Efficient algorithms in real algebraic geometry

Mohab Safey El Din

Univ. Pierre et Marie Curie, Paris

INRIA, POLSYS Team

CNRS

Institut Universitaire de France

Polynomials

Monomial: Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$

$$\mathbf{X}^\alpha = X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_n^{\alpha_n}$$

Degree $= \deg(\mathbf{X}^\alpha) = \alpha_1 + \cdots + \alpha_n$

Polynomial: Let A be a finite set of $\mathbb{N}^n$ and $\mathbf{X} = (X_1, \ldots, X_n)$.

$$F = \sum_{\alpha \in A} c_\alpha \mathbf{X}^\alpha \qquad \text{with} \qquad c_\alpha \in \mathbb{Q}, \mathbb{R}, \mathbb{C} \text{ and } c_\alpha \neq 0$$

Degree$= \deg(F) = \max(\deg(\mathbf{X}^\alpha), \alpha \in A)$

Basic semi-algebraic set.

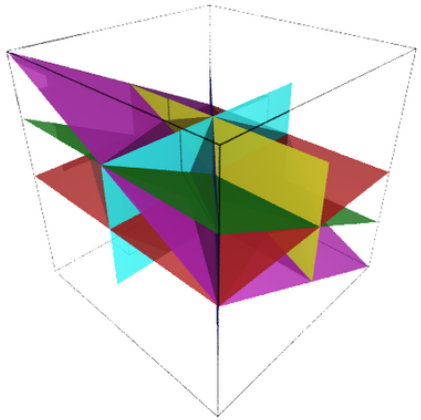
$$F_1 = \cdots = F_p = 0, \quad G_1 \ \sigma \ 0, \ldots, G_s \ \sigma \ 0$$

with $\sigma \in \{>, \geq\}$, F_i, G_j in $\mathbb{Q}[X_1, \ldots, X_n]$ of degree $\leq D$.

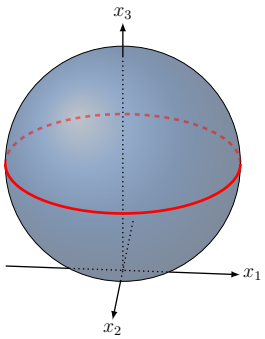
Semi-algebraic sets are the class of sets stable by finite unions, intersections, complements of basic semi-algebraic sets.

Examples and first observations

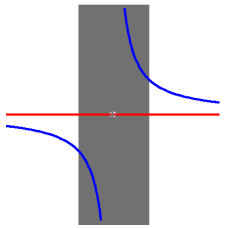
The very basic polynomials that everybody met are linear polynomials.
BUT allowing inequalities/inequations make things complicated

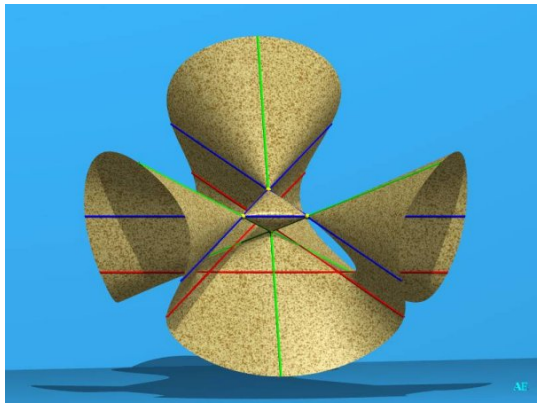


$X_1^2 + X_2^2 + X_3^2 - 1 \rightarrow$



$X_1 X_2 - 1 \rightarrow$





More general situations

$(x + y + z - 1)(xy + yz + xz) = 2xyz$

Another observation

Consider

$$\boxed{F_1 = \cdots = F_n = 0}$$

such that

- $F_i \in \mathbb{Q}[X_1, \ldots, X_n]$
- $F_i = L_{1,i} \cdots L_{D,i}$ with $L_{j,i} \in \mathbb{Q}[X_1, \ldots, X_n]$ and $\deg(L_{j,i}) = 1$.

If all linear forms are linearly independent then the system has

$\boxed{D^n \text{ solutions}}$ and all of them are real.

$$\boxed{\text{Bézout bound} = \deg(F_1) \cdots \deg(F_n)}$$

$\rightarrow$ sharp bound on the number of solutions in $\mathbb{C}^n$.

Real algebraic geometry / Algebraic geometry

Real Algebraic Geometry: Study of real solutions of polynomial systems of equations and inequalities with real coefficients and maps between them.

Computational aspects: Start with Fourier (Linear programming), Univariate cases (17-th – 19-th, Descartes/Vincent, Sturm).

Multivariate aspects $\rightarrow$ Tarski ($30's$ – Decidability) / Collins (1975) –

A decision method for elementary algebra and geometry

Algebraic Geometry: Study of complex solutions of polynomial systems of equations and inequalities with complex coefficients and maps between them.

Computational aspects: 19-th century (Macaulay, Kronecker) Buchberger (Gröbner bases, $60's$), revisit of Macaulay's theory, etc.

Eliminate, eliminate, eliminate Eliminate the eliminators of the elimination theory S. S. Abhyankar

Emptiness decision – Computing sample points in semi-algebraic sets

F_i, G_j in $\mathbb{Q}[X_1, \ldots, X_n]$

Input: $F_1 = \cdots = F_p = 0, G_1 > 0, \ldots, G_s > 0$ that defines $S \subset \mathbb{R}^n$

Output: true iff $S \neq \emptyset$ else false

This is a decision problem → Exact/Symbolic computation.

Input: $F_1 = \cdots = F_p = 0, G_1 > 0, \ldots, G_s > 0$ that defines $S \subset \mathbb{R}^n$

Output: *Some* solutions whenever they exist.

- How to encode them? What to do when $\sharp S = \infty$?
- Representative points in all the *connected* components of S.
- Quantitative results on the number of connected components of S?
- Algebraic nature of the problem → Exact/Symbolic computation.

One-block quantifier elimination

F_i, G_j in $\mathbb{Q}[X_1, \ldots, X_n, Y_1, \ldots, Y_t]$

Input: $F_1 = \cdots = F_p = 0, G_1 > 0, \ldots, G_s > 0$ that defines $S \subset \mathbb{R}^n \times \mathbb{R}^t$

Output: A description of $\pi_Y(S)$

where $\pi_Y : (x_1, \ldots, x_n, y_1, \ldots, y_t) \to (y_1, \ldots, y_t)$

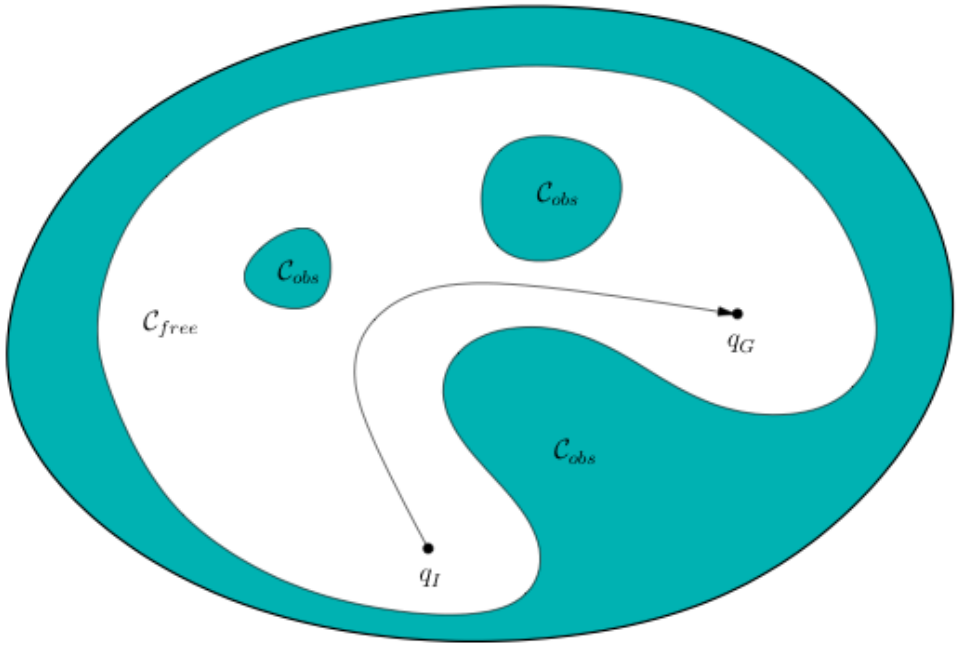
$$\exists\, \mathbf{x} \in \mathbb{R}^n \qquad \mathbf{F}(\mathbf{x}, \mathbf{y}) = 0, \mathbf{G}(\mathbf{x}, \mathbf{y}) > 0 \Longleftrightarrow \Psi(\mathbf{y})$$

Examples:

- $\exists x \in \mathbb{R} \quad x^2 + bx + c = 0 \Leftrightarrow b^2 - 4c \geq 0$
- $\exists x \in \mathbb{R} \quad ax^2 + bx + c = 0 \Leftrightarrow$
  $(a \neq 0 \wedge b^2 - 4c \geq 0) \vee (a = 0 \wedge b \neq 0) \vee (a = 0 \wedge b = 0 \wedge c = 0)$

Output is a formula $\to$ Symbolic computation

Connectivity queries



Outline of the course

- **Part I:** Motivations – basic objects – State of the art
- **Part II:** Some algebra and reductions – Polynomial optimization
- **Part III:** Computing sample points in semi-algebraic sets
- **Part IV:** Quantifier elimination over the reals
- **Part V:** Connectivity queries

Part I:
Motivations – basic objects
State of the art

Semi-algebraic sets and their properties

Recall that the class of semi-algebraic sets in $\mathbb{R}^n$

- contains all sets that are described by $F \geq 0$ for some $F \in \mathbb{R}[X_1, \ldots, X_n]$;
- is stable by taking finite intersections, finite unions and complements of the above sets.

Semi-algebraic sets of $\mathbb{R}$ are finite unions of intervals and points.

Counter-example: The graph of $x \to \sin(x)$ is not semi-algebraic.

Another example: The set $\{(\cos(t), \sin(t)) \in \mathbb{R}^2 \mid t \in \mathbb{R}\}$ is semi-algebraic.

Real algebraic sets of $\mathbb{R}^n$ is the class of subsets of $\mathbb{R}^n$ that is defined as the real solution set of $F_1 = \cdots = F_p = 0$ with $F_i \in \mathbb{R}[X_1, \ldots, X_n]$.

All real algebraic sets can be described by a single equation.

Real algebraic sets of $\mathbb{R}$ are finite unions of points.

Semi-algebraic sets and their properties

Let $S \subset \mathbb{R}^n \times \mathbb{R}^t$ be a semi-algebraic set and $\pi : (x, y) \in \mathbb{R}^n \times \mathbb{R}^t \to y$.

Tarski-Seidenberg's theorem

$\pi(S)$ is a semi-algebraic set.

Quantifier elimination (and many other problems) is decidable !

Finiteness of connected components

S has finitely many connected components and
all of them are semi-algebraic sets.

Let $S \subset \mathbb{R}^n$ be a real algebraic set defined by polynomials of degree $\leq D$.

Quantitative aspects

The number of connected components of S is bounded by $O(D)^n$.

Algebraic sets and their properties

Algebraic sets in $\mathbb{C}^n$ are the sets of complex solutions to polynomial systems of equations with coefficients in $\mathbb{C}$.

A real algebraic set is the real trace of an algebraic set defined by polynomials with coefficients in $\mathbb{R}$.

Zariski topology.

Algebraic sets are closed sets for the **Zariski topology**.

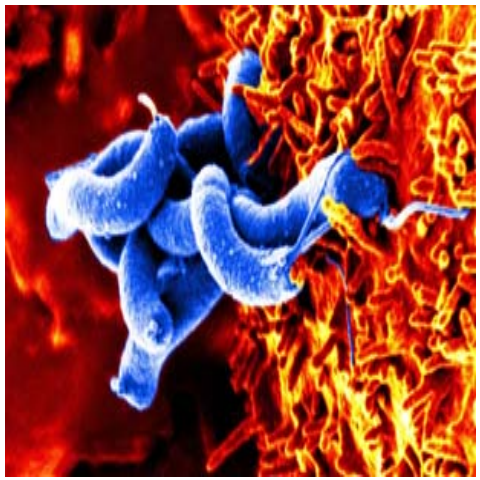
By definition, Zariski open sets are complements of Zariski closed sets. A non-empty Zariski open set is dense in $\mathbb{C}^n$.

Constructible sets are finite unions of sets which are the intersection of a (Zariski) open set and a (Zariski) closed set.

Projections. The projection of a constructible set is constructible.

The projection of an algebraic set is a constructible set.

Some applications to our algorithmic problems (I)



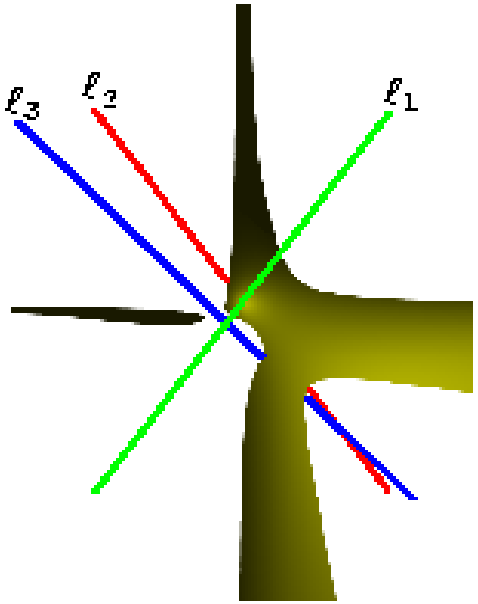
Gene regulation $\rightarrow$ **Dynamical Systems**

$$\dot{\mathbf{X}} = \mathsf{M}(X)$$

Information on the eigenvalues of $\mathsf{M}(X)$

$\rightarrow$ Emptiness decision on the real solution set of polynomial systems.

10 variables – degree 8



Voronoi diagram of 3 lines in $\mathbb{R}^3$

Topological invariance determined by the existence of real solutions to a polynomial inequality.

4 variables – degree 18

Some applications to our algorithmic problems (II)

Size optimization of sextic polynomials in the number field sieve,

S. Bai and P. Zimmermann, Math. of Comp., 2012.

Problem: global infimum of a rational fraction under some linear constraints.

This is a One-Block Quantifier Elimination Problem

Input size:

- 6 variables are involved;
- Degree of the polynomial is 12 (162 monomials);
- Coefficients of bit size $\simeq 254$ bits;

Output:

- 14 local minimizers *very* close and of large magnitude ($\simeq 10^{67}$);
- 200 digits are needed to distinguish these points;

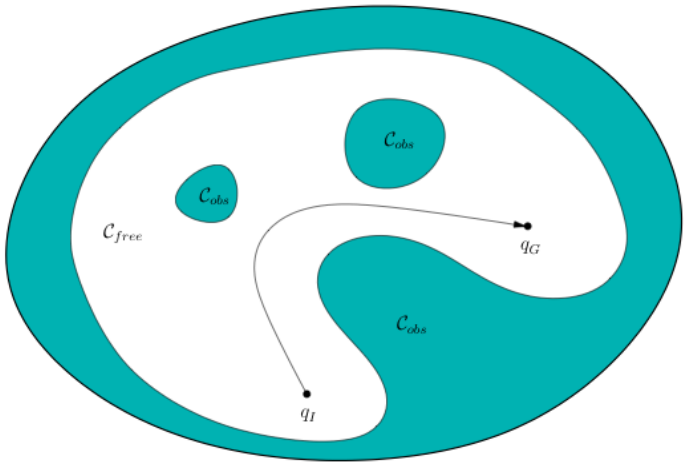
Some applications to our algorithmic problems (III)

$\mathscr{S}$ is a configuration space (algebraic, semi-algebraic)

Problem: given two query points q_0 and q_1, find a continuous path $\gamma : [0,1] \to \mathscr{S}$ such that

$$\gamma(0) = q_0, \quad \gamma(1) = q_1, \quad \forall t \in [0,1]$$

or determine that such a path does not exist.



Algorithmic Needs

- **Reliability issues** – crucial for decision problems/algebraic nature
- **Efficiency issues** – complexity may be exponential in n
- **Main challenge:** obtain fast implementations through algorithms with asymptotically optimal complexities.
- Use of symbolic computation / computer algebra.
  - Efficient tools for algebraic/exact computations
  - Large algorithmic scope (differential algebra $\rightarrow$ arithmetics)
  - BUT **algebraic** manipulations on polynomial expressions give information on **complex roots**
- Millions of users.


Maple™


State of the art

Collins $\sim$ 70's Cylindrical algebraic decomposition – doubly exponential in n

Hong, McCallum, Arnon, Brown, Strzebonski, Anai, Sturm, Weispfenning

Software: QEPCAD, Redlog, SyNRAC, Mathematica, Maple, ...

▷ Quest for algorithms **singly exponential** in n ($\sim 90's$)

Grigoriev/Vorobjov, Canny, Renegar, Heintz/Roy/Solerno, Basu/Pollack/Roy

Existence	$D^{O(n)}$
One-Block QE	$D^{O(nt)}$
Connectivity	$D^{O(n^2)}$

▷ **Challenge:** combine theoretical and practical efficiency

▷ **Primary goal: obtain fast and reliable software** $\rightarrow$ RAGlib

▷ Better understanding of the complexity $\rightarrow$ **constant in the exponent?**

Part II: Some algebra and reductions
Polynomial optimization

Encoding finite (real) algebraic sets

Easy (univariate) case: $q(T) = 0$ + isolating intervals for real roots.

Let $V \subset \mathbb{C}^n$ be a finite algebraic set $\rightarrow$ **parametrizations**

$$\left\{\begin{array}{rcl} X_n & = & q_n(T) \\ & \vdots & \\ X_1 & = & q_1(T) \\ q(T) & = & 0 \end{array}\right. \quad + \quad \text{isolating boxes to encode } V \cap \mathbb{R}^n$$

with q square-free

We may also use **rational parametrizations**

$$\left\{\begin{array}{rcl} X_n & = & q_n(T)/q_0(T) \\ & \vdots & \\ X_1 & = & q_1(T)/q_0(T) \\ q(T) & = & 0 \end{array}\right. \quad \text{with } \mathsf{gcd}(q, q_0) = 1.$$

Note that $\deg(q) = \sharp V$.

Algebraic operations – Ideals

Parametrizations may be obtained by algebraic operations.

Recall that $V \subset \mathbb{C}^n$ is given as the solution set of $F_1 = \cdots = F_p = 0$.

Nullstellensatz (Hilbert)

$V = \emptyset$ iff there exists $Q_1, \ldots, Q_p$ in $\mathbb{Q}[X_1, \ldots, X_n]$ s.t. $1 = Q_1 F_1 + \cdots Q_p F_p$.

$\{Q_1 F_1 + \cdots + Q_p F_p\}$ is the ideal $\langle F_1, \ldots, F_p \rangle$

Let $\mathbb{Q}_d[X_1, \ldots, X_n] = \{F \in \mathbb{Q}[X_1, \ldots, X_n] \mid \deg(F) \leq d\}$.

Note that $\langle F_1, \ldots, F_p \rangle \cap \mathbb{Q}_d[X_1, \ldots, X_n]$ is a finite-dimensional $\mathbb{Q}$-vector space.

$\rightarrow$ reductions to linear algebra are around.

Let $\pi_i : (x_1, \ldots, x_n) \rightarrow (x_1, \ldots, x_i)$.

Elimination theorem

$\langle F_1, \ldots, F_p \rangle \cap \mathbb{Q}[X_1, \ldots, X_i]$ defines the Zariski closure of $\pi_i(V)$.

Gröbner bases (I)

$$F_1 = \cdots = F_p = 0 \quad \text{in} \quad \mathbb{Q}[X_1, \ldots, X_n]$$

Assume that the number of monomials == the number of equations

$$\begin{cases} X_1X_2 + X_3^2 - X_2X_3 &= 1 \\ X_1X_2 + 2X_3^2 + X_2X_3 &= 3 \\ 5X_1X_2 - X_3^2 + X_2X_3 &= 7 \end{cases}$$

- Substitute monomials by new variables

$$\begin{cases} Y_1 + Y_2 - Y_3 &= 1 \\ Y_1 + 2Y_2 + Y_3 &= 3 \\ 5Y_1 - Y_2 + Y_3 &= 7 \end{cases} \rightsquigarrow \begin{matrix} F_1 \rightarrow \\ F_2 \rightarrow \\ F_3 \rightarrow \end{matrix} \begin{bmatrix} 1 & 1 & -1 & 1 \\ 1 & 2 & 1 & 3 \\ 5 & -1 & 1 & 7 \end{bmatrix}$$

- Solve the linear system (gaussian elimination) and retrieve the initial solutions

BUT, usually number of equations $\ll$ number of monomials

Gröbner bases (II)

Need of more rewriting rules $\rightsquigarrow$ monomial ordering $\rightsquigarrow$ Macaulay's matrix

$$\mathsf{Mac}_{\succ}(\mathbf{F}, d) = \begin{array}{c} \\ t_1 F_1 \rightarrow \\ \vdots \\ t_k F_p \rightarrow \end{array} \begin{array}{c} \begin{array}{cccc} m_1 & \cdots & \cdots & m_{\ell(d),d} \end{array} \\ \begin{bmatrix} \cdots & \cdots & \cdots & \cdots \\ \ddots & \vdots & \vdots & \vdots \\ \cdots & \cdots & \cdots & \cdots \end{bmatrix} \end{array} \quad \text{with } d \geq \deg(t_i F_j)$$

Property For d large enough, a row echelon form of $\mathsf{Mac}_{\succ}(\mathbf{F}, d)$ provides a basis of $\langle \mathbf{F} \rangle \cap \mathbb{Q}_d[\mathbf{X}]$

Gröbner bases (FGb, Magma, ...) Buchberger, Faugère (F4 and F5)

Finite case When $\sharp\mathsf{Sols} < \infty$, $q(T) = 0, X_1 = q_1(T), \ldots, X_n = q_n(T)$

from a Gröbner basis + extra linear algebra operations

From semi-algebraic sets to real algebraic sets

Let $S \subset \mathbb{R}^n$ be defined by

$$F_1 = \cdots = F_p = 0, \quad G_1 > 0, \ldots, G_s > 0$$

and C be a connected component of S.

Theorem There exists $e > 0$ s.t. for any $0 < e' < e$ the following holds.

There exists $\{i_1, \ldots, i_\ell\} \subset \{1, \ldots, s\}$ and a connected component C' of the real algebraic set defined by

$$F_1 = \cdots = F_p = 0, \quad G_{i_1} = \cdots = G_{i_s} = e'$$

such that $C' \subset C$.

Sample points: first reduction

System of equations and inequalities in $\mathbb{Q}[X_1, \ldots, X_n]$

$\Downarrow$

Systems of equations in $\mathbb{Q}[X_1, \ldots, X_n]$

$\Downarrow$

Systems of equations in $\mathbb{Q}[X_1, \ldots, X_n]$
with finitely many complex solutions

$\Downarrow$

Rational parametrizations $q(T) = 0, X_i = q_i(T)/q_0(T)$

We retrieve a univariate situation.

One-Block Quantifier Elimination: second reduction

$$\boxed{\exists \mathbf{X} \in \mathbb{R}^n \Phi(\mathbf{X}, \mathbf{Y}) \Longleftrightarrow \Psi(\mathbf{Y})}$$

This can be seen as a **decision problem with parameters**

$\rightarrow$ running algorithms for computing sample points yield

$$q(Y_1, \ldots, Y_r, T) = 0, \qquad X_i = q_i(Y_1, \ldots, Y_r, T)/q_0(Y_1, \ldots, Y_r, T)$$

$$\Downarrow$$

$$\boxed{\text{Sturm-like algorithm on } q(Y_1, \ldots, Y_r, T) = 0}$$

$$\Downarrow$$

$$\boxed{\text{Conditions on } Y_1, \ldots, Y_r}.$$

Connectivity queries: third reduction

Connectivity queries in semi-algebraic sets

$\Downarrow$

Connectivity queries in real algebraic sets

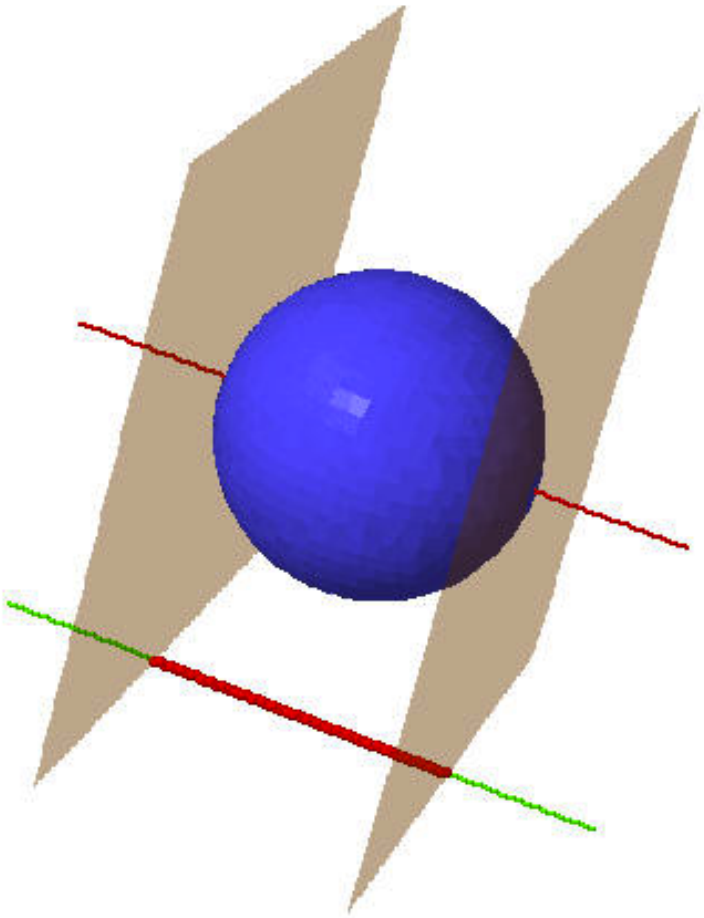
$\Downarrow$

Reduction to the curve case.

$$q(U,T) = 0, \qquad X_i = q_i(U,T)/q_0(U,T)$$

We retrieve a bivariate situation.

Polynomial optimization – Critical points (I)



Reduction of the dimension through Global Optimization

Properties of Critical Points

Vorobjov, Renegar, Gournay/Risler, Heintz/Roy/Solerno, Basu/Pollack/Roy 96

Polynomial optimization – Critical points and polar variety (II)

For $1 \leq i \leq n$, let $\pi_i : (\mathbf{x}_1, \ldots, \mathbf{x}_n) \to (\mathbf{x}_1, \ldots, \mathbf{x}_i)$ and $\mathbf{F} = (F_1, \ldots, F_p)$

$$V = V(\mathbf{F}) \subset \mathbb{C}^n,\ \mathrm{jac}(\mathbf{F}, i) = \begin{bmatrix} \frac{\partial F_1}{\partial X_{i+1}} & \cdots & \cdots & \frac{\partial F_1}{\partial X_n} \\ \frac{\partial F_2}{\partial X_{i+1}} & \cdots & \cdots & \frac{\partial F_2}{\partial X_n} \\ \vdots & & & \vdots \\ \frac{\partial F_p}{\partial X_{i+1}} & \cdots & \cdots & \frac{\partial F_p}{\partial X_n} \end{bmatrix},\ \mathrm{jac}(\mathbf{F}) = \mathrm{jac}(\mathbf{F}, 0).$$

Polar variety $\mathrm{crit}(\pi_i, V)$ **associated to** π_i **and** $V = V(F_1, \ldots, F_p) \subset \mathbb{C}^n$

$$F_1 = \cdots = F_p = 0 \quad \text{and} \quad \mathsf{rank}\,(\mathrm{jac}(\mathbf{F}, i)) \leq p - 1$$

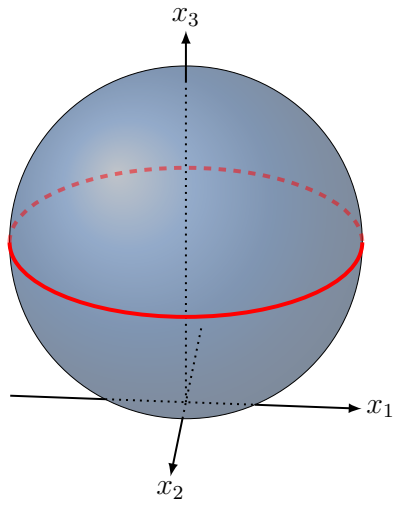
Regularity hyp.: $\mathrm{reg}(V) = \{x \in V \mid \mathsf{rank}\,(\mathrm{jac}_x(\mathbf{F})) = p\}$ is Zariski dense in V.

Critical points $\mathrm{crit}(\pi_i, V) \cap \mathrm{reg}(V)$.

Critical values image by π_i of the critical locus.

Polynomial optimization – Critical points (III)

Example: $F_1 = X_1^2 + X_2^2 + X_3^2 - 1$



- $i = 2,\ F = \frac{\partial F}{\partial X_3} = 0$
- $i = 1,\ F = \frac{\partial F}{\partial X_3} = \frac{\partial F}{\partial X_2} = 0$

Modelings

▷ **Minors of the truncated jacobian matrix** $\rightsquigarrow$ Determinantal modeling

▷ **Linearly independant vectors in the kernel** $\rightsquigarrow$ Lagrange system

$$\mathbf{F} = 0, \qquad \Lambda \cdot \mathrm{jac}(\mathbf{F}, 1) = \mathbf{0}, \quad \mathbf{u} \cdot \Lambda = 1$$

Can we compute efficiently finitely many critical points?

(Arithmetic) Complexity results

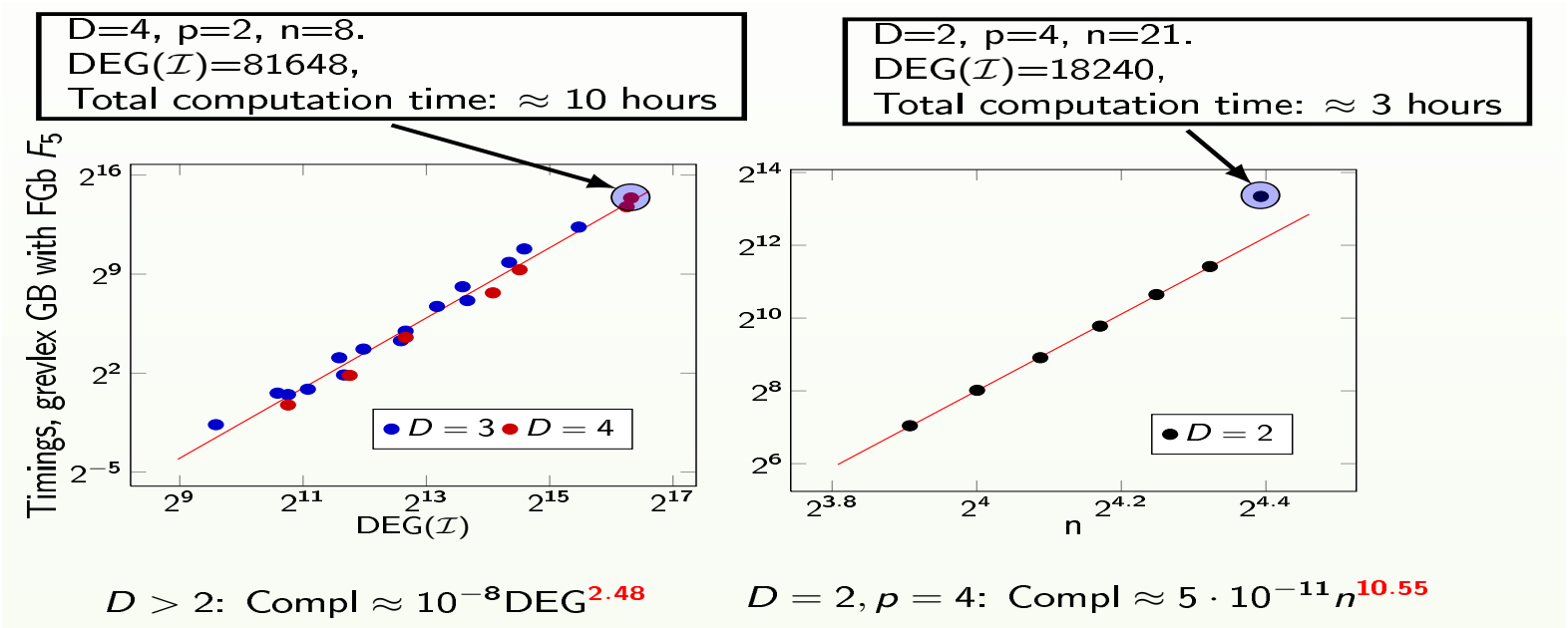
(determinantal modeling, $\deg(F_i) = D$ for $1 \leq i \leq p$)

- $\mathbb{D}_{\text{reg}} \leq D(p-1) + (D-2)n + 2$, $\quad \sharp\text{Sols} \leq D^p(D-1)^{n-p}\binom{n-1}{p-1}$
- When $D = 2$, $O(n^{2p\omega})$
- $O\left(\frac{1}{\sqrt{n}}((D-1)e)^{n\omega}\right)$ if $D > 2$ and p is fixed.

(Arithmetic) Complexity results

(determinantal modeling, $\deg(F_i) = D$ for $1 \le i \le p$)

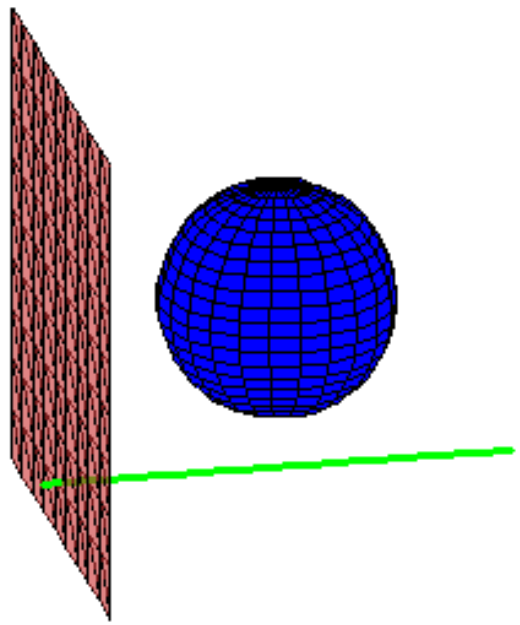
- $\mathbb{D}_{\text{reg}} \le D(p-1) + (D-2)n + 2$, $\quad \sharp\text{Sols} \le D^p (D-1)^{n-p} \binom{n-1}{p-1}$
- When $D = 2$, $O(n^{2p\omega})$
- $O\left(\frac{1}{\sqrt{n}}((D-1)e)^{n\omega}\right)$ if $D > 2$ and p is fixed.



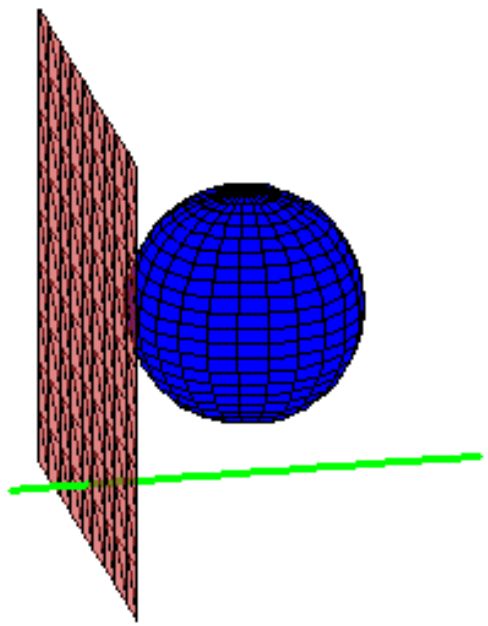
Part III:

Computing sample points in semi-algebraic sets

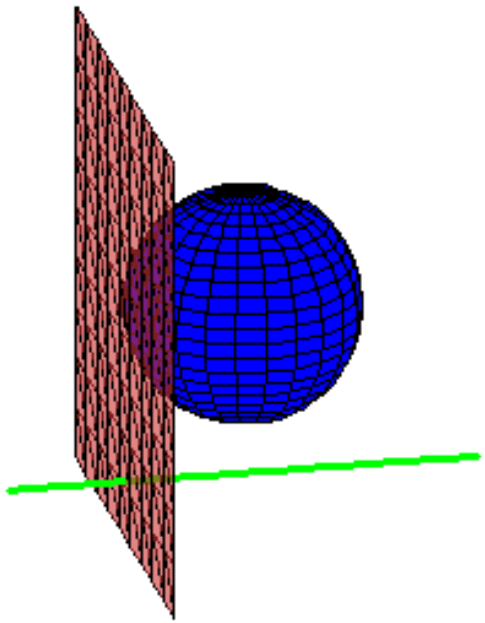
A = -1.8333



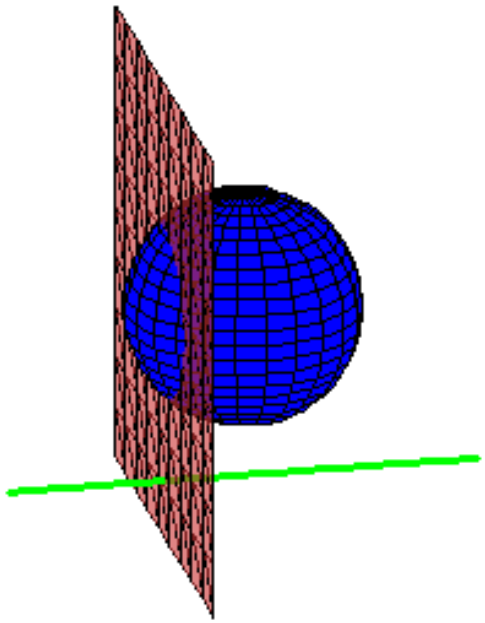
A = -1.3333



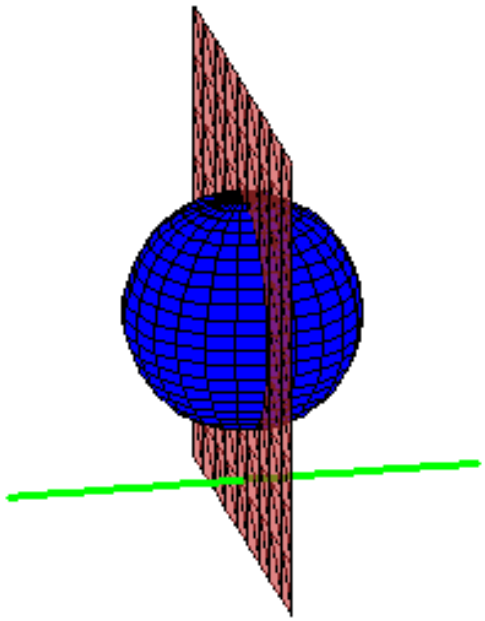
A = -1.0000



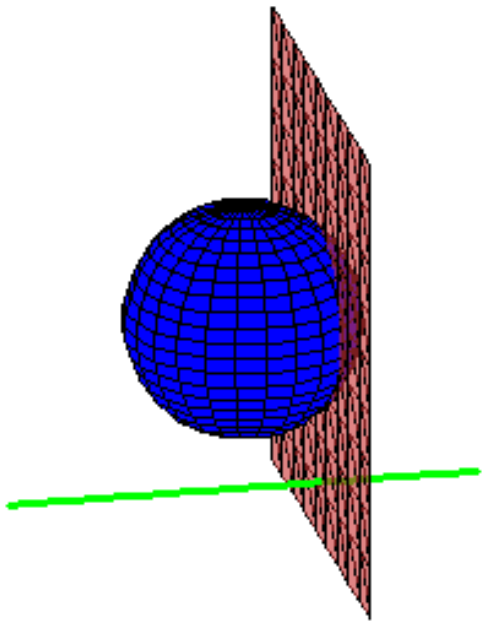
A = -.66667



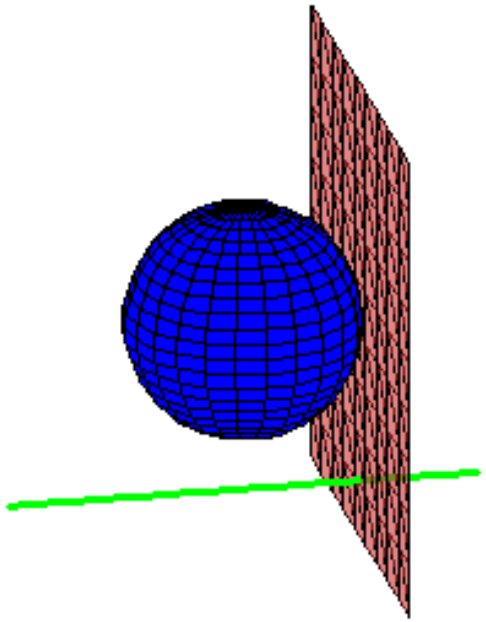
A = 0.



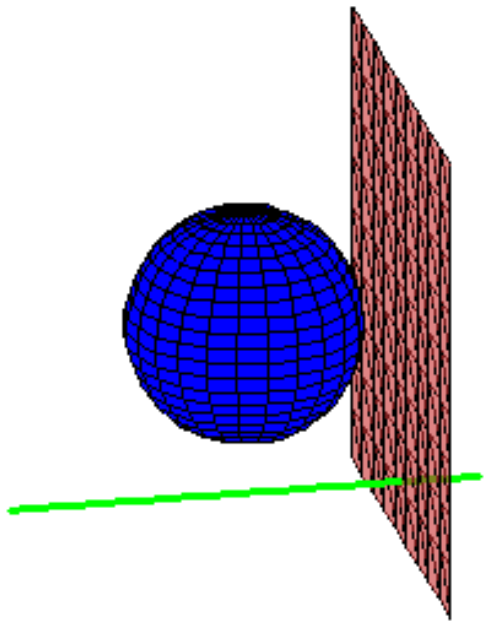
A = .66667



A = 1.0000



A = 1.3333



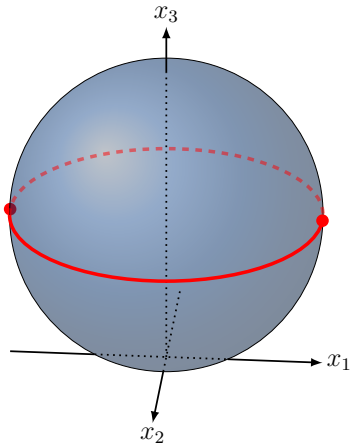
Geometry of polar varieties (I)

Let $V = \{\mathbf{x} \in \mathbb{C}^n \mid F_1(\mathbf{x}) = \cdots = F_p(\mathbf{x}) = 0\}$

Regularity assumption: $\boxed{V - \mathrm{reg}(V) \text{ is finite.}}$

Transfer of properties of V to polar varieties in generic coordinates.

We need first to control the dimension of polar varieties

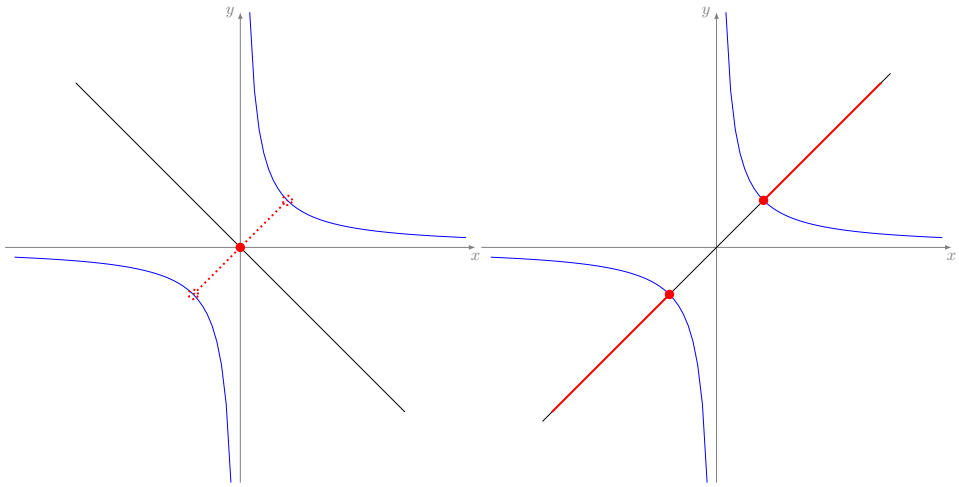


Dimension is well controlled

$$\boxed{\mathrm{crit}(\pi_1, V) \subset \mathrm{crit}(\pi_2, V) \subset \cdots \subset \mathrm{crit}(\pi_i, V)}$$

$$\boxed{\dim(\mathrm{crit}(\pi_1, V)) = 0, \dim(\mathrm{crit}(\pi_2, V)) = 1, \ldots, \dim(\mathrm{crit}(\pi_i, V)) = i - 1}$$

Geometry of polar varieties (II)



Closedness of projections. Let C be a connected comp. of $V \cap \mathbb{R}^n$.
$\text{crit}(\pi_1, V) \cap C = \emptyset$ and $V \cap \mathbb{R}^n \neq \emptyset \Longrightarrow \pi_1(V \cap \mathbb{R}^n) = \mathbb{R}$

Transfer of **Noether position** properties to polar varieties.

Can be checked algebraically

Algorithmic consequence. In generic coordinates

- If V is finite, compute a parametrization of V else
- Compute $\text{crit}(\pi_1, V)$
- Recursive call to $V \cap \pi_1^{-1}(0)$

Summary

	Before	**Now**
Existence	$D^{O(n)}$	$\simeq O(D^{3n})$ (regular)
		$\simeq O(D^{4n})$ (singular)
1-Block QE	$D^{O(r(n-r))}$	$\simeq O(D^{3r(n-r)})$ (boundary of projection)

Software RAGlib (Real Algebraic Geometry Library)

Scales to $\simeq$ 8–10 variables ($D = 4$, $n = 8$, dense equation $\rightarrow$ 2 hours)

Applications in biology, comput. geometry, numerical analysis, robotics, etc.

- Non-validity of models in bio-informatics
- Discovery fo the stability region of MacCormack's scheme for PDEs
- Computational geometry: Voronoi diagram, Perspective problems, etc.

HRL LABORATORIES, LLC

Used for an engineering application

Systems of inequalities with $\simeq$ 6 $\rightarrow$ 8 variables

Unreachable by current CAD implementations

Part IV:
Quantifier elimination over the reals

One-block quantifier elimination and its variants

$$\boxed{\exists \mathbf{X} \in \mathbb{R}^n \Phi(\mathbf{X}, \mathbf{Y}) \Longleftrightarrow \Psi(\mathbf{Y})}$$

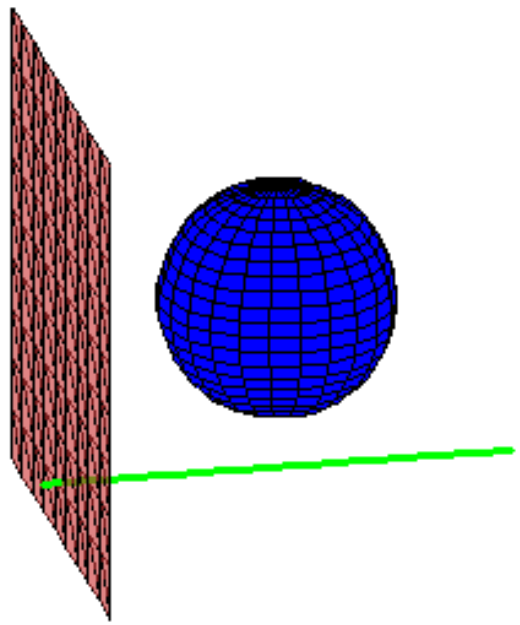
Recall our observations on the length of formula.

- $\exists x \in \mathbb{R} \quad x^2 + bx + c = 0 \Leftrightarrow b^2 - 4c \geq 0$
- $\exists x \in \mathbb{R} \quad ax^2 + bx + c = 0 \Leftrightarrow$
  $(a \neq 0 \wedge b^2 - 4c \geq 0) \vee (a = 0 \wedge b \neq 0) \vee (a = 0 \wedge b = 0 \wedge c = 0)$

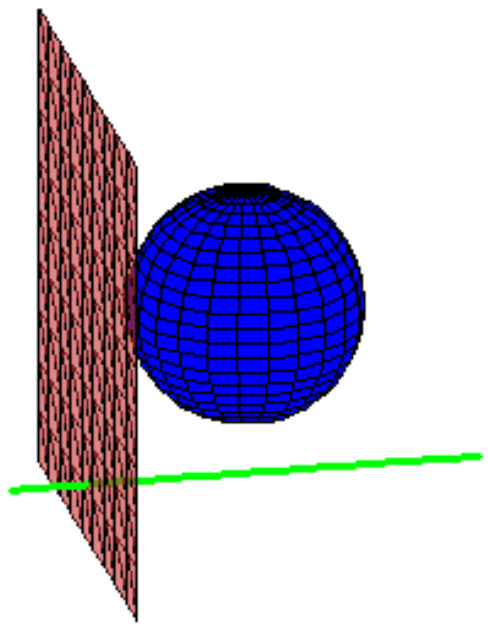
Variant Quantifier Elimination

- Input: $\exists \mathbf{X} \in \mathbb{R}^n \Phi(\mathbf{X}, \mathbf{Y})$
- Output: $\Psi'(\mathbf{Y})$ such that
  - $\mathsf{Sols}(\Psi'(\mathbf{Y})) \subset \mathsf{Sols}(\Psi(\mathbf{Y}))$
  - $\mathsf{Sols}(\Psi(\mathbf{Y})) - \mathsf{Sols}(\Psi'(\mathbf{Y}))$ has dimension less than $\sharp\mathbf{Y}$.

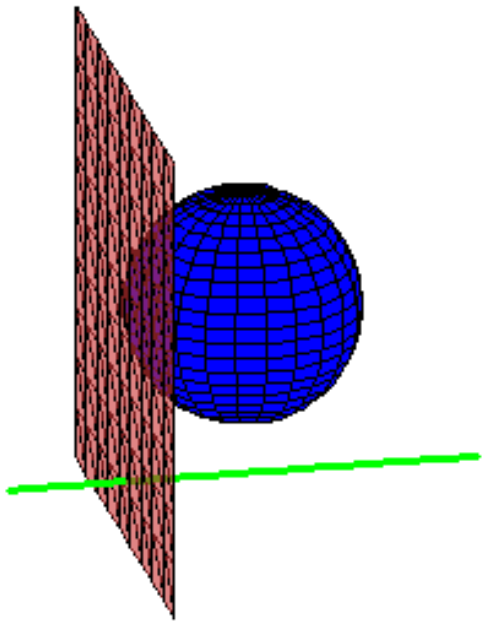
A = -1.8333



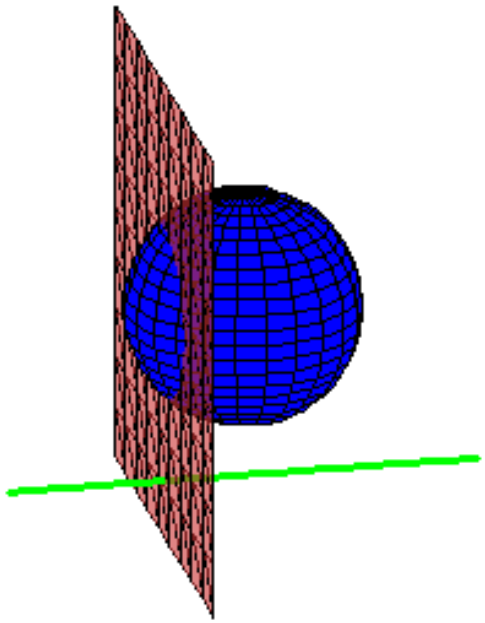
A = -1.3333



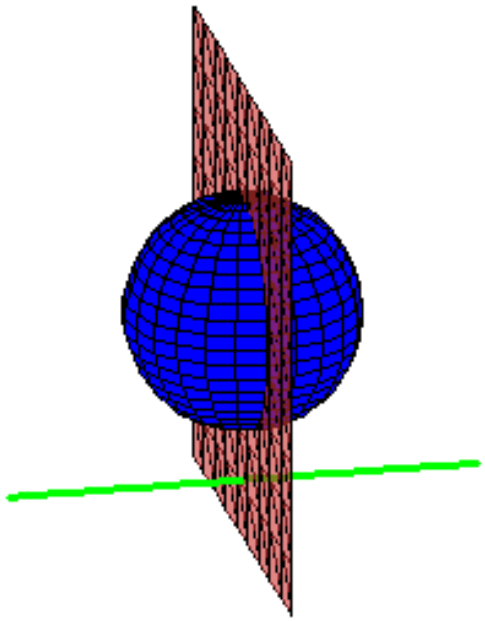
A = -1.0000



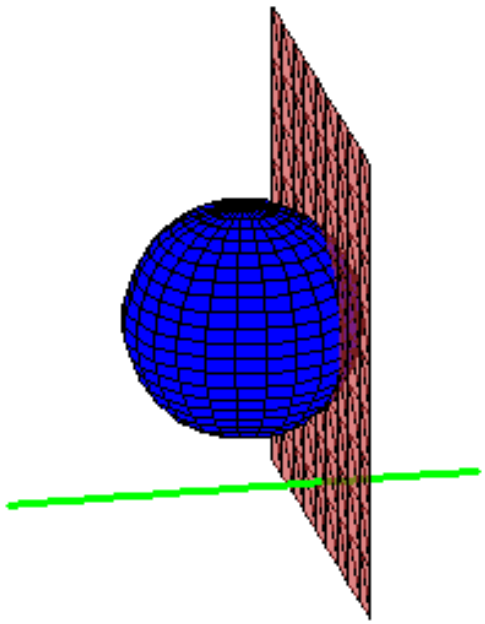
A = -.66667



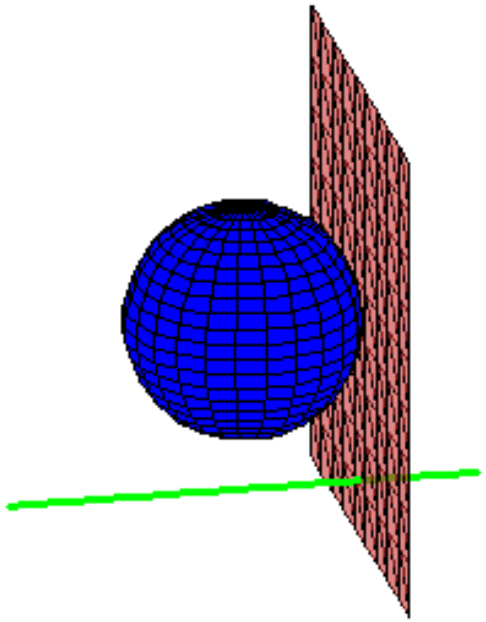
A = 0.



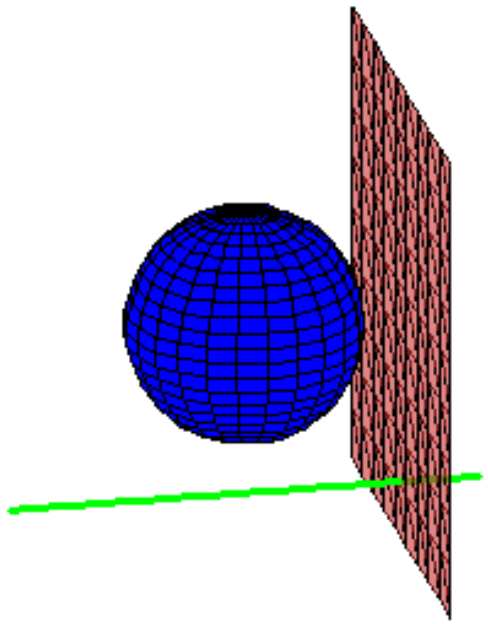
A = .66667



A = 1.0000



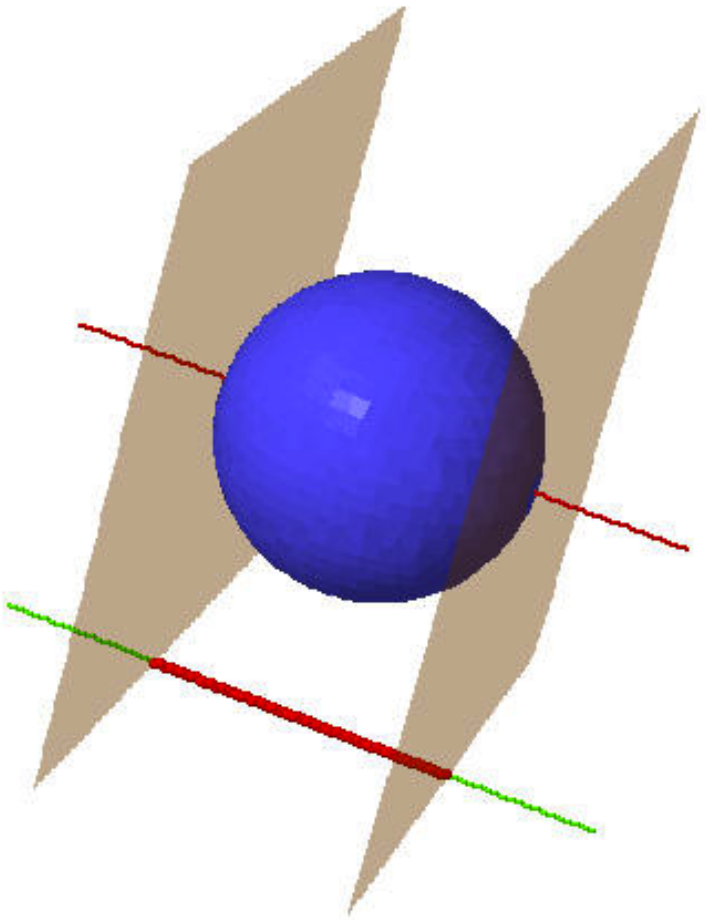
A = 1.3333



From Ehresmann's theorem to Quantifier Elimination

Topology

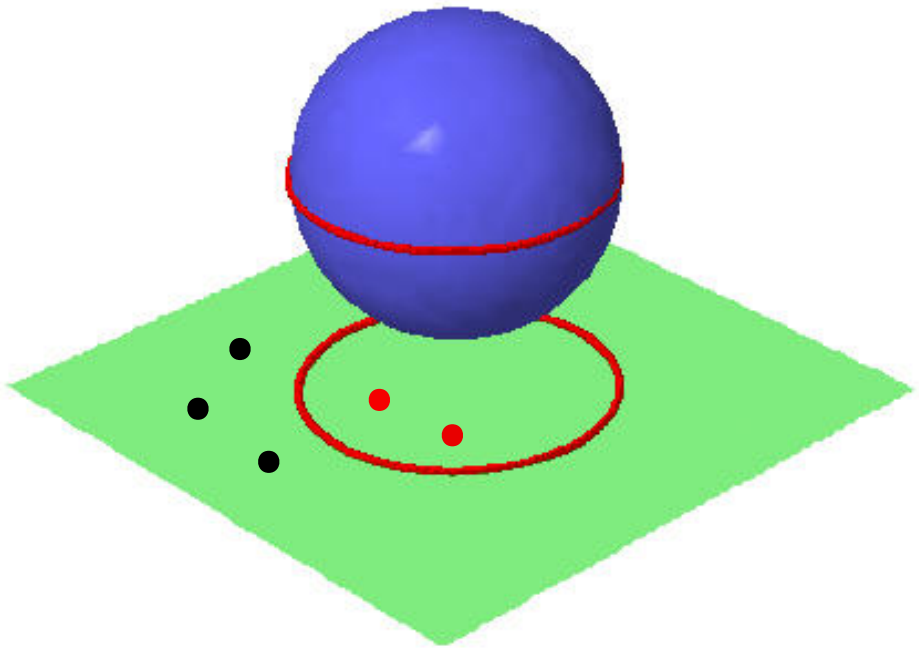
Polar varieties $\leftrightarrow$ Critical points $\leftrightarrow$ Morse theory



Ehresmann's fibration theorem

- Under some **properness assumptions**, the boundary of $\pi_i(V \cap \mathbb{R}^n)$ is contained in the image by π_i of $\mathrm{crit}(\pi_i, V)$.
- Describing the components of the complement of $\pi_i(\mathrm{crit}(\pi_i, V))$ allows to solve our VQE problem.
- Projection of critical points computed with evaluation/interpolation techniques

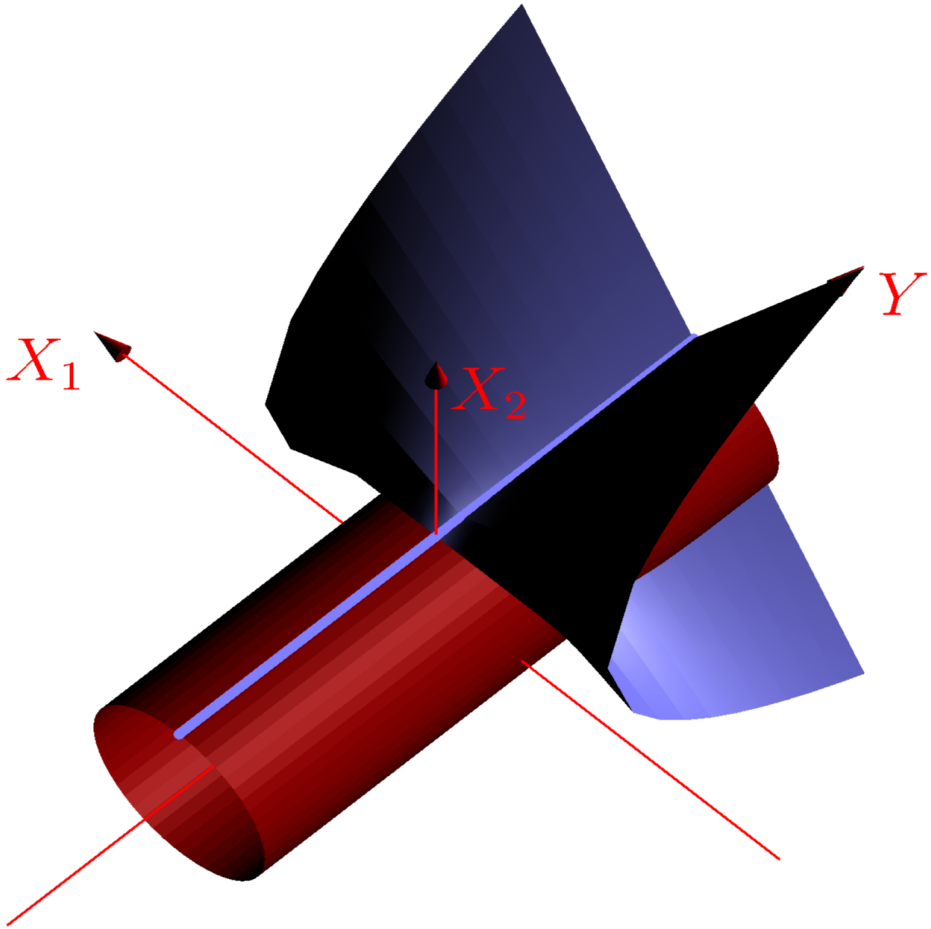
Asymptotically optimal complexity.



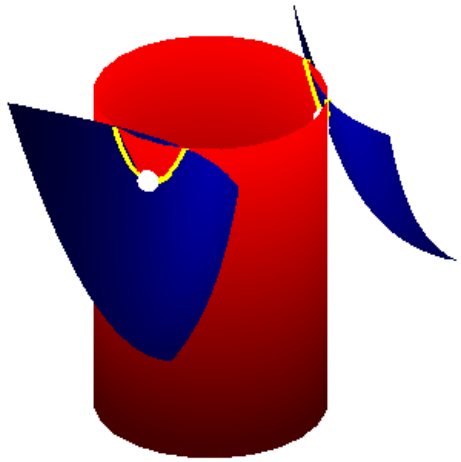
Singular situations

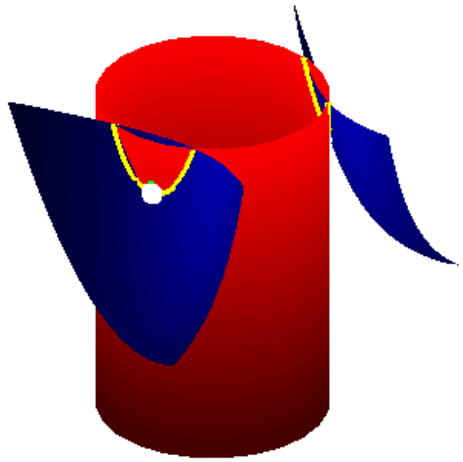
We want to compute $\pi_{\mathbf{Y}}(\{(x,y) \in \mathbb{R}^n \times \mathbb{R}^t \mid \mathbf{F}(x,y) = 0, \mathbf{G}(x,y) > 0\})$.

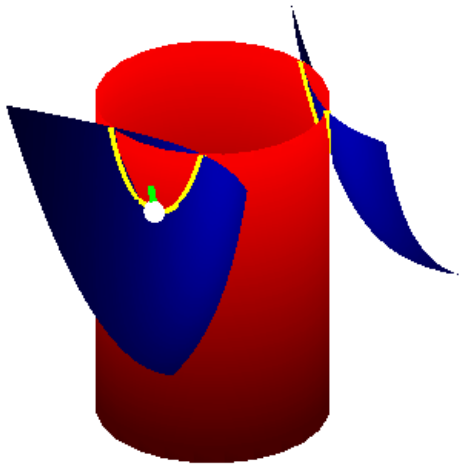
$\boxed{\mathbf{F} = \mathbf{G} = 0}$ with $\sharp\{\mathbf{x} \in V(\mathbf{F},\mathbf{G}) \mid \mathrm{jac}_x(\mathbf{F},\mathbf{G}) \text{ rank defective}\} = \infty$

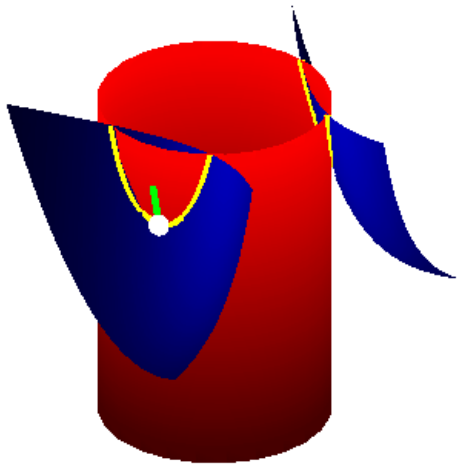


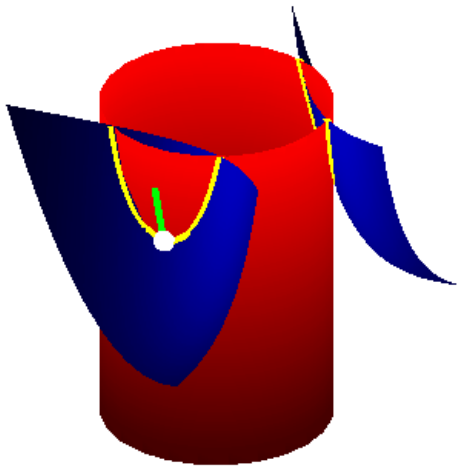
Regularization techniques: $\rightsquigarrow \mathbf{F} = 0, G = \varepsilon$ | ideal theoretic operations |

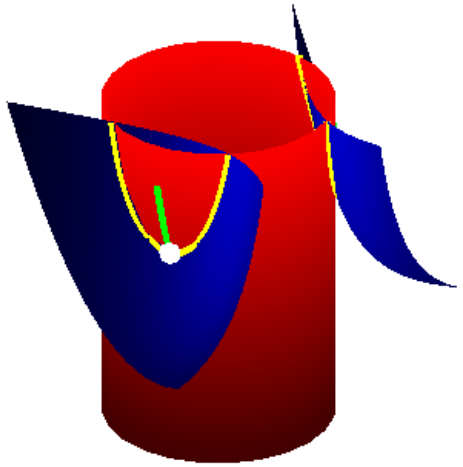


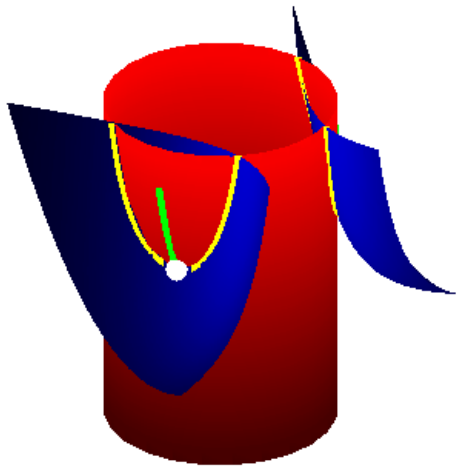


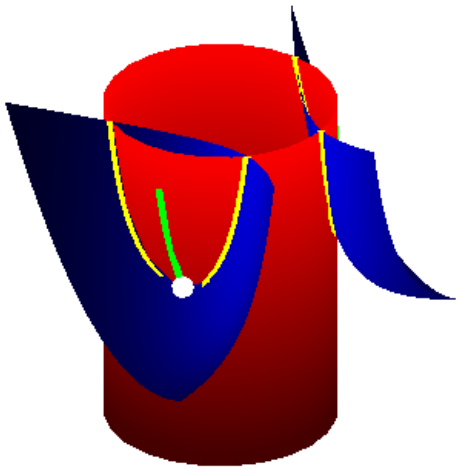


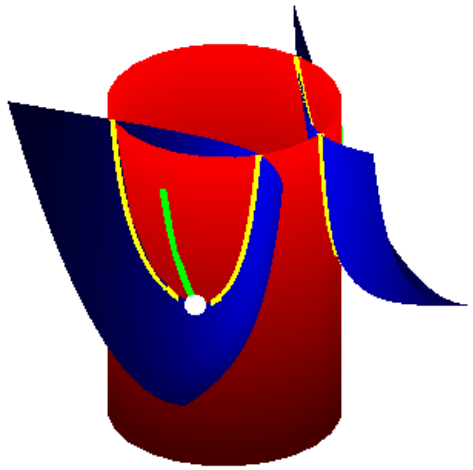


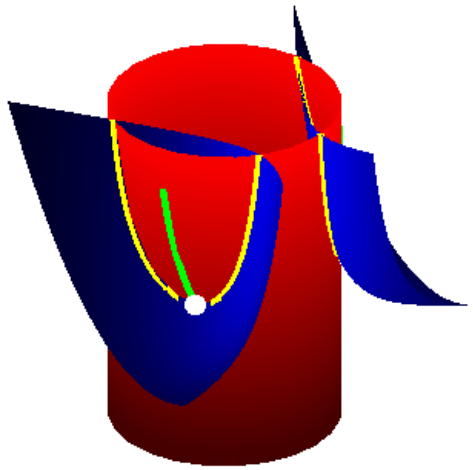


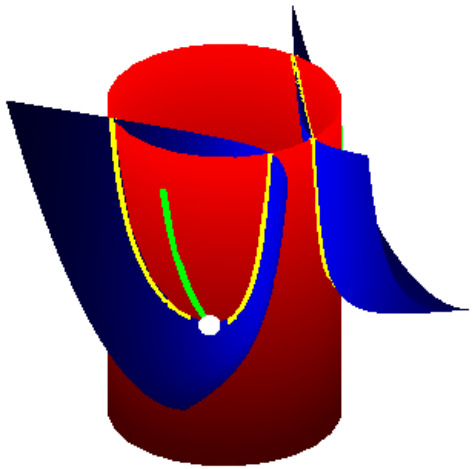


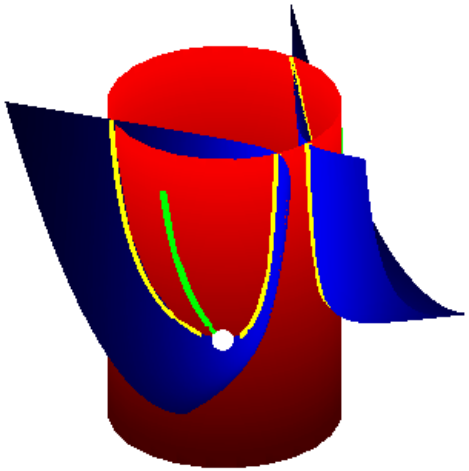


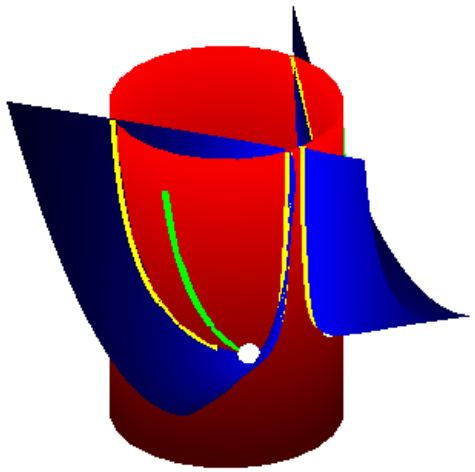


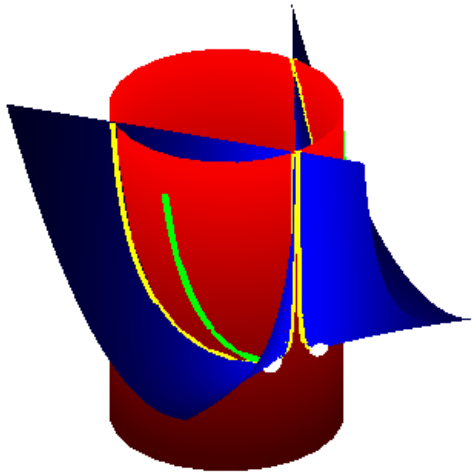


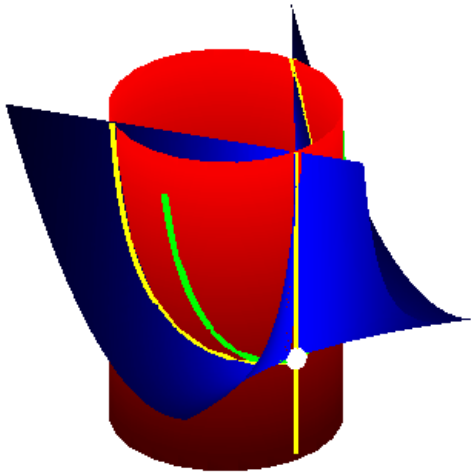










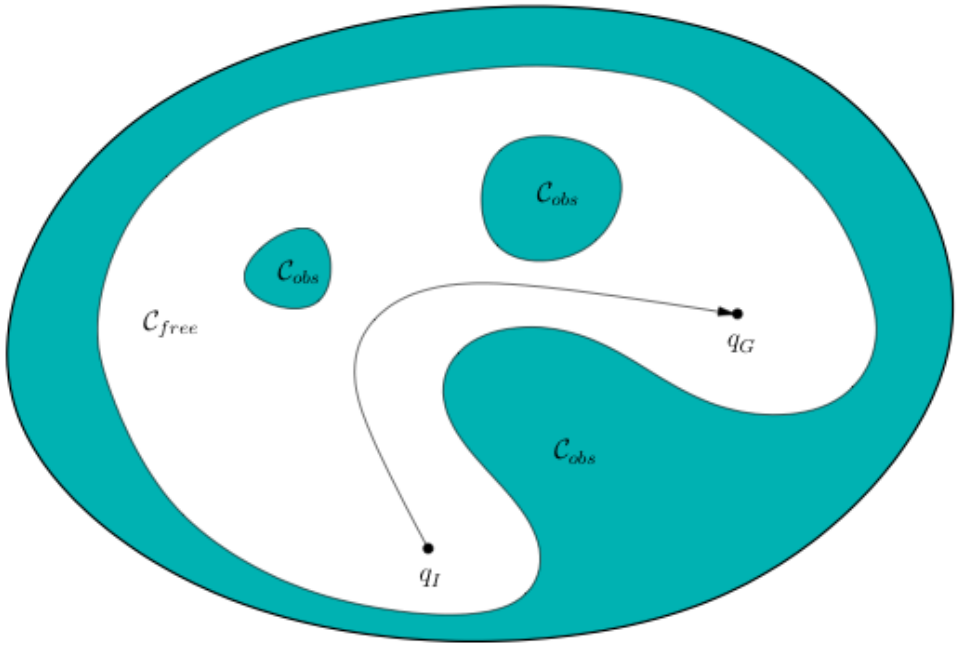


Some practical results

	IBVP	LW	LV	MC	Stab1	Stab2
$[n, t, D]$	[6,2,2]	[4,2,6]	[4,2,7]	[4,2,14]	[4,2,2]	[4,2,2]
QEPCAD	∞	∞	∞	∞	∞	∞
Mathematica	∞	∞	∞	∞	∞	∞
VQE	13.5 sec.	18.5 sec.	63 sec.	$\approx$ 12h	$\approx$ 1.6h	$\approx$ 2.3h
VQE Proj	6 sec.	4 sec.	7 sec.	$\approx 3h$	35 sec.	12.5 min.
Dec+Lift	8 sec.	16 sec.	55 sec.	9 h.	1.5h	2h.
				$\approx$8000	$\approx$7000	$\approx$9000

Part V:
Connectivity queries

Connectivity queries



Roadmaps

Consider an algebraic set V.

An algebraic set $\mathscr{R} \subset \mathbb{C}^n$ is a roadmap of V if:

- Each connected component of $V \cap \mathbb{R}^n$ has a non-empty and connected intersection with $\mathscr{R} \cap \mathbb{R}^n$.
- $\mathscr{R}$ is contained in V.
- $\mathscr{R}$ is a curve.

Adding a finite set of control points $\mathscr{P}$ to our input, $\mathscr{R}$ is a roadmap of $(V, \mathscr{P})$ if we also have:

- $\mathscr{R}$ contains $\mathscr{P}$.

Roadmaps

Consider an algebraic set V.

An algebraic set $\mathscr{R} \subset \mathbb{C}^n$ is a roadmap of V if:

- Each connected component of $V \cap \mathbb{R}^n$ has a non-empty and connected intersection with $\mathscr{R} \cap \mathbb{R}^n$.
- $\mathscr{R}$ is contained in V.
- $\mathscr{R}$ is a curve.

Adding a finite set of control points $\mathscr{P}$ to our input, $\mathscr{R}$ is a roadmap of $(V, \mathscr{P})$ if we also have:

- $\mathscr{R}$ contains $\mathscr{P}$.

Upshot: once we have the roadmap, we have to decide connectivity on a space curve; *relatively* easy.

Roadmaps have become *"standard"* tools to high-level algorithms in real algebraic geometry

Basic and fundamental routine in effective real algebraic geometry

- Semi-algebraic description of connected components
- Classification problems for polynomial systems with parameters
- Quantifier elimination over the reals
- Useful for computing the real dimension of semi-algebraic sets

Encoding roadmaps

Roadmaps are (semi)-algebraic curves

$$q(U,V)=0, \begin{cases} X_1 = q_1(U,V)/q_0(U,V) \\ \vdots \\ X_n = q_n(U,V)/q_0(U,V) \end{cases}$$

with q unitary in U and V, $\delta = \deg(q) \geq \deg(q_i)$.

Remarks:

- The size of the output is quadratic in $\delta = \deg(q)$;
- Any algorithm that runs in time $\simeq O(\delta^3)$ is subquadratic in the output size.

New results

S./Schost (2011):

- $V = V(f)$; $f \in \mathbb{Q}[X_1, \ldots, X_n]$ of degree d.
- $V \cap \mathbb{R}^n$ is compact
- V has finitely many singular points

There exists a probabilistic algorithm computing a roadmap of V in time $(nd)^{O(n^{1.5})}$.

New results

S./Schost (2011):

- $V = V(f)$; $f \in \mathbb{Q}[X_1, \ldots, X_n]$ of degree d.
- $V \cap \mathbb{R}^n$ is compact
- V has finitely many singular points

There exists a probabilistic algorithm computing a roadmap of V in time $(nd)^{O(n^{1.5})}$.

Further improvements generalizations by Basu - Roy - S. - Schost (2014), Basu - Roy (2014) and S. - Schost (2014) $\rightsquigarrow\simeq O((nD)^{12n\log(n)})$

Polar varieties

Studied by Bank *et al.* in computational real geometry.

V is a smooth, r-equidimensional algebraic set; we consider projections

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

and

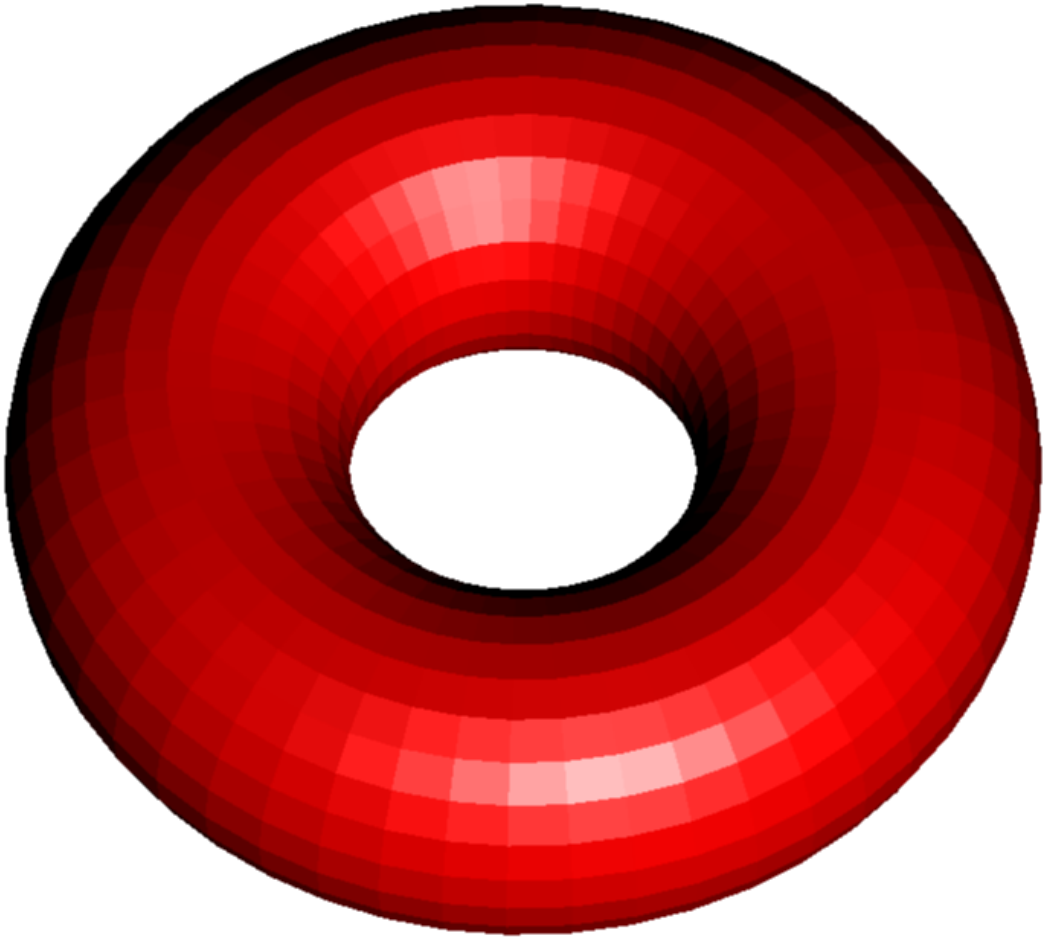
$$\boxed{W_i = \mathrm{crit}(\pi_i, V) = \{\mathbf{x} \in V \mid \pi_i(T_{\mathbf{x}}V) \neq \mathbb{C}^i\}.}$$

W_i is an algebraic set (defined by minors of a Jacobian matrix). Expectedly (in generic coordinates), it has dimension $i - 1$:

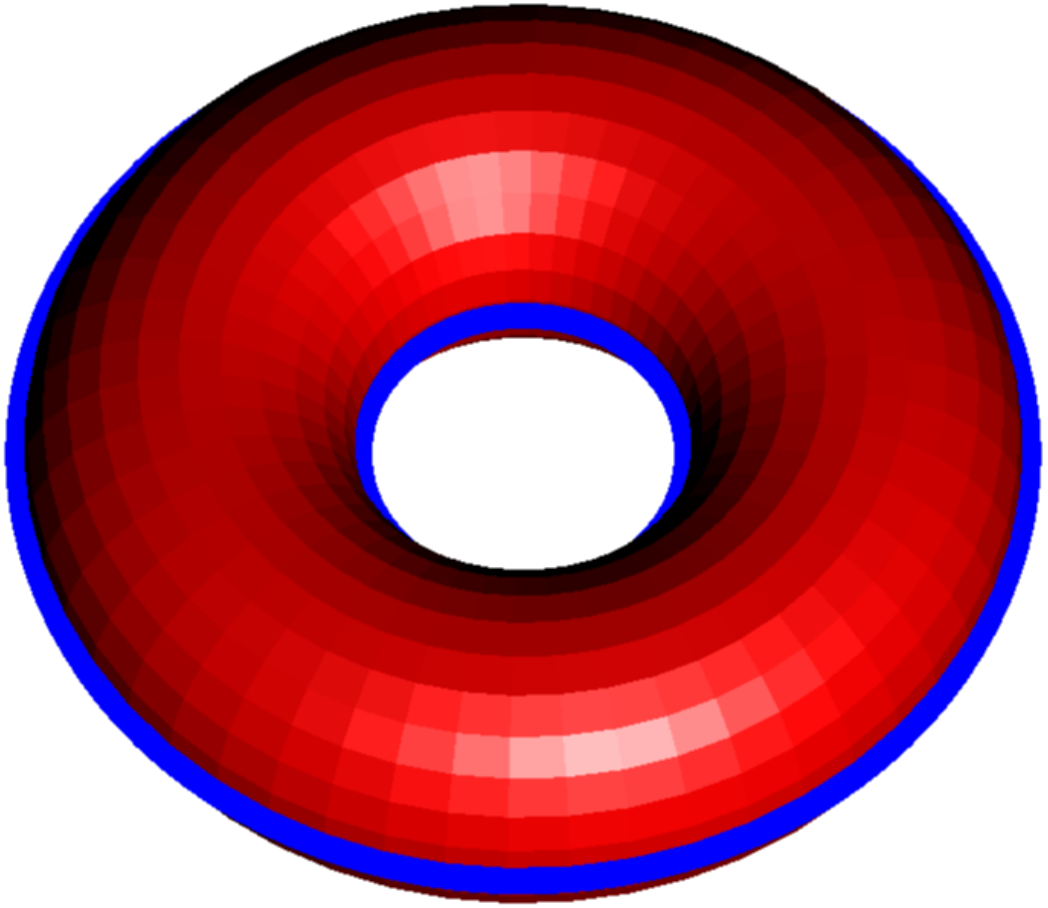
- W_2 is a curve,
- W_1 is a finite of points.

For $i \leq (r+3)/2$, in generic coordinates, W_i is smooth.

Example: torus



Example: torus



A general form of Canny's algorithm

S./Schost 2011

Input / output

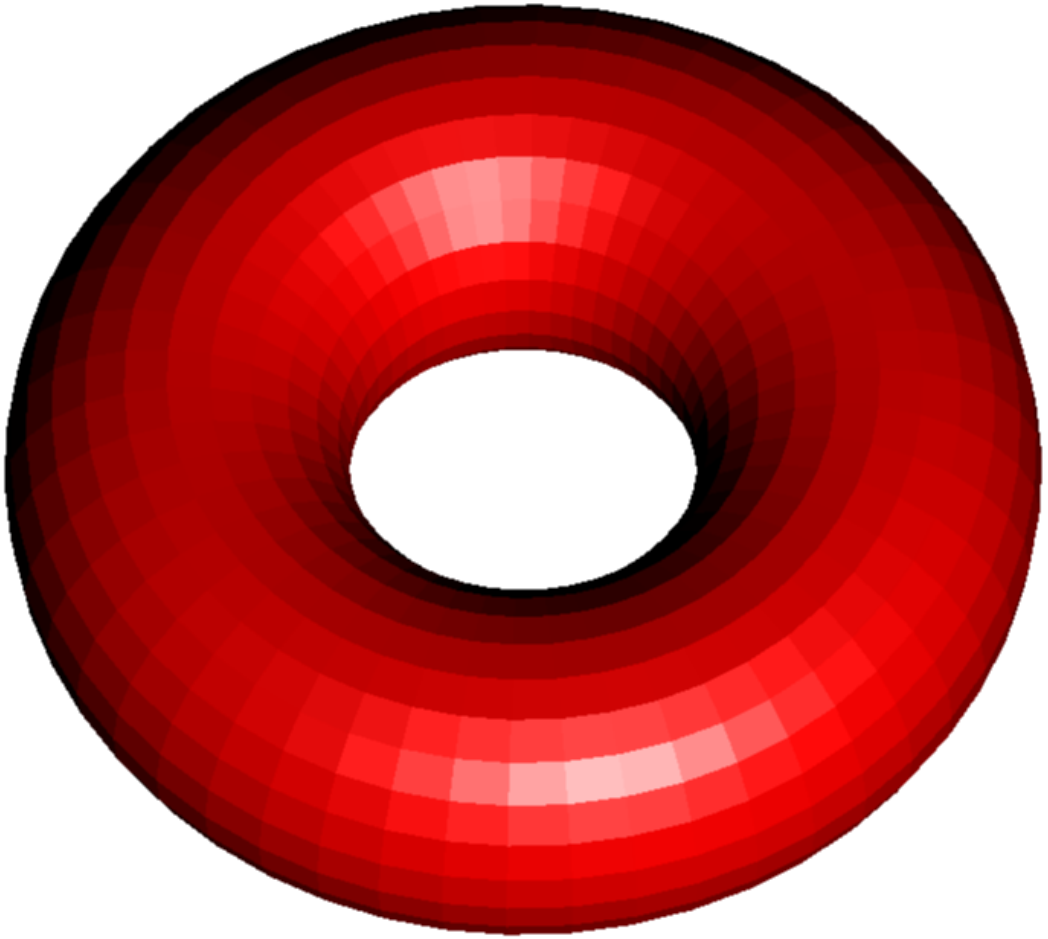
- input: a "nice" system $\mathbf{F} = (f_1, \ldots, f_p)$
  - $V(\mathbf{F}) \cap \mathbb{R}^n$ compact, smooth; regular sequence
  - generic coordinates
- output: a roadmap of $V(\mathbf{F})$

Main idea: for a suitable i

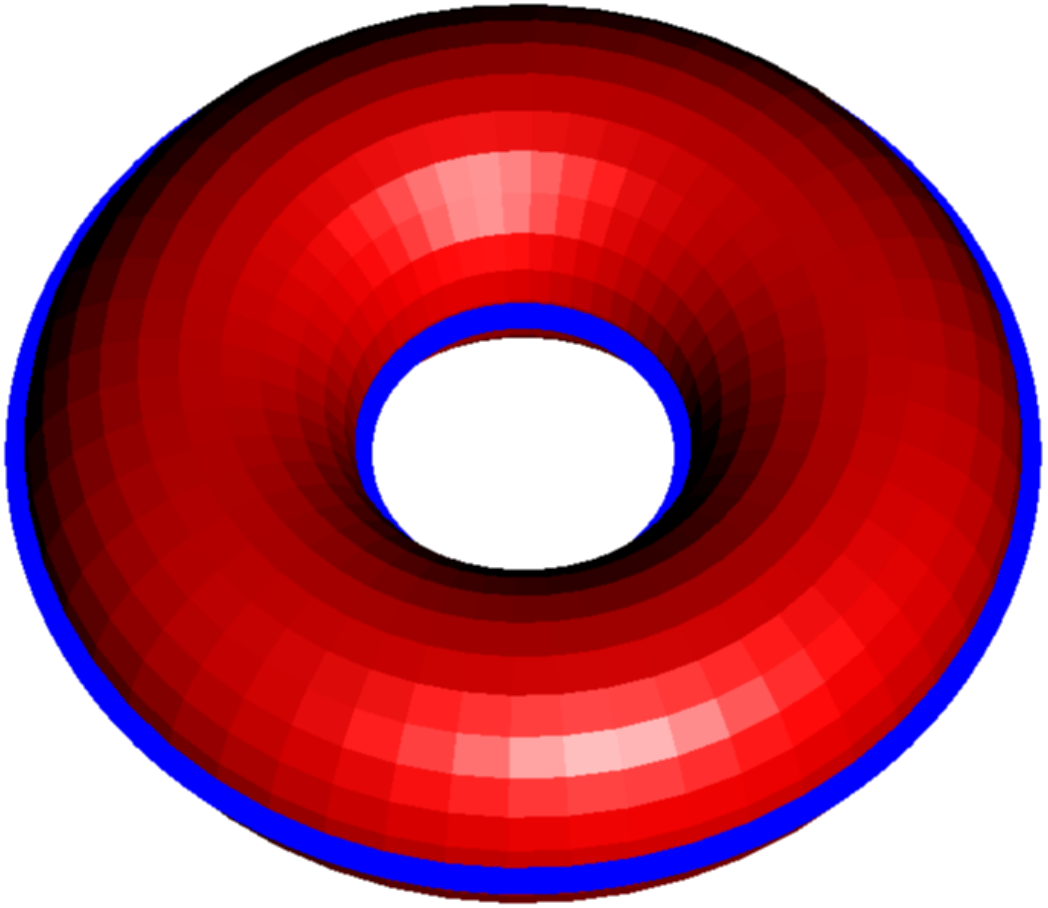
- recursive call on W_i
- recursive call on finitely many fibers of π_{i-1} (about D^n)
- merge the results

Expectedly, running time about $D^{O(\rho n)}$, where ρ is the depth of the recursion.

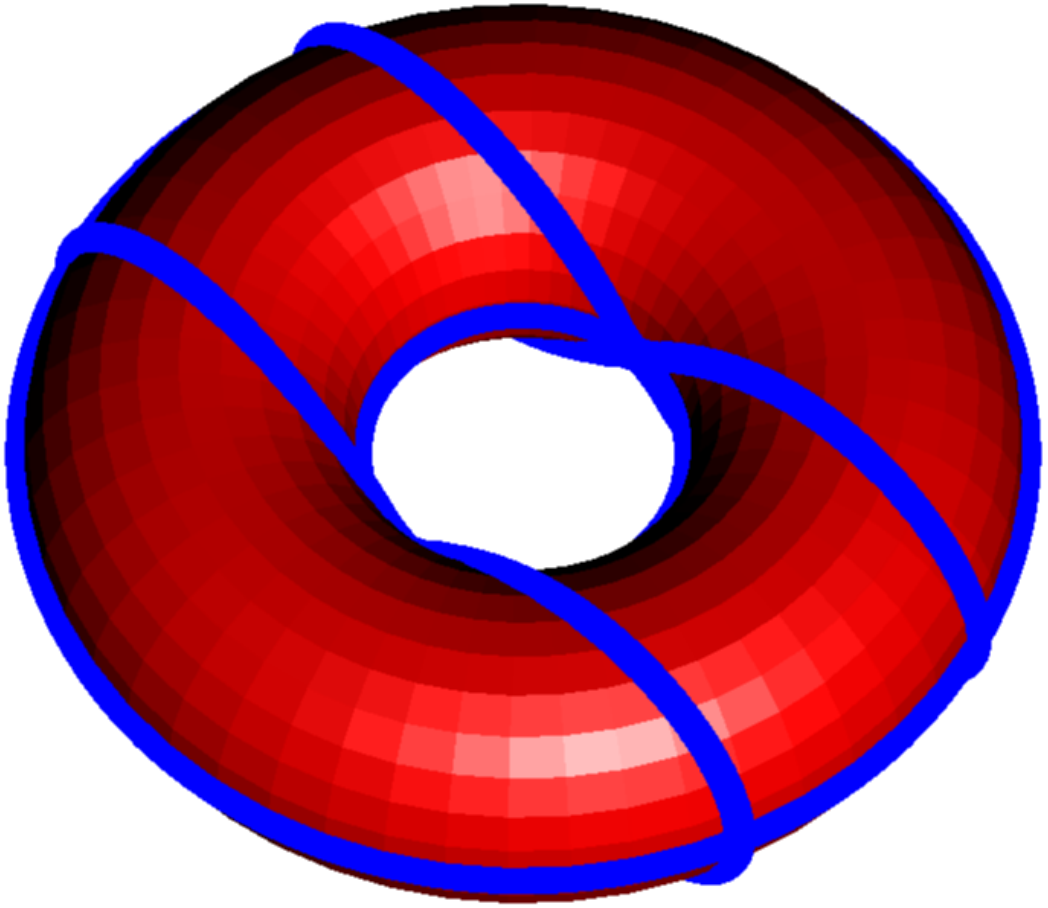
Example: torus



Example: torus



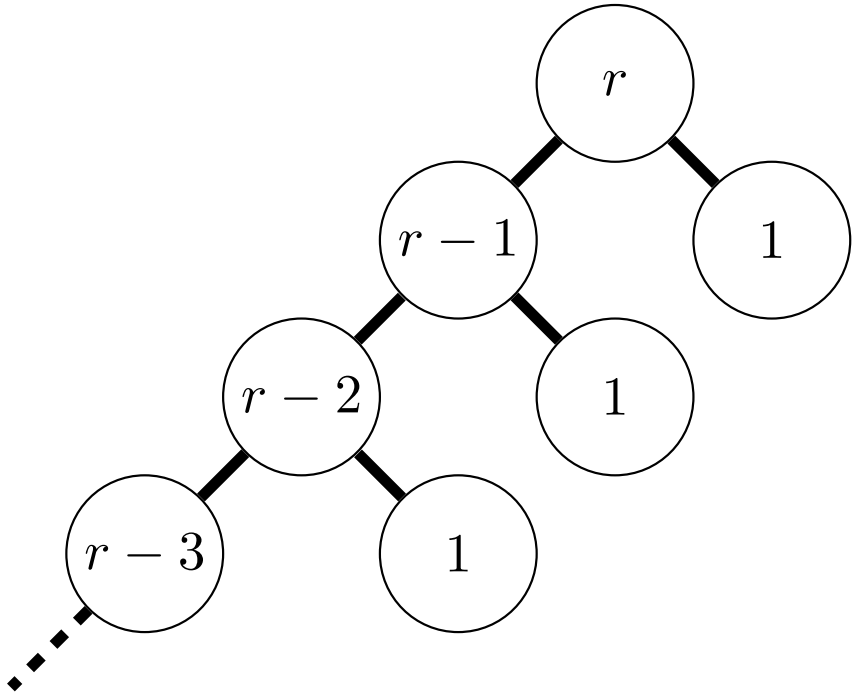
Example: torus



Previous designs: Canny (1988)

Canny

- $i = 2$, so we look at W_2 (curve), and fibers of π_1 (dimension drops by 1)
- recursion of depth n, so $d^{O(n^2)}$



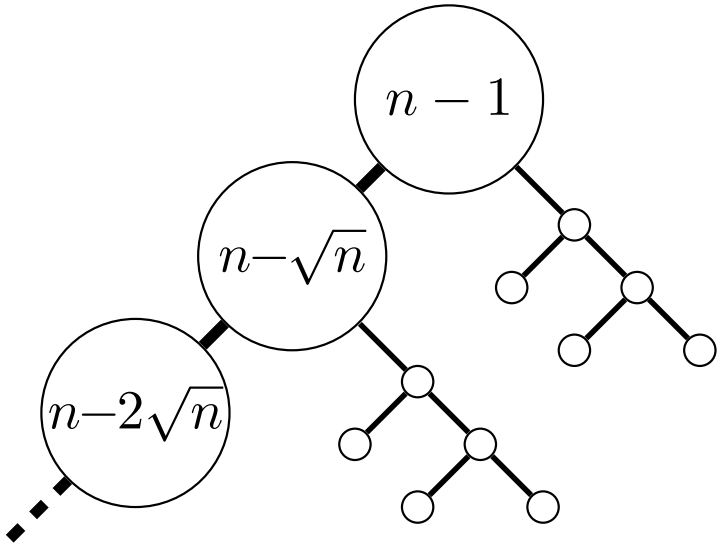
Handles not only hypersurfaces; complete intersections are OK (W_2 is easy and fibers too)

Previous designs: Baby steps - giant steps

S./Schost 2011

V hypersurface

- take $i \simeq \sqrt{n}$
- dimension of $W_i = \sqrt{n} - 1$ (dealt with using Canny's algorithm); fibers are still hypersurfaces
- recursion of depth $\sqrt{n}$, so $D^{O(n^{1.5})}$



generalized to arbitrary algebraic sets Basu/Roy/S./Schost

Conclusions/Perspectives

- Obtaining theoretically and practically fast algorithms is achievable in RAG.
- Develop algorithms for computing certificates (back to Hilbert)
- Develop algorithms for describing the topology of semi-algebraic sets
- Exploit the structure of systems arising comonly in applications
- Last but not least, popularize by investigating new application domains

see Béatrice Bérard's talk.