Polynomial System Solving in Metric Algebraic Geometry

Jules Tsukahara

Sorbonne Université

INRIA

Arithmetic and Geometry Examples Seminar, 13/11/2026

Polynomial System Solving

Given $f_1, \ldots, f_s \in \mathbb{Q}[x_1, \ldots, x_n]$, describe

$$V(f_1, \ldots, f_s) = \{\alpha \in \mathbb{C}^n : f_1(\alpha) = \cdots = f_s(\alpha) = 0\} \quad \text{and} \quad V \cap \mathbb{R}^n.$$

In the sciences

- robotics: inverse kinematics
- chemistry: steady states of reaction networks
- economics: Nash equilibria
- statistics: maximum likelihood

In algebraic geometry

- enumerative geometry
- elimination and implicitization
- singularities

See Sturmfels, *Solving Systems of Polynomial Equations*; Dickenstein & Emiris.

Metric Algebraic Geometry

Metric algebraic geometry studies real varieties $X \subset \mathbb{R}^n$ *together with a metric*:

- distance from a point to X, nearest points
- Voronoi cells, volumes, sampling
- Wasserstein distance, condition numbers

Breiding, Kohn & Sturmfels, *Metric Algebraic Geometry*, 2024.

Euclidean Distance Degree

Many models in the sciences and engineering are expressed as sets of real solutions to systems of polynomial equations in n unknowns. For such a real algebraic variety $X \subset \mathbb{R}^n$, we consider the following problem: given $u \in \mathbb{R}^n$, compute $u^* \in X$ that minimizes the squared Euclidean distance $d_u(x) = \sum_{i=1}^n (u_i - x_i)^2$ from the given point u. This optimization problem arises in a wide range of applications. For instance, if u is a noisy sample from X, where the error model is a standard Gaussian in $\mathbb{R}^n$, then u^* is the maximum likelihood estimate for u.

Draisma, Horobeț, Ottaviani, Sturmfels & Thomas, 2016

Definition. The *ED degree* of X is the number of complex critical points of d_u on X_{reg}, for u in a dense **Zariski** open subset of $\mathbb{C}^n$.

The nearest point u^* is one of these critical points.

Plan

1. Introducing the example polynomial system
2. Computing a Gröbner basis of it
3. Computing a Rational Univariate Representation of the system
4. Counting and isolating the real roots of the system

Effective Fields

$\mathbb{K}$ is an **effective field** if:

- elements of $\mathbb{K}$ have an exact finite representation
- $+, -, \times, \div$ and equality tests can be done algorithmically.

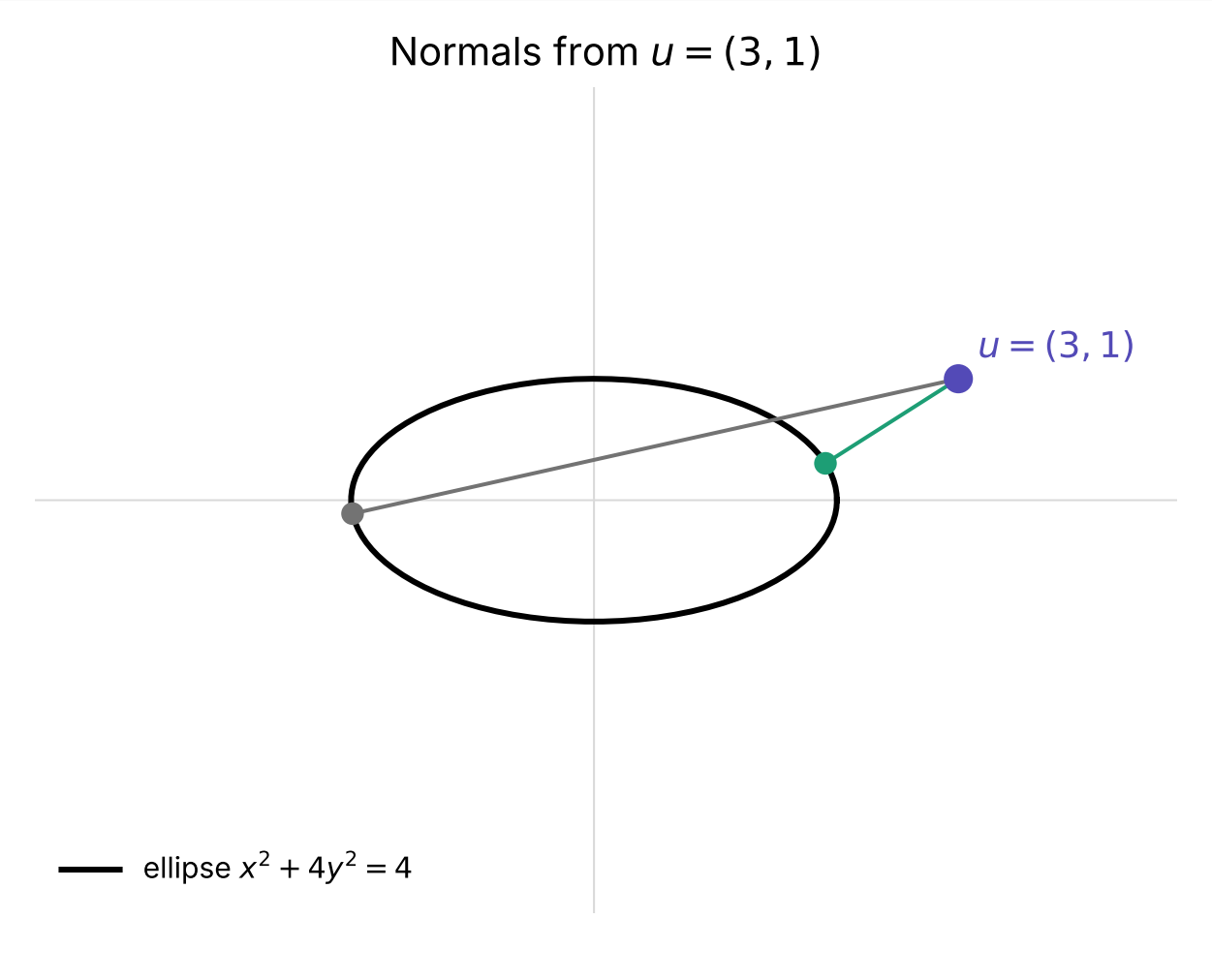
Examples: $\mathbb{Q}$, $\mathbb{F}_p$
Non-examples: $\mathbb{R}$, $\mathbb{C}$

In the remainder of the presentation $\mathbb{K} = \mathbb{Q}$.

Motivating Example: Ellipse

Nearest point on an ellipse X to a point $u = (u, v)$.

- Bézout bound $2 \cdot 2 = 4$, and $\mathrm{EDdeg}(X) = 4$;
- the number of **real** critical points is 2 or 4



The Polynomial System

Let X denote the ellipse in $\mathbb{R}^2$ with equation

$$x^2 + 4y^2 = 4.$$

Let $(u, v) \in \mathbb{R}^2$ be a point, and let $d_{(u,v)}(x, y) = (u - x)^2 + (v - y)^2$ be the squared Euclidean distance.

$(x, y) \in X$ is a critical point of $d_{(u,v)}|_X$ iff $(u - x,\ v - y)$ is **parallel to the normal** $\nabla f = (2x, 8y)$, i.e. **orthogonal to the tangent** direction $(-4y,\ x)$:

$$(u - x,\ v - y) \cdot (-4y,\ x) = 0 \iff 3xy - 4uy + vx = 0.$$

The critical points are the solutions of

$$f_1 = x^2 + 4y^2 - 4 = 0,$$
$$f_2 = 3xy - 4uy + vx = 0.$$

Take $(u, v) = (3, 1)$.

Gröbner Basis

Polynomial System

$f_1 = x^2 + 4y^2 - 4 = 0$
$f_2 = -12y + 3xy + x = 0$

Let $I = \langle f_1, f_2 \rangle$.
We want to do linear algebra in the quotient $\mathbb{Q}[x, y]/I$. **Problem**:

1. we need to be able to test whether a polynomial $g \in I$;
2. we would like a "canonical" expression for g mod I.

Not a given: $g = xy^2 - x$, $g_1 = xy - 1$, $g_2 = y^2 - 1$. Then

$$xy^2 - x = y\, g_1 + 0 \cdot g_2 + (-x + y),$$
$$xy^2 - x = 0 \cdot g_1 + x\, g_2 + 0.$$

The remainder depends on the order of the divisions.

A **Gröbner basis** of I is a generating set G for which division by G always gives the **same** remainder, so that each class in $\mathbb{K}[X]/I$ has a unique representative.

Monomial Orders and Leading Terms

Polynomial System

$f_1 = x^2 + 4y^2 - 4 = 0$
$f_2 = -12y + 3xy + x = 0$

A **monomial order** is a total order on monomials, compatible with multiplication, with 1 as smallest element.

- **lex** ($x > y$): compare the exponent of x first, then of y.
  $x > y^3 > y^2 > y > 1$
- **grevlex** ($x > y$): compare total degree first, break ties using **lex**, reverse the outcome.
  $y^3 > x^2 > xy > y^2 > x > y > 1$

For $f \neq 0$: $\mathrm{LT}(f)$ is its leading term, $\mathrm{LM}(f)$ the corresponding monomial, $\mathrm{LC}(f)$ its coefficient. In grevlex:

$$\mathrm{LT}(f_1) = x^2, \qquad \mathrm{LT}(f_2) = 3xy.$$

G is a Gröbner basis of I iff $\langle \mathrm{LT}(I) \rangle = \langle \mathrm{LT}(g) : g \in G \rangle$.

Algorithm for Gröbner Bases

S-polynomial. Cancel the leading terms of g_i and g_j:

$$S(g_i, g_j) = \frac{\mathrm{LT}(g_j)\, g_i - \mathrm{LT}(g_i)\, g_j}{\gcd(\mathrm{LM}(g_i), \mathrm{LM}(g_j))}.$$

Buchberger's criterion. Let $I = \langle g_1, \ldots, g_s \rangle$ and fix a monomial order. Then $G = \{g_1, \ldots, g_s\}$ is a Gröbner basis of I iff, for all $i < j$, $S(g_i, g_j)$ has remainder 0 after division by G.

Algorithm 1: Buchberger

Input: $F = \{f_1, \ldots, f_s\}$
Output: a Gröbner basis G of $\langle F \rangle$

```
1 G ← F,    P ← {(g, h) : g ≠ h ∈ G};
2 while P ≠ ∅ do
3 |   pick and remove (g, h) from P;
4 |   r ← remainder of S(g, h) divided by G;
5 |   if r ≠ 0 then
6 |   |   P ← P ∪ {(g, r) : g ∈ G},    G ← G ∪ {r};
7 return G
```

Gröbner Basis of the Example

Polynomial System

$f_1 = x^2 + 4y^2 - 4 = 0$
$f_2 = -12y + 3xy + x = 0$

We use the **grevlex** monomial order.
Let $G = \{f_1, f_2\}$ We compute:

$$\begin{aligned} S(f_1, f_2) &= 3yf_1 - xf_2 \\ &= x^2 + 12xy + 12y^3 - 12y \end{aligned}$$

One can check that $S(f_1, f_2) = 12y^3 + 4y^2 - 4x + 36y - 4 \mod \{f_1, f_2\}$.
Let $f_3 = 3y^3 + y^2 + 9y - x + 1$. Add it to $G \leftarrow G \cup \{f_3\}$.
Check the remaining S-polynomials $S(f_1, f_3)$ and $S(f_2, f_3)$: they both reduce to 0.
A Gröbner basis of $\{f_1, f_2\}$ is thus $G = \{f_1, f_2, f_3\}$.

VSCode Demo 1

The Quotient Algebra

$$\mathrm{LT}(G) = \{x^2,\ xy,\ y^3\}$$

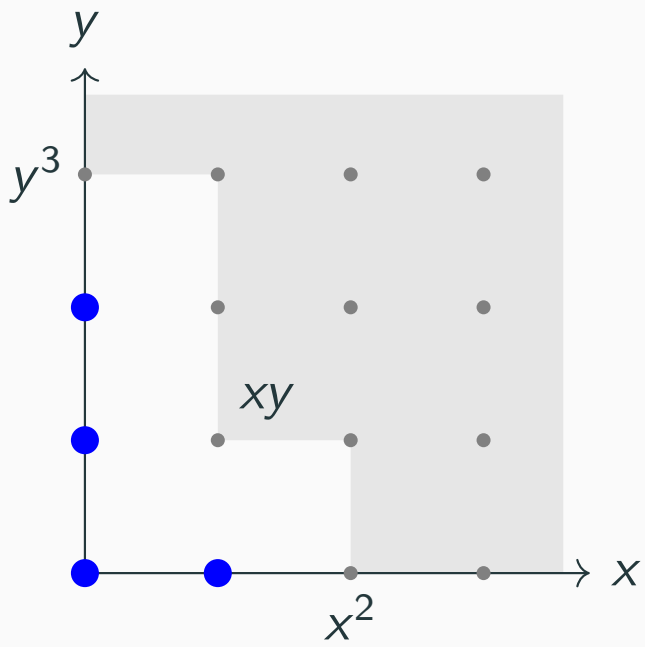
Standard monomials:

$$B = \{1,\ x,\ y,\ y^2\}.$$

Hence

$$A = \mathbb{Q}[x, y]/I, \qquad \dim_{\mathbb{Q}} A = 4.$$

Finiteness theorem. I is zero-dimensional ($|V_{\mathbb{C}}(I)| < \infty$) iff $\dim A < \infty$ iff G has a leading monomial that is a pure power of each variable.



Blue: standard monomials.
Grey: $\langle \mathrm{LT}(I) \rangle$.

Stickelberger's Theorem

For $f \in A$, let $M_f : A \to A$ be the multiplication map by f such that $M_f(g) = fg$.

Stickelberger's Theorem

- $\text{Trace}(M_f) = \sum_{\alpha \in V_{\mathbb{C}}(I)} \mu(\alpha) f(\alpha)$
  - $\text{Trace}(M_1) = \dim_{\mathbb{C}} (\mathbb{Q}[X]/I)$
- $\det(M_f) = \prod_{\alpha \in V_{\mathbb{C}}(I)} f(\alpha)^{\mu(\alpha)}$
- $\mathcal{X}_{M_f}(T) = \prod_{\alpha \in V_{\mathbb{C}}(I)} (T - f(\alpha))^{\mu(\alpha)}$

Eigenvalues of M_f = Evaluations of f on $V_{\mathbb{C}}(I)$!

Multiplication Matrices

For $h \in A$, multiplication by h is a linear map $M_h : A \to A$. Column j of M_h contains the coordinates of $(h \cdot b_j)$ in $B = (1, x, y, y^2)$.

Example: $x \cdot y^2 = \frac{1}{9}x - \frac{4}{3}y + 4y^2 \mod G$.

$$M_x = \begin{pmatrix} 0 & 4 & 0 & 0 \\ 1 & 0 & -\frac{1}{3} & \frac{1}{9} \\ 0 & 0 & 4 & -\frac{4}{3} \\ 0 & -4 & 0 & 4 \end{pmatrix}, \qquad M_y = \begin{pmatrix} 0 & 0 & 0 & \frac{1}{3} \\ 0 & -\frac{1}{3} & 0 & \frac{1}{3} \\ 1 & 4 & 0 & -3 \\ 0 & 0 & 1 & -\frac{1}{3} \end{pmatrix}.$$

$M_x M_y = M_y M_x = M_{xy}$, and $M_{g(x,y)} = g(M_x, M_y)$.
Everything about A is now **finite-dimensional linear algebra**.

Multiplication Matrices

- eigenvalues of M_x: $1.906,\ -1.988,\ 4.041 \pm 0.752\,i$
- eigenvalues of M_y: $0.303,\ -0.111,\ -0.430 \pm 1.768\,i$

Problem: which x goes with which y? 4! possible matchings.

Is it possible to represent the solutions using a single univariate polynomial?

Rational Univariate Representation

A linear form t is **separating** if it takes distinct values at distinct points of $V_{\mathbb{C}}(I)$. Here $t = y$ works: χ_{M_y} is squarefree of degree 4.

Definition. Due to Rouiller. A RUR of I is $f, g_{x_1}, \ldots, g_{x_n} \in \mathbb{Q}[t]$ such that

$$V_{\mathbb{C}}(I) = \left\{ \left(\frac{g_{x_1}(\tau)}{f'(\tau)}, \ldots, \frac{g_{x_n}(\tau)}{f'(\tau)} \right) \ : \ f(\tau) = 0 \right\}.$$

Gives a bijection: $\phi : V_{\mathbb{C}}(I) \to V_{\mathbb{C}}(f)$ which preserves multiplicity and real zeros. Can be computed from traces of multiplication matrices!

Then: isolate the roots of f, and evaluate.

VSCode Demo 2

Real Root Counting: Sturm's Theorem

Theorem (Sturm). Let $S_0 = f$, $S_1 = f'$, $S_{i+1} = -\operatorname{rem}(S_{i-1}, S_i)$. If $V(a)$ is the number of sign changes in $(S_0(a), S_1(a), \ldots)$, then

$$\#\{\text{real roots of } f \text{ in } (a, b]\} = V(a) - V(b).$$

Example.

$$S_0 = t^4 + \tfrac{2}{3}t^3 + \tfrac{28}{9}t^2 - \tfrac{2}{3}t - \tfrac{1}{9}, \qquad S_1 = 4t^3 + 2t^2 + \tfrac{56}{9}t - \tfrac{2}{3},$$
$$S_2 = -\tfrac{53}{36}t^2 + \tfrac{41}{54}t + \tfrac{1}{12}, \qquad S_3 = \tfrac{3680}{8427} - \tfrac{24000}{2809}t,$$
$$S_4 = -\tfrac{862363}{7290000}.$$

$$V(-\infty) = 3, \qquad V(0) = 2, \qquad V(+\infty) = 1.$$

Root Isolation and the Nearest Point

Isolating intervals for the real roots of f :

$$\left(-\tfrac{1}{4}, -\tfrac{1}{16}\right), \qquad \left(\tfrac{1}{8}, \tfrac{5}{16}\right).$$

Refine by dichotomy to any precision, then evaluate $x = g_x(t)/f'(t)$ in interval arithmetic:

$t = y$	x	distance to $(3, 1)$
0.3033358440	1.9057674210	1.2971838 (nearest)
−0.1106552778	−1.9877176957	5.1098809 (farthest)

Certifying the minimum. Evaluated on the two isolating intervals, the results are disjoint, so the nearest point is certified.

VSCode Demo 3

Conclusion

Thank you for your attention!