# On sign conditions over real multivariate polynomials

Gabriela Jeronimo

Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Joint work with Daniel Perrucci and Juan Sabia

Given $f_1, \dots, f_m \in \mathbb{Q}[x_1, \dots, x_n]$, decide whether the set

$$\mathcal{P} = \{x \in \mathbb{R}^n \mid f_1(x) = 0, \dots, f_p(x) = 0, f_{p+1}(x) > 0, \dots, f_m(x) > 0\}$$

is empty or not.

If $\mathcal{P}$ is not the empty set, exhibit a point in $\mathcal{P}$.

A (closed) sign condition over $f_1, \dots, f_m \in \mathbb{Q}[x_1, \dots, x_n]$ is $\sigma \in \{<, =, >\}^m$ (resp. $\sigma \in \{\leq, =, \geq\}^m$).

We say $\sigma = (\sigma_1, \dots, \sigma_m)$ is feasible if the set

$$\mathcal{P}_\sigma = \{x \in \mathbb{R}^n \mid f_1(x)\sigma_1 0, \dots, f_m(x)\sigma_m 0\}$$

is not empty. We call this set the realization of $\sigma$.

**Two questions.** Given $f_1, \dots, f_m \in \mathbb{Q}[x_1, \dots, x_n]$:

- Determine all feasible (closed) sign conditions over $f_1, \dots, f_m$.
- Exhibit a point in $\mathcal{P}_\sigma$ for each feasible sign condition $\sigma$.

# Related Work

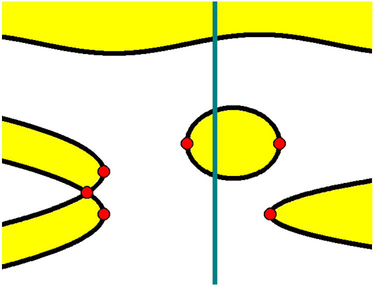
- Quantifier elimination.

  Tarski (1951), Collins (1975), Grigoriev-Vorobjov (1988, 1992), Heintz-Roy-Solernó (1990), Renegar (1992), Canny (1993), Basu-Pollack-Roy (1996).

- Polynomial equation systems.
  - Bank-Giusti-Heintz-Mbakop (1997, 2001).
  - Safey El Din-Schost (2003), Bank-Giusti-Heintz-Pardo (2005).

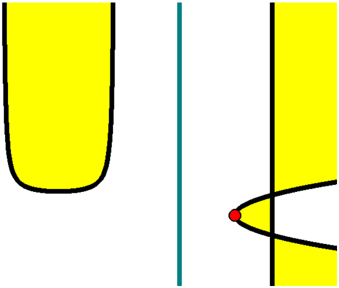
- Feasible sign conditions over a single polynomial.
  Safey El Din (2007).

Search for a point in the closure of each connected component of the set.



**Sketch of the Algorithm**

- Find points where the maximum or minimum of the projection over $x_1$ is attained.
- Intersect with $x_1 = c$ and proceed in the same way, recursively, with $x_2, \ldots, x_n$.



The following conditions could be met by a connected component $C$:

- there are no extremal points for $x_1$ over $C$ and,
- $\{x_1 = c\} \cap C = \emptyset$.

Also, there might be infinitely many extremal points over $C$.

How to avoid these situations: consider a generic linear form instead of $x_1$.

For a nonempty set $C \subset \mathbb{R}^n$ and a linear $\pi : \mathbb{R}^n \to \mathbb{R}$, let:

- $Z_i(C) = \overline{C} \cap \pi^{-1}(\inf \pi(C))$ if $\pi(C)$ is bounded from below, and $Z_i(C) = \emptyset$ otherwise.
- $Z_s(C) = \overline{C} \cap \pi^{-1}(\sup \pi(C))$ if $\pi(C)$ is bounded from above, and $Z_s(C) = \emptyset$ otherwise.
- $Z(C) = Z_i(C) \cup Z_s(C)$.

**Proposition.** Let $D \subset \mathbb{R}^n$ be a semialgebraic set. After a generic linear change of variables, for $p \in \mathbb{R}^n$, $C$ a connected component of $D \cap \{x_1 = p_1, \dots, x_{k-1} = p_{k-1}\}$, and $\pi(x_1, \dots, x_n) = x_k$:

- $Z(C)$ is a finite set (possibly empty).
- If $\pi(C)$ is bounded from below (resp. from above), $Z_i(C) \neq \emptyset$ (resp. $Z_s(C) \neq \emptyset$).

# A Finite Set of Sample Points

Let $D \subset \mathbb{R}^n$ be a semialgebraic set. After a generic linear change of variables:

**Proposition.** Let $p \in \mathbb{R}^n$ and, for $1 \leq k \leq n$, let $\mathcal{C}(k,p)$ be the set of connected components of $D \cap \{x_1 = p_1, \ldots, x_{k-1} = p_{k-1}\}$. Then

$$\{p\} \cup \Big( \bigcup_{k=1}^{n} \bigcup_{C \in \mathcal{C}(k,p)} Z^{(k)}(C) \Big)$$

is a finite set intersecting the closure of each connected component of $D$.

- Our problem amounts to the computation of extremal points of the projection on the first coordinate.

Given $f_1, \ldots, f_s \in \mathbb{R}[x_1, \ldots, x_n]$, the IFT implies that the maxima and minima of $x_1$ over $\mathcal{V} = \{f_1(x) = 0, \ldots, f_s(x) = 0\}$ occur at points $z \in \mathcal{V}$ for which there exists $\mu \in \mathbb{R}^s \setminus \{0\}$ such that:

$$\sum_{j=1}^{s} \mu_j \underbrace{\left(\frac{\partial f_j}{\partial x_2}(z), \ldots, \frac{\partial f_j}{\partial x_n}(z)\right)}_{\overline{\nabla} f_j(z)} = (0, \ldots, 0) \in \mathbb{R}^{n-1}.$$

**Generalization.** Let $f_1, \dots, f_m \in \mathbb{R}[x_1, \dots, x_m]$.
For $\sigma \in \{\leq, <, =, >, \geq\}^m$, if $C$ is a connected component of

$$\mathcal{P}_\sigma = \{x \in \mathbb{R}^n \mid f_1(x)\sigma_1 0, \dots, f_m(x)\sigma_m 0\},$$

then

$$Z(C) \subset \bigcup_{\{i | \sigma_i \text{ is } =\} \subset S \subset \{1,\dots,m\}} \Pi(W_S)$$

- $W_S = \left\{(x, \mu) \in \mathbb{C}^n \times \mathbb{P}^{s-1} \mid \left\{ \begin{array}{l} f_{i_1}(x) = 0, \dots, f_{i_s}(x) = 0, \\ \sum_{j=1}^s \mu_j \overline{\nabla} f_{i_j}(x) = 0 \end{array} \right. \right\}$ if $S = \{i_1, \dots, i_s\}$.
- $\Pi : \mathbb{C}^n \times \mathbb{P}^{s-1} \to \mathbb{C}^n$ is the projection onto the first factor.

# Our Work

- Aim. Find points in the closure of each connected component of $\mathcal{P}_\sigma$ for every sign condition $\sigma$ over $f_1, \ldots, f_m$.
- Strategy. Compute points in the sets $\Pi(W_S)$, by (partially) solving the polynomial systems defining them.
- Difficulty. Even though the sets $Z(C)$ are finite, the sets $\Pi(W_S)$ might be infinite sets.

We are able to overcome this difficulty in several different situations.

**Assumption**

For every $x \in \mathbb{C}^n$ such that $f_{i_1}(x) = 0, \cdots = f_{i_s}(x) = 0$, the set $\{\nabla f_{i_1}(x), \ldots, \nabla f_{i_s}(x)\}$ is linearly independent.

Under this assumption, for $S \subset \{1, \ldots, m\}$:

- $\mathcal{V}_S = \{x \in \mathbb{C}^n \mid f_j(x) = 0 \ \forall j \in S\} = \emptyset$ if $\#S > n$.
- After a generic linear change of variables,

  $$W_S = \left\{(x, \mu) \in \mathbb{C}^n \times \mathbb{P}^{s-1} \mid \left\{ \begin{array}{l} f_{i_1}(x) = 0, \ldots, f_{i_s}(x) = 0, \\ \sum_{j=1}^{s} \mu_j \overline{\nabla} f_{i_j}(x) = 0 \end{array} \right. \right\}$$

  is a finite set if $\#S \leq n$.

If $p = (p_1, \dots, p_n) \in \mathbb{R}^n$ is generic, for every $1 \le k \le n$, the previous assumption also holds for

$$f^{(k)} := \{f_j(p_1, \dots, p_{k-1}, x_k, \dots, x_n),\ 1 \le j \le m\}$$

Then,

$$\mathcal{M} = \bigcup_{k=1}^{n} \bigcup_{\substack{S \subset \{1, \dots, m\} \\ 1 \le \#S \le n-k+1}} \Pi(W_S^{(k)})$$

is a finite set intersecting the closure of each connected component of every $\mathcal{P}_\sigma$, where $W_S^{(k)} \subset \mathbb{C}^{n-k} \times \mathbb{P}^{\#S-1}$ is defined from $f^{(k)}$.

# Basic Step of the Algorithm

The computation of $\mathcal{M}$ amounts to solving in $\mathbb{C}^n \times \mathbb{P}^{s-1}$
0-dimensional polynomial equation systems of the type:

$$f_1(x) = 0, \dots, f_s(x) = 0$$
$$\sum_{j=1}^{s} \mu_j \frac{\partial f_j}{\partial x_2}(x) = 0, \dots, \sum_{j=1}^{s} \mu_j \frac{\partial f_j}{\partial x_n}(x) = 0$$

These systems have the following structure:

- $s$ equations involving only the variables $x$ with $\deg_x \leq d$,
- $n-1$ equations with $\deg_x \leq d-1$, homogeneous and linear in the variables $\mu$,

which we exploit to solve them within good complexity bounds.

Given $F = [f_1(x), \dots, f_s(x), f_{s+1}(x, \mu), \dots, f_r(x, \mu)]$:

- Choose an initial system $G = [g_1(x), \dots, g_s(x), g_{s+1}(x, \mu), \dots, g_r(x, \mu)]$ with the same structure and maximum number of known or "easy to compute" solutions.
- Consider the homotopy $H(t) = tF + (1 - t)G$ so that $H(0) = G$ and $H(1) = F$.
- Compute a description of the solutions to $H = 0$ over $\overline{\mathbb{Q}(t)}$ from the solutions to $G = 0$, by Newton-Hensel lifting.
- Substitute $t = 1$ in order to obtain the isolated roots of $F = 0$.

# Main Complexity Result

**Theorem A (J.-Perrucci-Sabia)**

Under the previous regularity assumption on the input polynomials $f_1, \dots, f_m \in \mathbb{Q}[x_1, \dots, x_n]$, there is a probabilistic algorithm which computes a finite set of points $\mathcal{M}$ such that $\mathcal{M} \cap \overline{C} \neq \emptyset$ for every connected component $C$ of $\mathcal{P}_\sigma$ for every feasible $\sigma \in \{<, =, >\}^m$.

The algorithm performs $O\big(\sum_{s=1}^{\min\{m,n\}} \binom{m}{s} \big(\binom{n-1}{s-1} d^n\big)^2 (L + d)\big)$ arithmetic operations in $\mathbb{Q}$ (up to logarithmic factors), where

- $d = \max\{\deg(f_i)\}$ and
- $L$ is the input size.

# Parametric Representation of Finite Sets

A set $\mathcal{M} = \{\xi_1, \dots, \xi_D\} \subset \mathbb{C}^n$, where $\xi_j = (\xi_{j1}, \dots, \xi_{jn})$, definable by polynomial equations over $\mathbb{Q}$ can be characterized by:

- $\ell = \ell_1 x_1 + \dots + \ell_n x_n \in \mathbb{Q}[x]$ a separating linear form for $\mathcal{M}$, i.e. $\ell(\xi_i) \neq \ell(\xi_j)$ for $i \neq j$,
- $m_\ell = \prod_{1 \le j \le D} (U - \ell(\xi_j)) \in \mathbb{Q}[U]$,
- $v_1, \dots, v_n \in \mathbb{Q}[U]$ with $\deg(v_i) < D$ and $v_i(\ell(\xi_j)) = \xi_{ji}$ $\forall j$.

These data provide the following parametric description of the set:

$$\mathcal{M} = \{(v_1(u), \dots, v_n(u)) \mid u \in \mathbb{C},\ m_\ell(u) = 0\}.$$

which we call a geometric solution of $\mathcal{M}$.

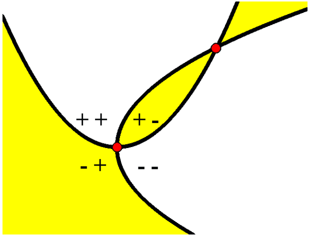
Example. $\mathcal{M} = \{(-1,3),(1,3),(2,0)\}$

- $\ell = x_1$ is a separating linear form,
- $m_\ell = (U+1)(U-1)(U-2) = U^3 - 2U^2 - U + 2$,
- $v_1 = U$,
  $v_2 \in \mathbb{Q}[U]$ such that:
  $$v_2(-1) = 3, \; v_2(1) = 3, \; v_2(2) = 0, \text{ and } \deg v_2 < 3$$
  $\Rightarrow v_2 = -U^2 + 4$,

$$\mathcal{M} = \{(u, -u^2+4) \mid u^3 - 2u^2 - u + 2 = 0\}$$

# Feasible Sign Conditions

From the finite set $\mathcal{M}$ the algorithm computes, we can list all the feasible sign conditions over $f_1, \ldots, f_m$:




- Determine the signs of $f_1, \ldots, f_m$ at each point in $\mathcal{M}$ (Canny, 1993).
- If $f_j(\xi) = 0$ for $\xi \in \mathcal{M}$, in a neighborhood of $\xi$, $f_j$ takes both positive and negative values.

**Proposition**

If $\mathcal{L}$ is the set of the sign conditions of $f_1, \ldots, f_m$ at the points in $\mathcal{M}$, all feasible sign conditions over $f_1, \ldots, f_m$ are $\bigcup_{\sigma \in \mathcal{L}} L_\sigma$, where $L_\sigma = \{\sigma' \in \{<, =, >\}^m \mid \sigma'_i = \sigma_i \text{ if } \sigma_i \text{ is } < \text{o} >\}$.

# II - Bivariate polynomials

Let $f_1, \ldots, f_m \in \mathbb{R}[x_1, x_2]$. Even if they do not satisfy the regularity assumption and the considered sets of critical points are not finite, due to

- a better understanding of the sets $Z(C)$ for the connected components $C$ of $\mathcal{P}_\sigma$, and
- polynomial equations defining the auxiliary varieties $\mathcal{W}_S$,

proceeding as in the previous case, we can locate a finite subset $\mathcal{M}$ of critical points such that $\mathcal{M} \cap \overline{C} \neq \emptyset$ for each connected component of $\mathcal{P}_\sigma$ for all feasible $\sigma$.

If $C$ is a connected component of $\mathcal{P}_\sigma$ for $\sigma \in \{<, =, >\}^m$, and $\xi \in Z(C)$, one of the following conditions holds:

1. $\exists\ f_{i_0}\ /\ q_1(\xi) = q_2(\xi) = 0$ for non-associate irred. factors $q_1$ and $q_2$ of $f_{i_0}$ or $q(\xi) = \frac{\partial q}{\partial x_2}(\xi) = 0$ for an irred. factor $q$ of $f_{i_0}$.

   $\Rightarrow \xi \in \pi_x(\mathcal{W}_{\{i_0\}} \cap \{t = 0\})$, $\mathcal{W}_{\{i_0\}}$ = union of irred. comp. of $\{(1-t)f_{i_0} + tg_1 = 0, (1-t)\frac{\partial f_{i_0}}{\partial x_2} + tg_2 = 0\}$ not in $\{t = 0\}$

2. $\exists\ f_{i_1}, f_{i_2}\ /\ q_1(z) = q_2(z) = 0$ for a single irred. factor $q_1$ of $f_{i_1}$ and a single irred. factor $q_2$ of $f_{i_2}$, $q_1$ and $q_2$ non-associate.

   $\Rightarrow \xi \in \pi_x(\mathcal{W}_{\{i_1,i_2\}} \cap \{t = 0\})$, $\mathcal{W}_{\{i_1,i_2\}}$ = union of irred. comp. of $\{(1-t)f_{i_1} + tg_1 = 0, (1-t)f_{i_2} + tg_2 = 0\}$ not in $\{t = 0\}$.

$$\mathcal{M} = \bigcup_{S \subset \{1,\dots,m\}, 1 \le \#S \le 2} \pi_x(\mathcal{W}_S \cap \{t = 0\})$$

Given $f \in \mathbb{R}[x_1, \ldots, x_n]$, after a generic linear change of variables, the finitely many extremal points of $x_1$ over the connected components of $\{f < 0\}$, $\{f = 0\}$ and $\{f > 0\}$ lie in

$$W = \left\{ f(x) = 0, \frac{\partial f}{\partial x_2}(x) = 0, \ldots, \frac{\partial f}{\partial x_n}(x) = 0 \right\}$$

However, $W$ may be an infinite set.

Example. If $f = (x_1 - x_3^2)^3 - x_2^2 \in \mathbb{R}[x_1, x_2, x_3]$, then:

- $\dfrac{\partial f}{\partial x_2} = -2x_2$ and $\dfrac{\partial f}{\partial x_3} = -6x_3(x_1 - x_3^2)^2$,
- $W = \{x_2 = 0, x_1 - x_3^2 = 0\}$.

Given $f \in \mathbb{Q}[x_1, \ldots, x_n]$, consider the Thebychev polynomial $\mathcal{T}_d$ of degree $d = 2\lceil \deg f/2 \rceil$ and define $h = (1-t)f + tg$, where $g = n + 1 + \sum_{k=1}^{n} \mathcal{T}_d(x_k)$ (positive over $\mathbb{R}^n$).

- $W(g) = \{x \in \mathbb{C}^n \mid g(x) = \frac{\partial g}{\partial x_2}(x) = \cdots = \frac{\partial g}{\partial x_n} = 0\}$ is a finite set, and the same holds for $W(h \mid_{\{t=t_0\}})$ for all but a finite number of $t_0$.

**Proposition.** If $\mathcal{W}$ is the union of the irreducible components of $\{(t,x) \mid h(t,x) = \frac{\partial h}{\partial x_2}(t,x) = \cdots = \frac{\partial h}{\partial x_n}(t,x) = 0\}$ not contained in $t = c$, for every connected component $C$ of $\{f = 0\}$, $\{f < 0\}$ or $\{f > 0\}$, we have $Z(C) \subset \pi_x(\mathcal{W} \cap \{t = 0\})$.

**Idea.** If $\xi \in Z(C)$, for $t_0$ sufficiently small, there are points in $W(h(t_0, x)) = \pi_x(\mathcal{W} \cap \{t = t_0\})$ arbitrarily close to $\xi$.

**Theorem B (J.-Perrucci-Sabia)**

There is a probabilistic algorithm that, given an arbitrary polynomial $f \in \mathbb{Q}[x_1, \dots, x_n]$, computes a finite set $\mathcal{M}$ such that $\mathcal{M} \cap \overline{C} \neq \emptyset$ for every connected component $C$ of $\{f > 0\}$, $\{f = 0\}$ or $\{f < 0\}$.

The algorithm performs $O\big(d^{2n}L\big)$ arithmetic operations in $\mathbb{Q}$ (up to logarithmic factors), where $d := 2\lceil \frac{\deg f}{2} \rceil$ and $L$ is the size of the encoding of $f$.

Let $\mathcal{P} = \{x \in \mathbb{R}^n \mid f_1(x) = 0, \dots, f_m(x) = 0\}$ be defined by arbitrary polynomials $f_1, \dots, f_m \in \mathbb{Q}[x_1, \dots, x_n]$.

- For $i = 1, \dots, m$, define $g_i^+$ and $g_i^-$ in $\mathbb{Q}[x_1, \dots, x_n]$, such that $\forall\, x \in \mathbb{R}^n$, $g_i^+(x) > 0$ and $g_i^-(x) < 0$.

**Deformation.**

- For $i = 1, \dots, m$, let
$$h_i^+ = (1-t)f_i + tg_i^+ \quad \text{and} \quad h_i^- = (1-t)f_i + tg_i^-.$$
- $\mathcal{P}_t = \{x \in \mathbb{R}^n \mid \forall\, 1 \le i \le m,\ h_i^+(t,x) \ge 0 \text{ and } h_i^-(t,x) \le 0\}$.

The polynomials $h_i^+$ and $h_i^-$ are in general position and

$$\mathcal{P} \subset \mathcal{P}_t \quad \forall\, 0 \le t \le 1 \quad \text{and} \quad \mathcal{P}_0 = \mathcal{P}.$$

# Extremal Points of Projections

**General approach.** Find extremal points in a connected component of $\mathcal{P} = \mathcal{P}_0$ as "limits" of points in $\mathcal{P}_t$ for small $t$.

- If $C$ is a connected component of $\mathcal{P}$ and $\xi \in Z(C)$, $\forall\, \varepsilon > 0$, if $t$ is sufficiently small, there is a critical point of $x_1$, $\xi_t \in \mathcal{P}_t$, such that $d(\xi_t, \xi) < \varepsilon$.
- For a generic $t_0$,

$$\xi_{t_0} \in \bigcup_{\substack{S \subset \{1,\dots,m\} \times \{+,-\} \\ 1 \leq \#S \leq n}} \pi_x(\mathcal{W}_S \cap \{t = t_0\}),$$

$\mathcal{W}_S$ is the union of the irreducible components of

$\{(t, x, \mu) \mid h_i^\tau(t, x) = 0 \ \forall (i, \tau) \in S,\ \sum_{(i,\tau)} \mu_i^\tau \overline{\nabla} h_i^\tau(t, x) = 0\}$

not contained in a hyperplane $t = c$.

# Algorithm

**Proposition.** For every connected component $C$ of the set $\mathcal{P} = \{x \in \mathbb{R}^n \mid f_1(x) = 0, \ldots, f_m(x) = 0\}$, we have

$$Z(C) \subset \bigcup_{\substack{S \subset \{1,\ldots,m\} \times \{+,-\} \\ 1 \le \#S \le n}} \pi_x(\mathcal{W}_S \cap \{t = 0\}).$$

This enables us to compute a finite set of sampling points of the connected components of $\mathcal{P}$:

- recursive procedure;
- at each step, solve the polynomial systems defining the corresponding $\mathcal{W}_S$ over $\overline{\mathbb{Q}(t)}$ and set $t = 0$.

# Closed Sign Conditions

The previous result extends to sets defined by equalities and non-strict inequalities:

$$\mathcal{P}_\sigma = \{x \in \mathbb{R}^n \mid f_1(x)\sigma_1 0, \ldots, f_m(x)\sigma_m 0\}, \text{ with } \sigma \in \{\leq, =, \geq\}^m.$$

Deform $\mathcal{P}_\sigma$ by means of the sets $\mathcal{P}_{\sigma,t}$ defined by:

- $h_i^+(t,x) \geq 0$ and $h_i^-(t,x) \leq 0$ for all $i$ such that $\sigma_i$ is an $=$,
- $h_i^+(t,x) \geq 0$ for all $i$ such that $\sigma_i$ is a $\geq$,
- $h_i^-(t,x) \leq 0$ for all $i$ such that $\sigma_i$ is a $\leq$.

# Algorithm and Complexity

**Theorem C (J.-Perrucci-Sabia)**

There is a probabilistic algorithm which, given polynomials $f_1, \ldots, f_m \in \mathbb{Q}[x_1, \ldots, x_n]$, computes a finite set of points $\mathcal{M}$ such that $\mathcal{M} \cap C \neq \emptyset$ for each connected component $C$ of the realization of every feasible sign condition $\sigma \in \{\leq, =, \geq\}^m$.

The algorithm performs $O\Big((L+d)d^{2n}\big(\sum_{s=1}^{\min\{m,n\}} 2^s \binom{m}{s}\binom{n-1}{s-1}^2\big)\Big)$ arithmetic operations in $\mathbb{Q}$ (up to logarithmic factors), where $d = 2\lceil \frac{1}{2}\max\{\deg f_i\}\rceil$ and $L$ is the input length.

Therefore, we derive a probabilistic algorithm for the computation of all feasible sign conditions $\sigma \in \{\leq, =, \geq\}^m$ for arbitrary polynomials $f_1, \ldots, f_m$ in $\mathbb{Q}[x_1, \ldots, x_n]$.