Preorders and Computational Semi-Algebraic Geometry

Victoria Powers
Emory University
Atlanta, GA, USA

Claus Scheiderer
Universität Regensburg
Regensburg, Germany

San Diego	⟵	Honolulu	⟵	Atlanta
7:30 a.m.	=	5:30 a.m.		

1. What is semi-algebraic geometry and why is it interesting?
2. What are preorders and what do they have to do with semi-algebraic geometry?
3. Some results (not many!)
4. Algorithms
5. Open questions (many!)

Consider the following real variety:

$$V = \{(x, y) \in \mathbf{R}^2 \mid y^2 = x(x^2 - 1)\}$$

Then V is an irreducible variety, but not connected as a topological space. V has two connected components

$$C_1 = \{(x, y) \in \mathbf{R}^2 \mid y^2 = x(x^2 - 1), x \leq 0\}$$

$$C_2 = \{(x, y) \in \mathbf{R}^2 \mid y^2 = x(x^2 - 1), x > 0\}$$

Thus in Real Algebraic Geometry we should allow subsets of $\mathbf{R}^n$ defined by polynomial **inequalities**.

A **semi-algebraic set** in $\mathbf{R}^n$ is one defined by boolean combination of a finite number of polynomial inequalities.

Note: $\{f = 0\} \leftrightarrow \{f \geq 0, f \leq 0\}$.

Semi-algebraic sets arise naturally in Real Algebraic Geometry and in applications, e.g., to Robotics. They take into account the additional structure of the real numbers, namely, that they have an order.

Notations

We fix n and let $R := \mathbf{R}[x_1, \ldots, x_n]$. Let Σ denote the set of sums of squares of elements in R, and say $f \in \Sigma$ is **sos**.

$f \in R$ is **psd** (positive semi-definite) if $f(\alpha) \geq 0$ for all $\alpha \in \mathbf{R}^n$.

Semi-algebraic sets: Given a subset $W \subseteq R$, define $S(W) := \{\alpha \in \mathbf{R}^n \mid f(\alpha) \geq 0 \text{ for all } f \in W\}$.

A **basic closed semi-algebraic set** in $\mathbf{R}^n$ is a subset of the form $S(W)$, where W is finite. If $W = \{f_1, \ldots, f_k\}$, we write $S(f_1, \ldots, f_k)$ for $S(W)$.

Preorders: $P \subseteq R$ is a **preorder** if $P + P \subseteq P$, $P \cdot P \subseteq P$, and $\Sigma \subseteq P$.

Examples: Σ. The set of psd polynomials in R.

Given a subset $U \subseteq R$, the **preorder generated by** U , denoted $P(U)$, is $\{\sum_{i=1}^{m} a_i f_{i_1} \cdot \ldots \cdot f_{i_l} \mid m \in \mathbf{N}, a_i \in \Sigma, f_{i_j} \in U\}$. If $U = \{f_1, \ldots, f_k\}$ is finite, we write $P(f_1, \ldots, f_k)$ for the preorder generated by U.

It is clear from the definitions that $P \subseteq P(S(P))$.

A preorder is **saturated** if $P = P(S(P))$.

Preorders seem to be the "right" algebraic objects to study:

- Given $f_1, \ldots, f_k \in R$, then $S(f_1, \ldots, f_k) \neq \emptyset$ if and only if $-1 \notin P(f_1, \ldots, f_k)$.

- Schmüdgen's Theorem: Given $f_1, \ldots, f_k \in R$ and suppose $S = S(f_1, \ldots, f_k)$ is compact. Then $f > 0$ on S implies $f \in P(f_1, \ldots, f_k)$. (K. Schmüdgen, 1991) The original proof uses functional analysis. There is a purely algebraic proof due to T. Wörmann.

Definition: A preorder P is **archimedean** if for any $f \in R$ there is some $m \in \mathbf{N}$ such that $m \pm f \in P$. Equivalently, if there exists $N \in \mathbf{N}$ such that $N \pm x_i \in P$ for all i.

- Theorem: $S(f_1, \ldots, f_k)$ is compact if and only if $P(f_1, \ldots, f_k)$ is archimedean. This follows from Schmüdgen's Theorem, and there is also a direct proof due to T. Wörmann.

However, preorders behave badly!

- There exist preorders P so that $S(P)$ is not semi-algebraic. E.g., given $e^x = \sum_{i=0}^{\infty} c_i x^i$, set $p_j = y - \sum_{i=0}^{j} c_i x^i \in \mathbf{R}[x,y]$ and let P be the preorder generated by the p_j's. Then $S(P)$ is the graph plus interior of $y = e^x$, which is clearly not semi-algebraic.

- In fact, any closed subset of $\mathbf{R}^n$ can be written as $S(P)$ for some preorder $P \subseteq R$. (Perhaps preorders are too general an object?)

- In general, preorders are not finitely generated. For example, let $P \subseteq R$ be the set of psd polynomials in R. By Hilbert's 17th problem, we know that every $f \in P$ is a sum of squares of elements in $\mathbf{R}(X) := \mathbf{R}(x_1, \ldots, x_n)$. Further, for $n \geq 3$ it is well-known that there is no $g \in R$ such that every $f \in P$ has a representation $\sum (p_i/g)^2$ $p_i \in R$. However, if P were finitely generated, we could find such a common denominator, thus P cannot be finitely generated for $n \geq 3$.

Finite Generation of Preorders

Question: Let $S \subseteq \mathbf{R}^n$ be a basic closed semi-algebraic set and let $P = P(S)$ be the preorder of all polynomials which are non-negative on S. When is P finitely generated?

Theorem. Let P be a finitely generated preorder in $\mathbf{R}[x_1, \ldots, x_n]$ such that dim $S(P) \geq 3$. Then there exists a psd polynomial which is not contained in P.

Corollary. If $S \subseteq \mathbf{R}^n$ is a basic closed semi-algebraic set with $\dim(S) \geq 3$, then $P(S)$ is not finitely generated.

Proposition. Suppose S is a closed semi-algebraic subset of $\mathbf{R}^1$, then $P(S)$ is finitely generated. Further, if $S \subseteq \mathbf{R}^n$ is a finite set or a line, then $P(S)$ is finitely generated.

It is tempting to conjecture that given any basic, closed semi-algebraic set with $\dim(S) = 1$, then $S(P)$ is finitely generated. However, this is false!

Theorem. Let $g(x) \in \mathbf{R}[x]$ be a cubic polynomial with only one real root and let E be the elliptic curve $\{(x,y) \in \mathbf{R}^2 \mid y^2 = g(x)\}$. Given any finitely generated preorder $P = P(g_1, \ldots, g_k)$ where $g_i \geq 0$ on E. Then there is some f such that $f \geq 0$ on E and $f \notin P$. In particular, the preorder of all polynomials in $\mathbf{R}[x,y]$ which are ≥ 0 on E is not finitely generated.

The proof of the theorem is algorithmic, in the sense that if we are given E and the g_i's explicitly, there is an algorithm to produce the f. Further, we can show that given such an f, there exists an $h \in (y^2 - g(x))$ such that $f + h$ is psd (globally). Thus we know that $f + h$ is psd, but not sos. (Perhaps this yields a method for constructing explicit "families" of psd, not sos, polynomials in $\mathbf{R}[x,y]$?)

Corollary. The preorder of psd polynomials in $\mathbf{R}[x,y]$ is not finitely generated.

Question: Does there exist a "common denominator" for writing all psd polynomials in $\mathbf{R}[x,y]$ as sums of squares in $\mathbf{R}(x,y)$?

Algorithms

Given $f_1, \ldots, f_k \in R$, in general it is difficult to decide if the variety $V = V(f_1, \ldots, f_k)$ has a real point or not. If V is zero dimensional (as a complex variety), then there are good algorithms for counting the number of real points in V. In fact, there exists software: RealSolving (developed by F. Roullier and M.-F. Roy, Université Rennes).

Is there a way to work with preorders computationally? For example, given a finitely generated preorder $P = P(f_1, \ldots, f_k)$ and $g \in R$, is there an algorithm to decide if $g \in P$ or not? Given that $S(P)$ is compact and $g > 0$ on $S(P)$, we know that $g \in P$ (by Schmüdgen), can we find an explicit representation for $g \in P$?

Suppose P is the preorder of all psd polynomials in R and we want to decide if $f \in P$ or not. There is an algorithm (E. Becker, P., T. Wörmann): Let $F = t^2 f + 1$, where t is a new variable, then $f \in P$ iff $V(F)$ has no real point. We can reduce to the zero dimensional case and then use RealSolving.

There is an algorithm for deciding whether or not f is sos (P., Wörmann), based on work of (Choi, Lam, Reznick). This algorithm can be extended to an algorithm for the membership problem for preorders, but only if we put a bound on the degree of the sums of squares that occur in a representation of f in the preorder.

Question: Given $P = P(f_1, \ldots, f_k)$, does there exist a bound on the degree of the "occurring data" in a representation of $g \in P$?

It is easy to see that such a bound cannot be only in terms of the degrees of the f_i's and g. G. Stengle shows that such a bound exists in a very special case: In $\mathbf{R}[x]$, for any f.g. P with $S(P) = [-1, 1]$ and any $g > 0$ on $[-1, 1]$. There exists a computational proof of Schmüdgen's Theorem in $\mathbf{R}[x]$ (P., Reznick), and this proof should lead to a similar bound for any preorder P in $\mathbf{R}[x]$ with $S(P)$ compact.

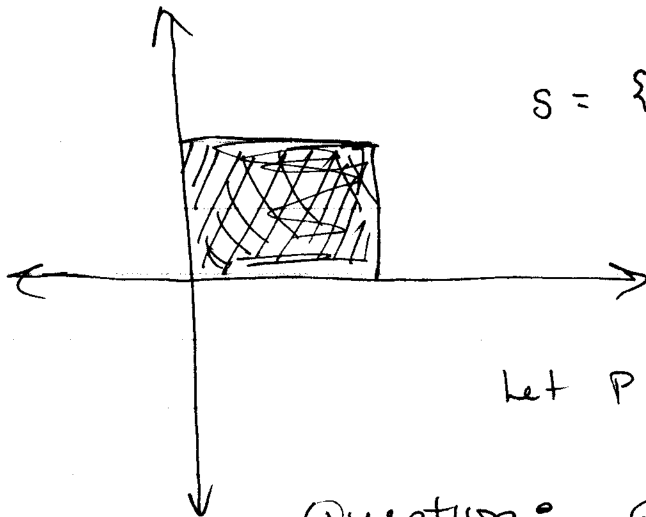
Question: Does there exist a computational proof of Schmüdgen's Theorem?

Question: In the definition of preorder, should be replace the requirement "$\Sigma \subseteq P$" by "all psd polynomials are in P"?

Question: When does Schmüdgen's Theorem hold for non-compact S? The only examples we know where it holds for non-compact S are 1-dimensional. Let P be a finitely generated preorder with $S(P)$ not compact and $\dim S(P) = 2$. Is there f such that $f > 0$ on S and $f \notin P$?

Question: Is there some kind of semi-algebraic "Groebner Basis" for preorders?

Let $S \subseteq \mathbb{R}^2$ be the square



$S = \{x \geq 0 \wedge y \geq 0 \wedge 1-x \geq 0 \wedge 1-y \geq 0\}$

Let $P = P(x, y, 1-x, 1-y)$

Question: Given $f \in \mathbb{R}[x,y]$, with $f \geq 0$ S, is $f \in P$?

Prove or find a counterexample