Complexity analysis of polynomial algorithms

Ignacio Iker Prado Rujas
Universidad Complutense de Madrid (UCM)
Doble Grado en Matemáticas e Ingeniería Informática

May 6, 2016

Tutors:
José F. Fernando *&* J.M. Gamboa

Abstract

This work is about three different proofs of the same fact and a computational comparison between them, looking for the best one.

Let R be a real closed field and $n \geq 2$. We prove that: (1) for every finite subset F of R^n, the semialgebraic set $R^n \setminus F$ is a polynomial image of R^n; and (2) for any independent linear forms $l_1, \ldots, l_r$ of R^n, the semialgebraic set $\{l_1 > 0, \ldots, l_r > 0\} \subset R^n$ is a polynomial image of R^n.

The key proof here is that $Q = \{x > 0, y > 0\}$ is a polynomial image of $\mathbb{R}^2$. This assert is proved in three different ways: a first approach using real algebraic geometry; a second and shorter one, using the composition of 3 rather simple maps; and a third one that applies topology with no computer computations.

(...)

1

Polynomial images of R^n

1.1 Introduction

Definition 1.1. Let R be a real closed field and $m, n \in \mathbb{N}_{>0}$. A map $f = (f_1, \ldots, f_n) : R^m \longrightarrow R^n$ is said to be polynomial if $f_i \in R[x_1, \ldots, x_m], i = 1, \ldots, n$.

A very famous theorem by Tarski and Seidenberg states:

Theorem 1.1 (Tarski-Seidenberg)**.** The image of any polynomial map $f : R^m \longrightarrow R^n$ is a semialgebraic subset of R^n.

In this work we are studying sort of a converse of this statement. In an *Oberwolfach* week, J.M. Gamboa proposed to characterize the semialgebraic subsets of R^n that are polynomial images of R^m.

Notation. We need to mention to which topology we refer when we talk about closures, boundaries, etc. More specifically, the **exterior boundary** of a set S is $\delta S := \overline{S} \backslash S$, with $\overline{S}$ being the **closure** of S in R^n in the usual topology. $\overline{S}^{\text{zar}}$ is the closure of S with respect to the Zariski topology. $A \subset R^n$ is **irreducible** if its Zariski closure $\overline{A}^{\text{zar}}$ is an irreducible algebraic set.

1.1.1 Necessary conditions and examples

To begin working on this idea, we provide some necessary conditions for a set $S \subset R^n$ to be polynomial image of R^m.

It is trivial that for $m = n = 1$ (so $f : R \to R$), the images of polynomial maps are either a set of one point or singletons (if the map is constant), or unbounded closed intervals (think of $f(x) = x^2$), or the whole R (think of $f(x) = x$).

In the general case, by Tarski-Seidenberg, S must be a semialgebraic set and, moreover, semialgebraically connected. Even more, by the identity principle for polynomials, S is irreducible and pure dimensional.

In the polynomial case there are more constrains.

Definition 1.2. A polynomial map $f : R^m \longrightarrow R^n$ is said to be **semialgebraically proper at a point** $p \in R^n$ if there exists an open neighbourhood K of p such that the restriction

$$\begin{aligned} f^{-1}(K) &\longrightarrow K \\ x &\longmapsto f(x) \end{aligned}$$

is a semialgebraically proper map.

Definition 1.3. A parametric semiline of R^n is a non-constant polynomial image of R.

It is clear that every parametric semiline is semialgebraically closed, since every polynomial map from R to R^n is semialgebraically proper. Let $\mathscr{S}_f$ denote the set of points $p \in R^n$ at which f is **not** semialgebraically proper.

Theorem 1.2 (Jelonek)**.** Let $f : R^2 \longrightarrow R^2$ be a dominant polynomial map. Then $\mathscr{S}_f$ is a finite union of parametric semilines.

With all these ideas in mind, we can get some conclusions in the following proposition:

Proposition 1.1. *Let $f : R^m \longrightarrow R^n$ be a polynomial map and $S = f(R^m)$.*

(1) $\delta S \subset \mathscr{S}_f$.

Proof. Suppose $p \in \delta S \backslash \mathscr{S}_f$. Because $p \notin \mathscr{S}_f$, there exists an open neighbourhood K of p such that the restriction $f^{-1}(K) \to K$ of f is proper, and thus its image $K \cap S$ is a closed subset of K. Hence, $p \in K \cap \overline{S} = K \cap (\overline{K \cap S}) = K \cap S$, which yields in a contradiction.

(2) Let $m = n = 2$ and Γ be a 1-dimensional irreducible component of $\overline{S}^{zar}$. Γ is the Zariski closure of a parametric semiline of R^2.

Proof. Since f is a dominant map, we can apply Jelonek and get that $\mathscr{S}_f$ is a finite union of parametric semilines, say $M_1, \dots, M_s$ in R^2. Then, using (1) we get: $\Gamma \subset \overline{\delta S}^{\text{zar}} \subset \overline{\mathscr{S}_f}^{\text{zar}} = \cup_{i=1}^{s} \overline{M_i}^{\text{zar}}$. Lastly, using that both Γ and the $\overline{M_i}^{\text{zar}}$'s are irreducible, we must have that for some $i = 1, \dots, s : \Gamma = \overline{M_i}^{\text{zar}}$.

(3) Let $p : R^n \to R$ be a polynomial map which is non-constant on S. Then $p(S)$ is unbounded.

Proof. If $a \in R^m$, let us define $\varphi_a : R \to R$ as $\varphi_a(t) := p(f(ta))$. Then, $\forall a \in R^m$, $p(S)$ would contain the image $\varphi_a(R) :\ \varphi_a(R) \subset p(S)$. Now suppose that $\varphi_a(R)$ is bounded $\forall a$. Then $\varphi_a(R)$ would be a point r_a, and given $a, b \in R^m :\ \varphi_a(1) = p(f(ta)) = r_a = \varphi_a(0) = \varphi_b(0) = r_b = p(f(tb)) = \varphi_b(1)$. This implies that p would be constant on S, which is a contradiction.

Corolary 1.1. *Because of (3) in proposition 1.1, all linear projections of S are either a point or unbounded. Consequently, S is also unbounded or a point.*

Example 1.1.

(i) *One.*

A

Auxiliary definitions and results

Definition A.1. A **real closed field** is a field R that has the 1^{st} order properties as the field of real numbers $\mathbb{R}$.

Definition A.2. A **semialgebraic set** is a subset $S \subset R^n$ (for some real closed field R) defined by a finite sequence of polynomial equations of the form:

$$\begin{gathered} P_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ P_r(x_1, \ldots, x_n) = 0 \\ Q_1(x_1, \ldots, x_n) > 0 \\ \vdots \\ Q_l(x_1, \ldots, x_n) > 0 \end{gathered}$$

. A **semialgebraic map** is a map that has semialgebraic graph. Moreover, the finite union, intersection and complement of semialgebraic sets is still a semialgebraic set.

Definition A.3 (Zariski topology)**.** It is a topology on algebraic varieties whose closed sets are the algebraic subsets of the variety. Its sets are defined as the set of solutions of a system of polynomial equations over a field R. In this topology, when we talk about the irreducibility of a element, we mean that it is not the union of two smaller sets that are closed under the Zariski topology.

Definition A.4. A set $S \subset R^n$ is said to be **pure dimensional** if its irreducible components are of the same dimension.

Definition A.5. A map f is called **proper** if the preimage of every compact set is compact. A semialgebraic map $f : f^{-1}(K) \longrightarrow K$ is called **semialge-**

braically proper if the preimage $f^{-1}(C)$ of a compact and semialgebraic subset $C \subset K$ is compact. This condition is weaker than the previous one.

Definition A.6. A polynomial map is said to be **dominant** if it has a dense image.

Bibliography