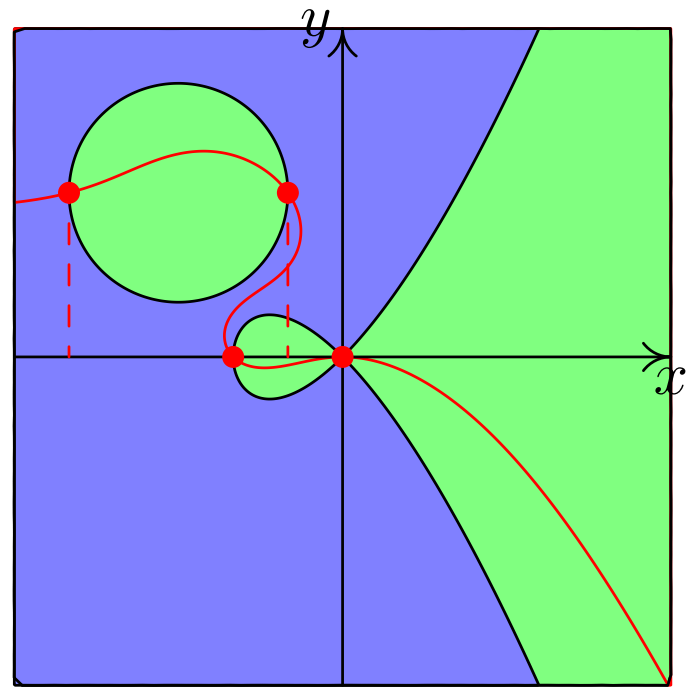
Singular Case – Curve

No guarantee of **finiteness** of solutions

$$f^{\boldsymbol{A}} = \frac{\partial f^{\boldsymbol{A}}}{\partial x_2} = \cdots = \frac{\partial f^{\boldsymbol{A}}}{\partial x_n} = 0$$

$$\mathcal{C}^{\boldsymbol{A}} := \overline{V\left(\frac{\partial f^{\boldsymbol{A}}}{\partial x_2}, \ldots, \frac{\partial f^{\boldsymbol{A}}}{\partial x_n}\right) \setminus V\left(\frac{\partial f^{\boldsymbol{A}}}{\partial x_1}\right)}^{\mathcal{Z}}$$

Generic $A \implies \mathcal{C}^{\boldsymbol{A}}$ is a **curve**



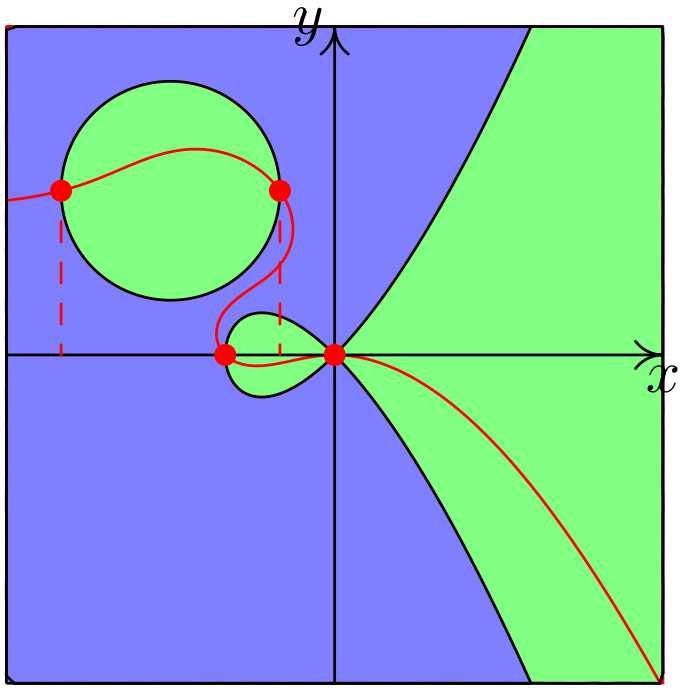
Singular $f^{\boldsymbol{A}} \neq 0$

Probability $\geq 1 - \epsilon/3$; **equivalent** polynomials $g_1, \ldots, g_n$ defining $\mathcal{C}$

Bit cost of computing a **parametrisation** of $\mathcal{C}$:
$\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^2)$

[Giusti–Lecerf–Salvy 2001] [Giménez–Matera 2019]

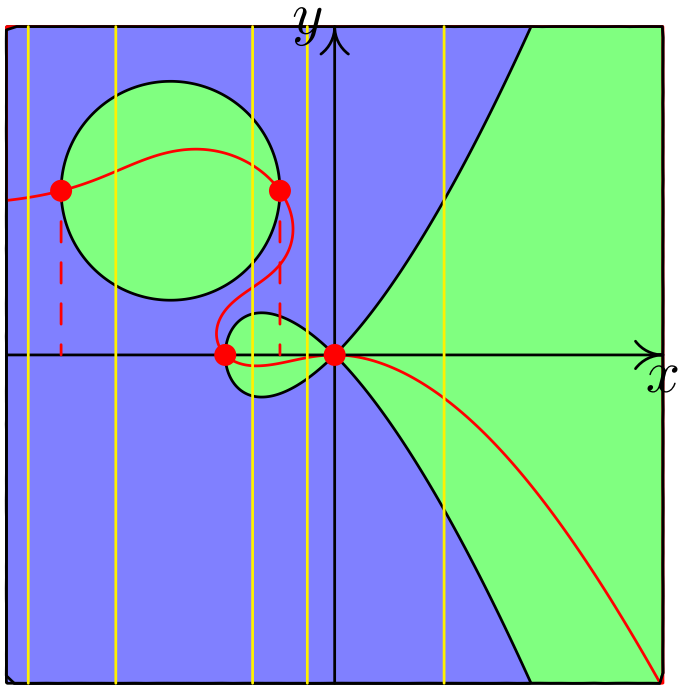
Singular Case – Intersection & Fibres



Bit cost of computing **intersection** $\mathcal{C} \cap V(f)$: $\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^3)$

[Giusti–Lecerf–Salvy 2001] [Giménez–Matera 2019]

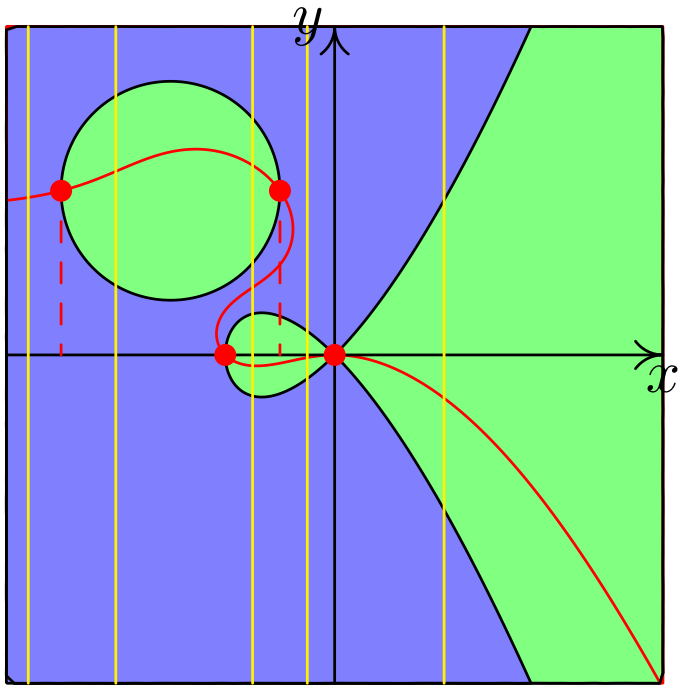
Singular Case – Intersection & Fibres



Bit cost of computing **intersection** $\mathcal{C} \cap V(f)$: $\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^3)$

[Giusti–Lecerf–Salvy 2001] [Giménez–Matera 2019]

Singular Case – Intersection & Fibres



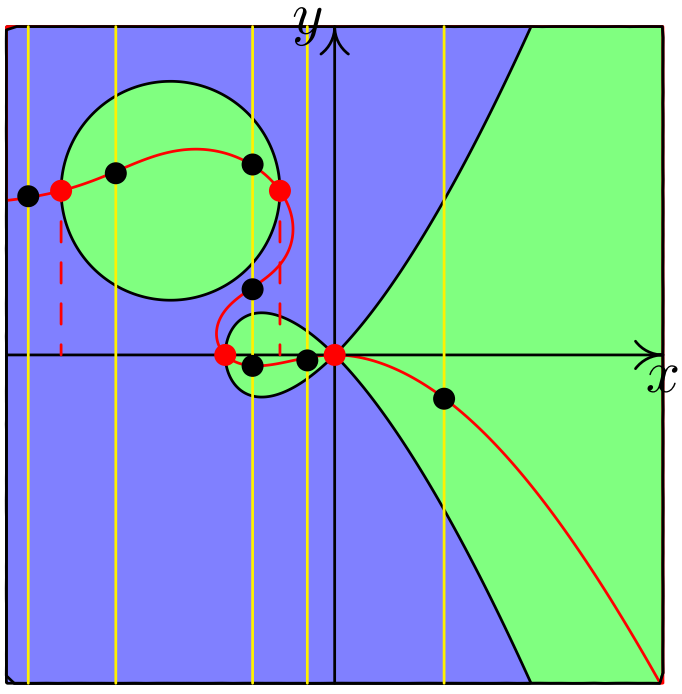
Bit cost of computing **intersection** $\mathcal{C} \cap V(f)$: $\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^3)$

[Giusti–Lecerf–Salvy 2001] [Giménez–Matera 2019]

Bit cost of computing **values** between each **intersection** values: $\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^3)$

[Sagraloff–Melhorn 2016] [Melczer–Salvy 2021]

Singular Case – Intersection & Fibres



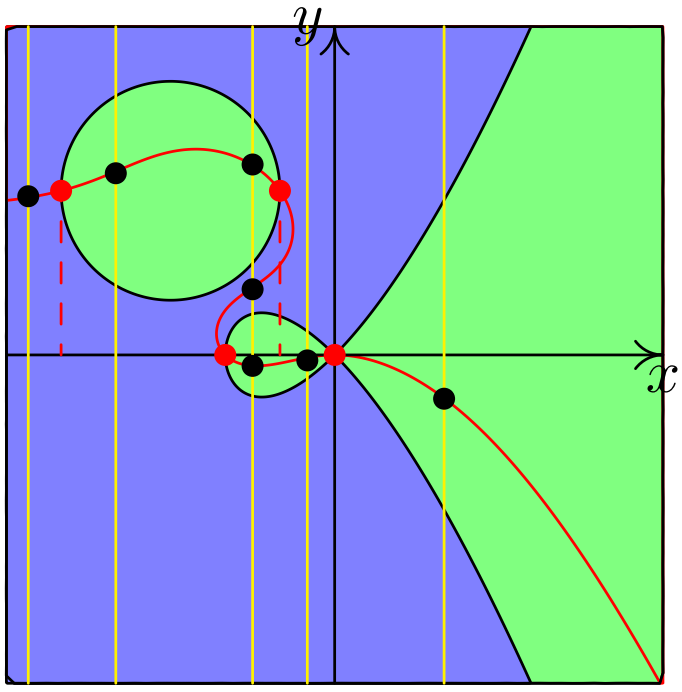
Bit cost of computing **intersection** $\mathcal{C} \cap V(f)$: $\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^3)$

[Giusti–Lecerf–Salvy 2001] [Giménez–Matera 2019]

Bit cost of computing **values** between each **intersection** values: $\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^3)$

[Sagraloff–Melhorn 2016] [Melczer–Salvy 2021]

Singular Case – Intersection & Fibres



Bit cost of computing **intersection** $\mathcal{C} \cap V(f)$: $\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^3)$

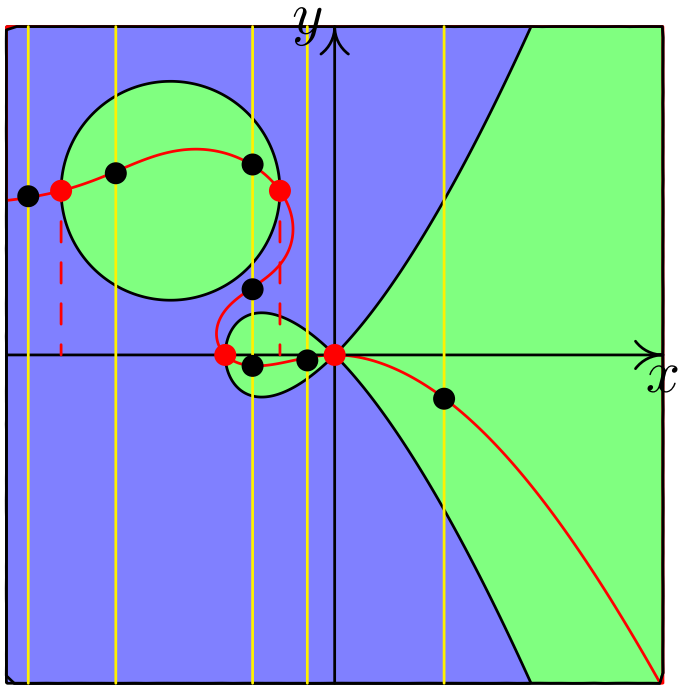
[Giusti–Lecerf–Salvy 2001] [Giménez–Matera 2019]

Bit cost of computing **values** between each **intersection** values: $\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^3)$

[Sagraloff–Melhorn 2016] [Melczer–Salvy 2021]

Bit cost of computing all **black** points: $\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^5)$

Singular Case – Intersection & Fibres



Bit cost of computing **intersection** $\mathcal{C} \cap V(f)$: $\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^3)$

[Giusti–Lecerf–Salvy 2001] [Giménez–Matera 2019]

Bit cost of computing **values** between each **intersection** values: $\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^3)$

[Sagraloff–Melhorn 2016] [Melczer–Salvy 2021]

Bit cost of computing all **black** points: $\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^5)$

Repeat with $x_1 = \sigma_1$, ... **Total** bit complexity $\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^5)$; **Probability** of success $\geq 1 - \epsilon$

Experiments

SageMath implementation, using **msolve** for zero dimensional polynomial system solving [Berthomieu–Eder–Safey El Din 2021]

Experiments

SageMath implementation, using **msolve** for zero dimensional polynomial system solving [Berthomieu–Eder–Safey El Din 2021]

n	CAD	[Safey El Din–Schost 2003]	New Algo
4	2min34s	1min7s	4s
5	$\gg$ 1mo	1h5min	1min7s
6	$\gg$ 1mo	2d4h	42min28s
7	$\gg$ 1mo	$\gg$ 1mo	2d10h
8	$\gg$ 1mo	$\gg$ 1mo	23d11h

Comparisons on generic dense degree 4
examples of fixed bitsize 8

Experiments

SageMath implementation, using **msolve** for zero dimensional polynomial system solving [Berthomieu–Eder–Safey El Din 2021]

n	CAD	[Safey El Din–Schost 2003]	New Algo
4	2min34s	1min7s	4s
5	$\gg$ 1mo	1h5min	1min7s
6	$\gg$ 1mo	2d4h	42min28s
7	$\gg$ 1mo	$\gg$ 1mo	2d10h
8	$\gg$ 1mo	$\gg$ 1mo	23d11h

Comparisons on generic dense degree 4 examples of fixed bitsize 8

n, k	[Safey El Din–Schost 2003]	New Algo
8, 4	OOM	$\gg$ 1d
8, 3	OOM	7h13min
8, 2	OOM	13s
12, 3	OOM	18h58min
12, 2	OOM	31s
20, 3	OOM	$\gg$ 1d
20, 2	OOM	1min40s
50, 2	OOM	23min27s
50, 1	OOM	86s
100, 0	OOM	47min39s
150, 0	OOM	8h15min

Comparisons on degree 12 examples with $n - k$ partial derivatives of degree 1

Conclusions & Further Works

New algorithms with **bit complexity** in terms of $\mathfrak{D} = \deg(f) \prod_{i=1}^{n} \deg\left(\frac{\partial f}{\partial X_i}\right)$, reflecting **structure**

Bit complexity: for $V(f)$ smooth: $\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^3)$, otherwise $\widetilde{O}(\tau \mathcal{P}(n, \log(1/\epsilon))\mathfrak{D}^5)$

Probability of success: at least $1 - \epsilon$, $0 < \epsilon < 1$

Practical Improvements!

Long-term aims: generalise to **several** polynomials;
apply to problems from other scientific fields;
study other structures