Variant Real Quantifier Elimination

Algorithm, Implementation, Complexity and Application

M. Safey El Din

INRIA Paris-Rocquencourt SALSA Project-team
Université Pierre et Marie Curie

Joint work with H. Hong
North Carolina State University, USA

Real Quantifier Elimination: Example and Definition

A simple (and well-known example)

$$\exists X \in \mathbb{R} \quad aX^2 + bX + c = 0 \Longleftrightarrow$$
$$\big(a \neq 0 \wedge b^2 - 4ac \geq 0\big) \vee (a = 0 \wedge b \neq 0) \vee (a = 0 \wedge b = 0 \wedge c = 0)$$

More generally, consider

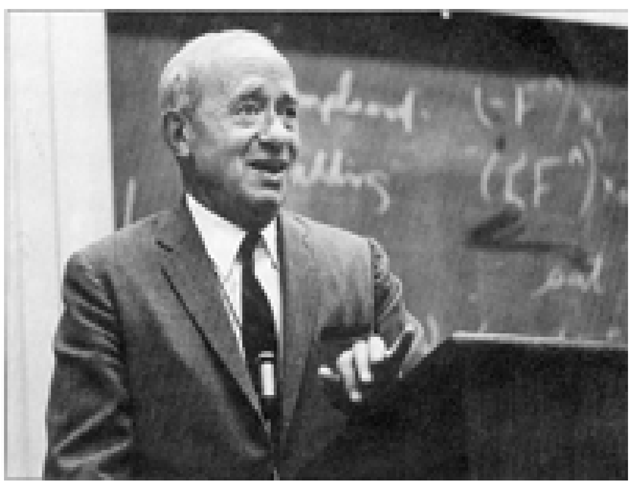
- Blocks of variables $\mathbf{X}^{(1)}, \ldots, \mathbf{X}^{(s)}$ $(\mathbf{X}^{(i)} = [X_1^{(i)}, \ldots, X_{k_i}^{(i)}])$
- A set of *free* variables $\mathbf{Y}$ (parameters)
- Boolean conjunctions of polynomial equations and inequalities $\Psi_1, \ldots, \Psi_r$ lying in $\mathbb{Q}[\mathbf{X}^{(1)}, \ldots, \mathbf{X}^{(s)}, \mathbf{Y}]$
- A formula

$$\mathfrak{Q}_1 \mathbf{X}^{(1)} \in \mathbb{R}^{k_1} \cdots \mathfrak{Q}_s \mathbf{X}^{(s)} \in \mathbb{R}^{k_s} \quad \Psi_1(\mathbf{Y}) \vee \cdots \vee \Psi_r(\mathbf{Y}) \quad (\mathfrak{Q}_i \in \{\forall, \exists\})$$

Real Quantifier Elimination: specifications

$$\mathfrak{Q}_1 \mathbf{X}^{(1)} \in \mathbb{R}^{k_1} \cdots \mathfrak{Q}_s \mathbf{X}^{(s)} \in \mathbb{R}^{k_s} \quad \Psi_1(\mathbf{Y}) \vee \cdots \vee \Psi_r(\mathbf{Y}) \quad (\mathfrak{Q}_i \in \{\forall, \exists\})$$

- Decide if the formula is feasible?
- Compute at least one point in each connected component of the feasicility set (in the real $\mathbf{Y}$-space)
- Compute an equivalent formula without quantifiers



Alfred Tarski (1902-1983). All these problems are **decidable**.

Sur les ensembles définissables de nombres réels, Fund. Math., 1931

A decision method for elementary algebra and geometry, California Press, 1951.

Motivations

Many applications of Real Quantifier Elimination's algorithms

- Historical problem shared by logic, computer algebra, and real algebraic geometry
- Engineering sciences (stability analysis of numerical schemes, control theory, global optimization, computer vision, etc.)
- Automated reasonning, Geometric theorem proving (see D. Kapur's works, Univ. of New Mexico and/or A. Mahboubi's works, INRIA Saclay/LIX)
- Program verification (see D. Monniaux's works, VERIMAG)

Quantifier elimination and Euclide's algorithm

Toy-example: values of a, b, c for which $aX^2 + bX + c$ has a multiple root.

$$\mathsf{Remainder}(aX^2 + bX + c, 2aX + b) = 1/4\,\frac{4\,ac - b^2}{a}$$

- Condition $a \neq 0$ and discussion about the sign of $4\,ac - b^2$ come naturally
- Other conditions corresponds to the case study $a = 0$

Ensuring that the number of real roots of $aX^2 + bX + c$ vary continuously as (a, b, c) varies in $\mathbb{R}^3$ is central and crucial for eliminating the quantifiers

- GCD-computations appear as a central tool – Elimination of variables/projection of solutions
- This is achieved by computing *parametric* polynomial remainder sequences (leading coefficients, see also Sturm sequences)

From Tarski to Collins

- **Tarski's algorithm**: parametric computations of polynomial remainder sequences – Complexity not bounded by a tower of exponents of finite height.
- **Collins'Cylindrical Algebraic Decomposition**: based on the same *geometric* ideas as those used by Tarski.
  - Main improvement: use of *subresultant* sequences (tool similar to polynomial remainder sequences, avoids denominators)
  - Complexity doubly exponential in the (total) number of variables and polynomial in the degree
  - **Software: RedLog, Mathematica, Maple, QEPCAD**
  - Practical limitations: 3 (sometimes 4) variables
- Complexity of QE: doubly exponential in the number of alternates of quantifiers (Heintz/Davenport).

Improvement through the critical point method

- Originally designed to decide if a polynomial system of equations and/or inequalities has real solutions
- (Grigoriev/Vorobjov, Heintz/Roy/Solerno, Renegar, Basu/Pollack/Roy)

Consider a quantified formula: $\mathfrak{Q}\mathbf{X} \in \mathbb{R}^n\ \Psi(\mathbf{Y})$

- Run the critical point method on Ψ over $\mathbb{Q}(\mathbf{Y})$ (the $\mathbf{Y}$s are parameters)
- **Parametric solutions are encoded by**

$$\mathscr{R}(\mathbf{Y}) = \begin{cases} X_n = q_n(T, \mathbf{Y}) \\ \quad\vdots \\ X_1 = q_1(T, \mathbf{Y}) \\ q(T, \mathbf{Y}) = 0 \end{cases}$$

- q_i's lie in $\mathbb{Q}(\mathbf{Y})[T]$
- T is a new variable
- Compute sign conditions in the $\mathbf{Y}$-space ensuring the existence of a real root of q

- **Complexity doubly exponential in the number of alternates of quantifiers**
- A lot of things (which make the algorithms relying on this method unefficient in practice) are hidden in this simplified description.

Application (Stability of MacCormack's scheme)

$$\forall (c_1, s_1, c_2, s_2) \in \mathbb{R}^4,\ c_1^2 + s_1^2 - 1 = c_2^2 + s_2^2 - 1 = 0 \Longrightarrow$$

$$\begin{aligned}
&4\,a^6b^2{c_1}^4{c_2}^2 - 8\,a^5b^3s_1s_2{c_1}^3c_2 - 8\,a^5b^3s_1s_2{c_1}^2{c_2}^2 + 4\,a^4b^4{c_1}^4{c_2}^2 + 16\,a^4b^4{c_1}^3{c_2}^3 + \\
&4\,a^4b^4{c_1}^2{c_2}^4 - 8\,a^3b^5s_1s_2{c_1}^2{c_2}^2 - 8\,a^3b^5s_1s_2c_1{c_2}^3 + 4\,a^2b^6{c_1}^2{c_2}^4 - 4\,a^7bs_1s_2{c_1}^3 + \\
&4\,a^6b^2{c_1}^4c_2 - 4\,a^6b^2{c_1}^3{c_2}^2 + 8\,a^5b^3s_1s_2{c_1}^3 + 12\,a^5b^3s_1s_2{c_1}^2c_2 + 16\,a^5b^3s_1s_2c_1{c_2}^2 - \\
&8\,a^4b^4{c_1}^4c_2 - 24\,a^4b^4{c_1}^3{c_2}^2 - 24\,a^4b^4{c_1}^2{c_2}^3 - 8\,a^4b^4c_1{c_2}^4 + 16\,a^3b^5s_1s_2{c_1}^2c_2 + \\
&12\,a^3b^5s_1s_2c_1{c_2}^2 + 8\,a^3b^5s_1s_2{c_2}^3 - 4\,a^2b^6{c_1}^2{c_2}^3 + 4\,a^2b^6c_1{c_2}^4 - 4\,ab^7s_1s_2{c_2}^3 + \\
&a^8{c_1}^4 + 12\,a^7bs_1s_2{c_1}^2 - 8\,a^6b^2{c_1}^4 - 12\,a^6b^2{c_1}^3c_2 - 12\,a^6b^2{c_1}^2{c_2}^2 - 4\,a^5b^3s_1s_2{c_1}^2 - \\
&8\,a^5b^3s_1s_2{c_2}^2 + 4\,a^4b^4{c_1}^4 + 22\,a^4b^4{c_1}^2{c_2}^2 + 4\,a^4b^4{c_2}^4 - 4\,a^4b^2{c_1}^4{c_2}^2 - 8\,a^3b^5s_1s_2{c_1}^2 - \\
&4\,a^3b^5s_1s_2{c_2}^2 + 8\,a^3b^3s_1s_2{c_1}^2{c_2}^2 - 12\,a^2b^6{c_1}^2{c_2}^2 - 12\,a^2b^6c_1{c_2}^3 - 8\,a^2b^6{c_2}^4 - \\
&4\,a^2b^4{c_1}^2{c_2}^4 + 12\,ab^7s_1s_2{c_2}^2 + b^8{c_2}^4 - 4\,a^8{c_1}^3 - 12\,a^7bs_1s_2c_1 + 16\,a^6b^2{c_1}^3 + 12\,a^6b^2{c_1}^2c_2 + \\
&20\,a^6b^2c_1{c_2}^2 - 16\,a^5b^3s_1s_2c_1 - 4\,a^5b^3s_1s_2c_2 + 4\,a^5bs_1s_2{c_1}^3 + 8\,a^4b^4{c_1}^3 + 12\,a^4b^4{c_1}^2c_2 + \\
&12\,a^4b^4c_1{c_2}^2 + 8\,a^4b^4{c_2}^3 + 4\,a^4b^2{c_1}^4c_2 + 4\,a^4b^2{c_1}^3{c_2}^2 - 4\,a^3b^5s_1s_2c_1 - 16\,a^3b^5s_1s_2c_2 - \\
&12\,a^3b^3s_1s_2{c_1}^2c_2 - 12\,a^3b^3s_1s_2c_1{c_2}^2 + 20\,a^2b^6{c_1}^2c_2 + 12\,a^2b^6c_1{c_2}^2 + 16\,a^2b^6{c_2}^3 + \\
&4\,a^2b^4{c_1}^2{c_2}^3 + 4\,a^2b^4c_1{c_2}^4 - 12\,ab^7s_1s_2c_2 + 4\,ab^5s_1s_2{c_2}^3 - 4\,b^8{c_2}^3 + 6\,a^8{c_1}^2 + 4\,a^7bs_1s_2 - \\
&4\,a^6b^2c_1c_2 - 8\,a^6b^2{c_2}^2 - 2\,a^6{c_1}^4 + 12\,a^5b^3s_1s_2 - 12\,a^5bs_1s_2{c_1}^2 - 14\,a^4b^4{c_1}^2 + 8\,a^4b^4c_1c_2 - \\
&14\,a^4b^4{c_2}^2 - 4\,a^4b^2{c_1}^3c_2 + 10\,a^4b^2{c_1}^2{c_2}^2 + 12\,a^3b^5s_1s_2 + 4\,a^3b^3s_1s_2{c_1}^2 + 16\,a^3b^3s_1s_2c_1c_2 + \\
&4\,a^3b^3s_1s_2{c_2}^2 - 8\,a^2b^6{c_1}^2 - 4\,a^2b^6c_1c_2 + 10\,a^2b^4{c_1}^2{c_2}^2 - 4\,a^2b^4c_1{c_2}^3 + 4\,ab^7s_1s_2 - \\
&12\,ab^5s_1s_2{c_2}^2 + 6\,b^8{c_2}^2 - 2\,b^6{c_2}^4 - 4\,a^8c_1 - 16\,a^6b^2c_1 + 8\,a^6{c_1}^3 + 12\,a^5bs_1s_2c_1 - 12\,a^4b^4c_1 - \\
&12\,a^4b^4c_2 - 8\,a^4b^2{c_1}^2c_2 - 16\,a^4b^2c_1{c_2}^2 - 4\,a^3b^3s_1s_2c_1 - 4\,a^3b^3s_1s_2c_2 - 16\,a^2b^6c_2 - \\
&16\,a^2b^4{c_1}^2c_2 - 8\,a^2b^4c_1{c_2}^2 + 12\,ab^5s_1s_2c_2 - 4\,b^8c_2 + 8\,b^6{c_2}^3 + a^8 + 8\,a^6b^2 - 12\,a^6{c_1}^2 - \\
&4\,a^5bs_1s_2 + 14\,a^4b^4 - 2\,a^4b^2{c_1}^2 + 12\,a^4b^2c_1c_2 + 6\,a^4b^2{c_2}^2 + a^4{c_1}^4 + 8\,a^2b^6 + 6\,a^2b^4{c_1}^2 + \\
&12\,a^2b^4c_1c_2 - 2\,a^2b^4{c_2}^2 + 2\,a^2b^2{c_1}^2{c_2}^2 - 4\,ab^5s_1s_2 + b^8 - 12\,b^6{c_2}^2 + b^4{c_2}^4 + 8\,a^6c_1 + 4\,a^4b^2c_1 - \\
&4\,a^4b^2c_2 - 4\,a^4{c_1}^3 - 4\,a^3bs_1s_2c_1 - 4\,a^2b^4c_1 + 4\,a^2b^4c_2 - 4\,ab^3s_1s_2c_2 + 8\,b^6c_2 - 4\,b^4{c_2}^3 - \\
&2\,a^6 - 2\,a^4b^2 + 8\,a^4{c_1}^2 + 4\,a^3bs_1s_2 - 2\,a^2b^4 - 2\,a^2b^2{c_1}^2 + 4\,a^2b^2c_1c_2 - 2\,a^2b^2{c_2}^2 + 4\,ab^3s_1s_2 - \\
&2\,b^6 + 8\,b^4{c_2}^2 - 8\,a^4c_1 - 4\,a^2b^2c_1 - 4\,a^2b^2c_2 - 8\,b^4c_2 + 3\,a^4 + 6\,a^2b^2 - 2\,a^2{c_1}^2 + 3\,b^4 - 2\,b^2{c_2}^2 + \\
&4\,a^2c_1 + 4\,b^2c_2 - 2\,a^2 - 2\,b^2 \le 0
\end{aligned}$$

Degree 14, 163 terms... Indeed, we are going to suffer...

Some preliminary remarks

- Let's try to solve it with the existing softwares:
  - Mathematica just crashed after 20 minutes
  - RedLog crashed after 2 days
  - QEPCAD crashed after 2 weeks
  - OpenCAD did not give an answer after 1 month.
- Algorithms based on the critical point method are not usable.
- The real solution set of $c_1^2 + s_1^2 - 1 = c_2^2 + s_2^2 - 1 = 0$ is compact in $\mathbb{R}^4$
- **Specification**: we don't need a full description of the feasibility set.
  This problem is a stability analysis problem: we only need a description of the interior of the feasibility set.
  The feasibility set is the stability region of a numerical scheme of resolution of a pde.

Solution set of polynomial systems of equations

Let $V \subset \mathbb{C}^n$ be the solution set of $g_1 = \cdots = g_k = 0$.

Example: $X_1(X_1 - 1) = X_1X_2 = 0$ or $X_1^2 + X_2^2 = 0$ or $X_1^2 = 0$

Its dimension $\dim(V)$ is an integer d s.t. for a generic choice of hyperplanes $H_1, \ldots, H_d$, $V \cap (H_1 \cap \cdots \cap H_d)$ is a finite set of points.

Let $I(V)$ be the set of polynomials s.t. $g \in I \Leftrightarrow \forall \mathbf{x} \in V \; g(\mathbf{x}) = 0$.

V can be decomposed as the union of irreducible components $W_1 \cup \cdots \cup W_r$ ("$I(W_i)$ can not be factored")

V is equidimensional iff all its irreducible components have the same dimension.

- The solution set of $c_1^2 + s_1^2 - 1 = c_2^2 + s_2^2 - 1 = 0$ is equidimensional
- This property is *natural* and arises frequently.

Solution set of polynomial systems of equations

Let $T_{\mathbf{x}}V$ the vector space defined by the equations $\mathbf{grad}_{\mathbf{x}}(g).\mathbf{v} = 0$ (for $\mathbf{g} \in I$).

When V is equidimensional, $\mathbf{x}$ is a regular point if $\dim(T_{\mathbf{x}}V) = \dim(V)$ else it is a singular point.

In many situations, V contains only regular points and $(\mathrm{grad}_{\mathbf{x}}(g_1), \ldots, \mathrm{grad}_{\mathbf{x}}(g_k))$ spans the co-tangent space of V at $\mathbf{x}$.

- $T_{\mathbf{x}}V$ is a local first-order approximation of V at $\mathbf{x}$.
- The solution set of $c_1^2 + s_1^2 - 1 = c_2^2 + s_2^2 - 1 = 0$ contains only regular points
- The set of gradient vectors spans the co-tangent space.
- These properties (smoothness) is *natural* and arises frequently.

Problem statement

Consider a polynomial system $\mathcal{G} = \{g_1, \ldots, g_k\} \subset \mathbb{Q}[\mathbf{X}]$ and suppose that

$\mathbf{H_1'}$: $\langle \mathcal{G} \rangle$ is radical and the complex variety defined by $\mathcal{G}$ is equidimensional, and of co-dimension k

$\mathbf{H_1''}$: the complex variety defined by $\mathcal{G}$ is smooth

$\mathbf{H_2}$: the real variety defined by $\mathcal{G}$ in the $\mathbf{X}$-space is compact.

Two formulas Ψ and Φ are *almost equivalent* iff the interior of the solution set of Ψ is the same as the interior of the solution set of Φ.

Problem: Variant Quantifier Elimination (VQE)

Input: Ψ, a quantified formula of the form

$$\forall \mathbf{X} \qquad \mathcal{G}(\mathbf{X}) = 0 \quad \Longrightarrow \quad f(\mathbf{X}, \mathbf{Y}) \leq 0$$

where $\mathbf{X}$ and $\mathbf{Y}$ are lists of variables, $f \in \mathbb{Q}[\mathbf{X}, \mathbf{Y}]$, and $\mathcal{G} \subset \mathbb{Q}[\mathbf{X}]$ satisfies $\mathbf{H_1}$ and $\mathbf{H_2}$.

Output: Φ, a quantifier-free formula almost equivalent to Ψ.

Polynomial mappings and Critical points

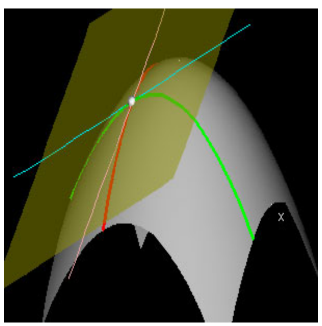
Let $V \subset \mathbb{C}^n$ be the solution set of $g_1 = \cdots = g_k = 0$ satisfying $\mathbf{H_1'}$.

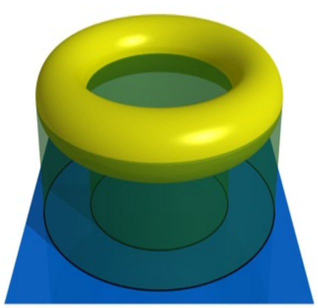
We consider $\varphi : \mathbf{x} \in V \to (\varphi_1(\mathbf{x}), \ldots, \varphi_s(\mathbf{x})) \in \mathbb{C}^s$

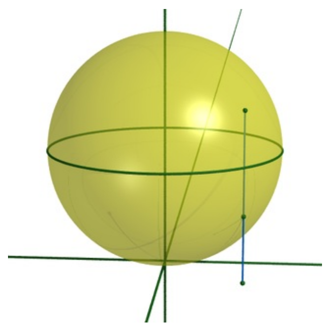
$$d_{\mathbf{x}}\varphi : \mathbf{v} \in T_{\mathbf{x}}V \to \mathrm{grad}_{\mathbf{x}}(\varphi_1).\mathbf{v}, \ldots, \mathrm{grad}_{\mathbf{x}}(\varphi_s).\mathbf{v}$$

$$\mathrm{crit}(\varphi, V) = \{\mathbf{x} \in \mathrm{reg}(V) \mid \mathrm{rank}(d_{\mathbf{x}}\varphi) \leq s-1\} \cup \mathrm{sing}(V)$$

$\mathrm{crit}(\varphi, V)$ is defined by the vanishing of all $(k+s, k+s)$-minors of $\mathrm{jac}([g_1, \ldots, g_k, \varphi_1, \ldots, \varphi_s])$







Example: $X_1^2 + X_2^2 + X_3^2 - 1 = 0$,
$\varphi : (\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3) \to (\mathbf{x}_1, \mathbf{x}_2)$,
$\mathrm{crit}(\varphi, V) = \{\mathbf{x} \mid \mathbf{x}_3 = 0, \mathbf{x}_1^2 + \mathbf{x}_2^2 - 1 = 0\}$

Under $\mathbf{H_1'}$, $\mathrm{sing}(V)$ is defined by the vanishing of all (k, k)-minors of $\mathrm{jac}([g_1, \ldots, g_k])$.

Properties

Critical values are the values taken by φ at critical points. They are enclosed in an algebraic variety (Sard's theorem).

The smallest variety of $\mathbb{C}^s$ containing the set of critical values is denoted by $\mathscr{D}(\varphi, V)$.

Suppose that V is smooth and let $\mathbf{y} \in \mathbb{C}^s \setminus \mathscr{D}(\varphi, V)$. The variety $V \cap \varphi^{-1}(\mathbf{y})$ is smooth.

Notion of properness of φ at $\mathbf{y}$: Given $\mathbf{y} \in \mathbb{C}^s$, there exists $B(\mathbf{y}, r)$ s.t. $\varphi^{-1}(B(\mathbf{y}, r)) \cap V \cap \mathbb{R}^n$ is compact.

Let C be a connected component of $V \cap \mathbb{R}^n$. If, for all $\mathbf{y} \in \mathbb{C}^s$, φ is proper at $\mathbf{y}$, the frontier of $\varphi(C)$ is contained in $\mathscr{D}(\varphi, V)$

Some ideas

Back to our QE problem: $\forall \mathbf{X} \in \mathbb{R}^n, \mathcal{G}(\mathbf{X}) = 0 \Rightarrow f(\mathbf{X}, \mathbf{Y}) \leq 0$

$\mathbf{X} = [X_1, \ldots, X_n]$ and $\mathbf{Y} = [Y_1, \ldots, Y_p]$

Sard's theorem implies that $\mathcal{G} = f - \mathbf{e} = 0$ defines a smooth variety for all $\mathbf{e} \in \mathbb{R} \setminus \mathscr{E}$ where $\sharp\mathscr{E} < \infty$

Consider the mapping $(\mathbf{x}, \mathbf{y}) \to f(\mathbf{x}, \mathbf{y})$

$V_{\mathbf{e}}$ denotes the complex solution set of $\mathcal{G} = f - \mathbf{e} = 0$

This implies that one $(k+1, k+1)$-minor of $\mathrm{jac}(\mathcal{G}, f)$ does not vanish at points of $\mathcal{V}_{\mathbf{e}}$ for a generic $\mathbf{e}$.

The compacity of the real variety defined by $\mathcal{G} = 0$ in the $\mathbf{X}$-space implies the properness of the projection $\Pi : (\mathbf{x}, \mathbf{y}) \to \mathbf{y}$ restricted to $V_{\mathbf{e}} \cap \mathbb{R}^{n+p}$.

This allows us to prove that the frontier of the feasibility set is contained in $\lim_{e \to 0} \Pi(\mathrm{crit}(\Pi, V_{\mathbf{e}}))$

Some ideas

The idea: Compute $\lim_{e\to 0} \Pi(\mathrm{crit}(\Pi, V_{\mathbf{e}}))$
to obtain the boundary of the feasibility set

- All $(k+1, k+1)$-minors of $\mathrm{jac}_{\mathbf{X}}(\mathcal{G}, f)$ vanish at points of $\mathrm{crit}(\Pi, V_{\mathbf{e}}) \rightarrow$ Δ_1 denotes this set of minors.
- For a generic $\mathbf{e}$, at least one $(k+1, k+1)$-minor of $\mathrm{jac}(\mathcal{G}, f)$ does not vanish (because $V_{\mathbf{e}}$ is smooth) $\rightarrow$ Δ_1 denotes the set of all these minors.
- Compute $W = \overline{V(\mathcal{G}, \Delta) \setminus V(\mathcal{G}, \Delta)}$
- Compute $\Pi(W \cap V(f))$.

A simple example

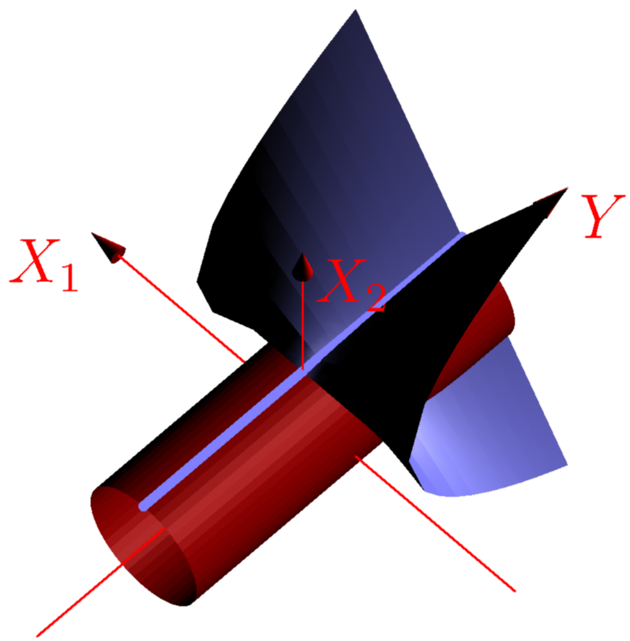
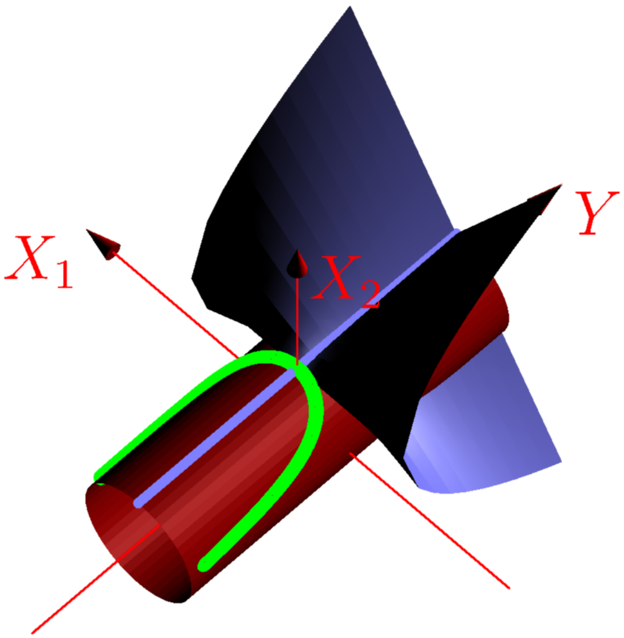


Figure 1: Example: Consider $\mathcal{G} = \{X_1^2 + X_2^2 - 1\}$ (cylinder in red) and $f = X_1^2 Y - (X_2 - 1)^2$ (the blue surface, this is the Whitney umbrella) Here the Y-axis is the cylinder axis.



1. We compute the jacobian of $\mathcal{G} \cup \{f\}$ w.r.t. $\mathbf{X}$,
2. We compute the set of all the minors of J_1 of size $1+1$, obtaining

$$\Delta_1 = \{-4\, X_1\, (X_2 - 1 + X_2 Y)\}$$

3. We compute the jacobian J of $\mathcal{G} \cup \{f\}$ w.r.t. $\mathbf{X} \cup \mathbf{Y}$,
4. We compute the set of all minors of J of size $1+1$, obtaining

$$\Delta = \left\{-4\, X_1\, (X_2 - 1 + X_2 Y)\,, \quad 2\, {X_1}^3, \quad 2\, X_2 {X_1}^2\right\}$$

5. We compute a set of generators of $\overline{V(\mathcal{G} \cup \Delta_1) \setminus V(\mathcal{G} \cup \Delta)}$, obtaining

$$G = \left\{{X_1}^2 + {X_2}^2 - 1, \quad X_2 - 1 + X_2 Y\right\}$$

6. We compute a set of generators of $\langle G \cup \{f\}\rangle \cap \mathbb{Q}[\mathbf{Y}]$, obtaining

$$E = \left\{Y^2\right\}$$

The algorithm

1. $J_1 \leftarrow$ the jacobian of $\mathcal{G} \cup \{f\}$ with respect to $\mathbf{X}$
2. $\Delta_1 \leftarrow$ the set of all minors of J_1 of size $k+1$
3. $J \leftarrow$ the jacobian of $\mathcal{G} \cup \{f\}$ with respect to $\mathbf{X} \cup \mathbf{Y}$
4. $\Delta \leftarrow$ the set of all minors of J of size $k+1$
5. $G \leftarrow$ a set of generators of $V(\mathcal{G} \cup \Delta_1) \setminus V(\mathcal{G} \cup \Delta)$
6. $E \leftarrow$ a set of generators of $\langle G \cup \{f\} \rangle \cap \mathbb{Q}[\mathbf{Y}]$

   Here, we get the boundary of the feasibility set
7. $P \leftarrow$ a set of squarefree parts of E
8. $\mathscr{C} \leftarrow \mathsf{SemiAlgebraicDescription}(P)$

   We want to describe the connected components of $P \neq 0$ and provide sampling points. This task can be achieved by CAD or roadmap computations
9. $\Phi \leftarrow \bigvee\{C \mid (C, S) \in \mathscr{C}$ and $\Psi(S)$ is true$\}$ Here, one has to decide the emptiness of polynomial systems of equations and inequalities for each computed sample point in the parameter-space.

Computations

Many algorithms can be used to implement the VQE algorithm (Gröbner bases, Triangular sets, Kronecker).

The computations have been performed on a PC Intel(R) Xeon(R) 2.50GHz with 6144 KB of Cache and 20 GB of RAM.

Computation of $\overline{V(\mathcal{G} \cup \Delta_1) \setminus V(\mathcal{G} \cup \Delta)}$

- FGB (Faugère, written in C): 80 sec., Regularity 34, dimension 2, degree 434
- REGULARCHAINS (Moreno Maza, written in Maple): > 1 day
- KRONECKER (Lecerf, written in Magma) – computing generic fibers: 7 hours

Second step (intersection with $f = 0$ and projection on the $\mathbf{Y}$-space):
1.5 **hours with** FGb – regularity 140 produces a single polynomial whose factorization gives 9 polynomials

$a+1, a, b, a-1, a^4 - a^2 + 1/2$. The remaining four are non-trivial:

$$\begin{aligned}
h_1 &= a^4 - a^2 + 1/2 - 2a^2b^2 - b^2 + b^4 \\
h_2 &= a^4 - a^2 - 2a^2b^2 - b^2 + b^4 \\
h_3 &= a^6 - 1 + 3b^2a^4 + 3a^2b^4 + b^6 - 3a^4 \\
&\quad +21a^2b^2 - 3b^4 + 3a^2 + 3b^2 \\
h_4 &= 4627325525704704\, b^{80}a^{18} \\
&\quad + \cdots + \mathbf{1199\ terms} + \cdots + \\
&\quad 850320000000000\, a^2.
\end{aligned}$$

Last steps with RAGlib **(16 hours):**

- computing sampling points outside the computed curve produces **7652 points**.
- For all of them one has to decide the emptiness of a semi-algebraic set lying in $\mathbb{R}^4$

Computations

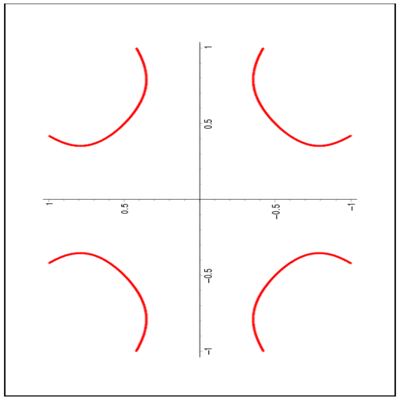


Figure 2: h_1

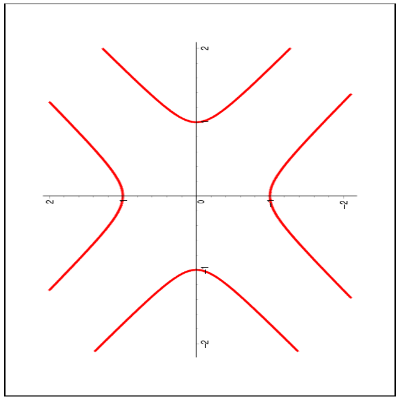


Figure 3: h_2

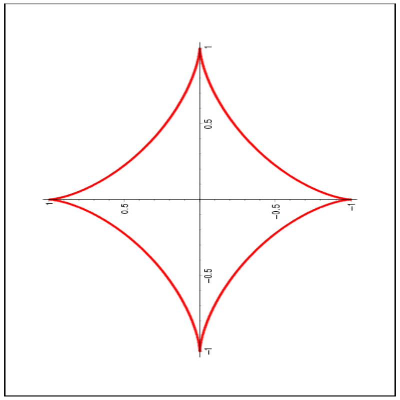


Figure 4: $h_3 < 0$ is the output

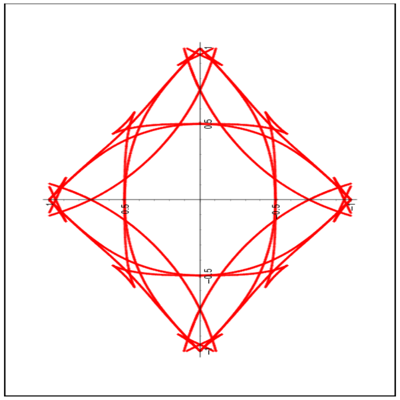


Figure 5: h_4

Degree bounds

Let D be an integer dominating the total degree of polynomials in $\mathcal{G}$ and f.

- **The degree of each variety algebraically represented in the algorithm VQE is dominated by** $\delta = D^k((k+1)D)^{n-k}$
- One can give more precise estimates using S./Trébuchet's results about the degrees of critical loci (using bi-homogeneous Bézout theorems and Lagrange's systems to define the critical points)
- **Complexity results of Lecerf** (inheriting from the works of Giusti/Heintz/Pardo) yield complexity results for a probabilistic version of VQE that are polynomial in δ^p.
- Same complexity class than algorithms based on the critical point method

And now?...

- On-going work : **Generalization to quantified formula of the form**

$$\forall \mathbf{X} \in \mathbb{R}^n \; \mathcal{G}(\mathbf{X},\mathbf{Y}) = 0 \Rightarrow f_1(\mathbf{X},\mathbf{Y}) \leq 0 \wedge \cdots \wedge f_s(\mathbf{X},\mathbf{Y}) \leq 0$$

- **Removing the compactness assumption**: generalized critical values
  - Introduced by Jelonek, Kurdyka, Orro, Simon
  - Algorithms for computing them (S. 04/06/07) implemented in RAGLIB
- **Specification of quantifier elimination**: avoid to write the equivalent formula (or the almost equivalent formula)
  - sampling points in the feasibility set and programs deciding in which connected component of the feasibility set a given point lies.
  - Need of roadmap algorithms (to answer connectivity queries)
  - S./Schost 2009 (first improvement of Canny's approach)
- Need of fast algorithms and implementations for computing sampling points in semi-algebraic sets (see RAGLIB)