comput complexity 4 (1994), 12–36 1016-3328/94/040012-25 $1.50+0.20

A NOTE ON RABIN'S WIDTH OF A COMPLETE PROOF

José L. Montaña, Luis M. Pardo
and Tomás Recio

Abstract. We introduce and analyze the concept of generic width of a semialgebraic set, showing that it gives lower bounds for decisional complexities. By means of the computation of the generic width we are able to solve rigorously the complexity problems posed by M.O. Rabin in [10], such as optimization of linear mappings on finite sets. We show that the results on the generic width can also be applied to obtain lower bounds for problems which in general do not admit a linear mapping description, such as optimization of polynomial mappings on finite sets, existence of a real root, finite selection and subset decision, or the direct oriented–convex hull problem introduced by J. Jaromczyk in [8].
Key words. Algebraic complexity theory; decisional complexity; semialgebraic sets; width of a complete proof; generic width of a semialgebraic set.
Subject classifications. 68Q25, 68Q40, 14P20, 14P10.

1. Introduction

Within the general framework of algebraic complexity theory, a paper of M. O. Rabin ([10]) discussed the optimality of algorithms solving the membership problem for convex sets given by the simultaneous positivity of linear forms. Formally, the author analyzed the complexity of convex sets of the kind

$$W = \{x \in \mathbb{R}^n : L_1(x) \geq 0, \dots, L_m(x) \geq 0\}$$

where the $L_j : \mathbb{R}^n \longrightarrow \mathbb{R}$ are affine linear functions for $1 \leq j \leq m$. The main applications presented by Rabin deal with lower bounds for the following problems (involving real numbers as inputs, and all having complexity $O(N)$).

Problem 1.1. *Given N real numbers $x_1, \dots, x_N \in \mathbb{R}$, find j such that x_j is the maximum of all of them.*

PROBLEM 1.2. *Given N real numbers $x_1, \ldots, x_N \in \mathbb{R}$, find j such that x_j is the minimum of all of them.*

PROBLEM 1.3. *Given $2N$ real numbers $x_1, \ldots, x_N, y_1, \ldots, y_N \in \mathbb{R}$, find j such that $x_j + y_j$ is the minimum of all the sums $x_i + y_i$ for $1 \leq i \leq N$.*

PROBLEM 1.4. *The membership problem for an N–orthant, i.e., given $x \in \mathbb{R}^N$ decide whether x belongs to the semialgebraic set*

$$O_N = \{x = (x_1, \ldots, x_N) \in \mathbb{R}^N : x_1 \geq 0, \ldots, x_N \geq 0\}.$$

Problems 1.1 to 1.3 above are particular cases of the *maximization and minimization of linear functions over finite sets* problem. As in [1], one can ask the natural question: why can't these problems be solved in constant time?

Rabin's computation model in [10] is the (non–uniform) model given by a sequence of algebraic computation trees $\{T_N\}_{N \in \mathbb{N}}$. In terms of the size N of the problem instances (the cardinality of the input set), the complexity of the problem is the number of arithmetic operations and polynomial sign tests that are performed to reach a leaf in T_N. As was observed in [9], a usual method to obtain lower bounds in this model is to choose a weaker measure of complexity: for instance, Rabin introduced *decisional* measures of complexity (taking arithmetic operations for free). Then, he computed the *width of a complete proof of a simultaneous positivity* for the convex set W, claiming that, in general, the minimum width gives a lower bound for the decisional complexity of each problem. In order to conclude this claim he argues that a complete proof is immediately obtained from an algebraic computation tree, showing in this way that $\Omega(N)$ is actually a lower bound for the problems. As remarked in Section 3 below, the relationship between complete proofs and algebraic computation trees is not so straightforward, and the validity of using the width as a lower bound is not so clear.

In 1981, J.W. Jaromczyk [8] extended the concept of the width of a complete proof to the case of non–linear polynomials, but without noticing this problem. Thus, he also assumes—without any proof—that the width of any complete proof relative to the trivial clause $[1 \neq 0]$ provides a lower bound for the following geometric problem.

DIRECT ORIENTED–CONVEX HULL PROBLEM (DO–CH PROBLEM). *Given a sequence $(z_1, \ldots, z_N)$ of points in the real plane, $z_i \in \mathbb{R}^2$, decide whether they are the clockwise oriented vertices of their convex hull.*

The present note intends to fill in the gaps in [8] and [10]. First, we consider the complexity analysis in the more general setting of semialgebraic sets; see

Section 2 for definitions. Then, in Section 3, after extending the definition of width in [8] and [10], we introduce the concept of the *generic width of a semialgebraic set*. The relation and differences between width and generic width are explained in Subsection 3.6. Next, in Section 4, we prove that the generic width gives a lower bound for the decisional complexity. We remark that it is unknown whether the "width" is a lower bound for decisional complexity. Luckily we are able to compute in many cases (see, for instance, Corollaries 3.9, 3.10, and 3.11) the generic width of a semialgebraic set and we observe that, in the examples studied by Rabin, the generic width agrees with the minimum width of any complete proof relative to any non-zero polynomial (see Subsection 4.5). As an application of Theorem 3.8, we are able to show that Problems 1.1 to 1.4 above and the DO–CH problem all have linear lower bounds, as stated by Rabin and Jaromczyk respectively (see Subsections 4.1 and 4.2).

Our techniques are also applied to new problems involving non–linear polynomials, as *finite polynomial optimization* (which strictly includes Problems 1.1 to 1.3 above).

Let $f \in \mathbb{R}[X_1, \ldots, X_n]$ be a fixed non–constant polynomial.

FINITE POLYNOMIAL MAXIMIZATION. *Given a finite set $\mathcal{F} = \{x_1, \ldots, x_N\} \subseteq \mathbb{R}^n$ find an element $x_i \in \mathcal{F}$ such that $f(x_i)$ is the maximum of $f(\mathcal{F})$.*

FINITE POLYNOMIAL MINIMIZATION. *Given a finite set $\mathcal{F} = \{x_1, \ldots, x_N\} \subseteq \mathbb{R}^n$ find an element $x_i \in \mathcal{F}$ such that $f(x_i)$ is the minimum of $f(\mathcal{F})$.*

Other applications are *finite subset decision, finite selection* (under the hypothesis of real complete intersection) and *existence of a real root* (see Section 4 for more detailed descriptions).

The main technique used in Section 3 of this paper to compute lower bounds of the generic width of semialgebraic sets detects a local obstruction which is invariant under semialgebraic diffeomorphisms (i.e., Nash diffeomorphisms). Namely, we find that for any semialgebraic set W with a *Nash m–corner point*, the inequality $m \leq \omega_{gen}(W)$ holds (see Theorem 3.8 below and [13] for the terminology). Therefore, the complexity of W is also greater than m. We think that this is an interesting result by itself, since the usual methods used to provide lower bounds of semialgebraic sets regard only some global geometric features of the considered set, such as connected components or geometric degrees (see [1], [9], [14], or [15]). For this reason, we have introduced as a mere technical device some facts from real algebraic geometry and elementary Nash function theory (see [2] and [3]).

2. Decisional Measures of Complexity

A *semialgebraic set* is a subset W of some real affine space, $W \subseteq \mathbb{R}^n$, that be described by a boolean combination of polynomial equations and inequ ties, i.e., the set W can be given as

$$W = \bigcup_{i \in I} \{x \in \mathbb{R}^n : \; p_i(x) = 0, \; q_{i,j}(x) > 0 \text{ for } j \in J\},$$

where the polynomials p_i, $q_{i,j} \in \mathbb{R}[X_1, \ldots, X_n]$ for $i \in I$, $j \in J$, and I are finite sets. The subset W is said to be *open basic* in $\mathbb{R}^n$ if $\#I$ and only strict inequalities occur. *Closed basic* semialgebraic subsets W $\mathbb{R}^n$ are those given as a simultaneous positivity of arbitrary polynomials, $W = \{x \in \mathbb{R}^n : p_1(x) \geq 0, \ldots, p_r(x) \geq 0\}$. The following result rel the property of being closed (respectively, open) for the Euclidean topol in $\mathbb{R}^n$ and the existence of formulae describing the set only with "≥ 0" conditions.

FINITENESS THEOREM *(see [3], 2.7.1, [7], and [11]). Every closed semia braic subset W of $\mathbb{R}^n$ is a finite union of closed basic semialgebraic sets, there are non–negative integers k, t, and polynomials $p_{i,j} \in \mathbb{R}[X_1, \ldots,$ such that*

$$W = \bigcup_{i=1}^{t} \{x \in \mathbb{R}^n : p_{i,1}(x) \geq 0, \ldots, p_{i,k}(x) \geq 0\}.$$

As a consequence of this, by taking complements, semialgebraic sets o in the Euclidean topology in $\mathbb{R}^n$ are finite unions of open basic semialgeb sets.

An *algebraic computation tree* (ACT for short), $T = T(X_1, \ldots, X_n)$, in duced in [1] and [10], is a rooted binary tree with a finite number of no Nodes are of four types: just one input node (the root of the tree, accept $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$ as input), computation nodes (nodes with just one c where an arithmetic operation is performed), branching nodes (nodes with children where a sign test "$z_i \; \mu \; 0$?", $\mu \in \{\geq, >, =\}$ is executed for some prec puted z_i) and output nodes (also called leaves, labeled with the correspon *YES/NO* answer). With respect to the definitions in [10] we have added tests of the form "$P = 0$?" but this does not modify either the model of c putation or the complexity measure we describe below. Both approache describing ACT's are essentially equivalent.

The subset $W(T)$ of $\mathbb{R}^n$ accepted by an ACT, $T = T(X_1, \ldots, X_n)$, is subset of all points in $\mathbb{R}^n$ that follow a path in T from the root to some

ROLLARY 4.5. *Under the above hypotheses, finite subset decision and finite ction have complexity in $\Omega(\#(\mathcal{F})) = \Omega(N)$.*

OOF. First of all, observe that the ideal $\mathcal{I} = (f_1, \ldots, f_d)$ is a real complete rsection ideal and there must be a point $\alpha \in \mathbb{R}^n$ such that

$$f_1(\alpha) = 0, \ldots, f_d(\alpha) = 0, \text{ and } \operatorname{rank} J(f_1, \ldots, f_d)_\alpha = d.$$

On the other hand, to get lower bounds for finite subset decision, we note it can be understood as the membership problem for a semialgebraic subset $\subseteq \mathbb{R}^{nN}$. As above let us denote by $(X_1, \ldots, X_{nN})$ the coordinates of the ients of $\mathbb{R}^{nN}$ and define the polynomials

$$g_{i,j}(X_1, \ldots, X_{nN}) = f_i(X_{jn+1}, \ldots, X_{(j+1)n}). \tag{4.4.2}$$

We have the following equality:

$$SD = \{(x_1, \ldots, x_{nN}) \in \mathbb{R}^{nN} : g_{i,j}(x_1, \ldots, x_{nN}) \geq 0 \text{ for } 1 \leq i \leq d \text{ and } 1 \leq j \leq N\}.$$

Finally, the point $A = (\alpha, \ldots, \alpha) \in \mathbb{R}^{nN}$ verifies the hypothesis of Corollary and $dN \leq \omega_{gen}(SD, \mathbb{R}^{nN})$, which is smaller than the complexity of finite set decision.

For finite selection, the hypothesis implies that the property $\mathcal{R}$ above is trivial, so we have a non–empty semialgebraic subset of $S \subseteq \mathbb{R}^{nN}$ given $S = \{(x_1, \ldots, x_N) \in \mathbb{R}^{nN} :$ no x_i verifies property $\mathcal{R}\}$.

Lower bounds for finite selection can be immediately obtained from lower nds from the membership problem for S. However, using the notation of .2), we observe that

$$S = \{(x_1, \ldots, x_{nN}) \in \mathbb{R}^{nN} : g_{i,j}(x_1, \ldots, x_{n.N}) < 0 \text{ for } 1 \leq i \leq d \text{ and } 1 \leq j \leq N\}.$$

The point $B = (\alpha, \ldots, \alpha) \in \mathbb{R}^{nN}$ verifies the hypothesis of Corollary 3.9. ce, $dN \leq \omega_{gen}(S, \mathbb{R}^{nN}) \leq C_D(S)$, which is a lower bound for the complexity nite selection. □

Existence of real root condition. Here we consider the size of forle that describe the existence of real roots for any polynomial of a fixed ee d. Any of these formulae describes a semialgebraic subset of $\mathbb{R}^{d+1}$. Our ose now will be to prove the following Corollary.

COROLLARY 4.6. *Any quantifier free first order formula equivalent to*

$$\exists z \in \mathbb{R} \quad X_d z^d + X_{d-1} z^{d-1} + \cdots + X_0 = 0 \tag{4.5.1}$$

involves at least $\frac{d}{2}$ polynomials.

PROOF. Consider the polynomial

$$P(T_1, \ldots, T_{\frac{d}{2}}, X) = (X^2 + T_1) \cdots (X^2 + T_{\frac{d}{2}}).$$

From any formula $\Phi(X_d, \ldots, X_0)$ equivalent to (4.5.1), we obtain by substitution a formula $\varphi(T_1, \ldots, T_{\frac{d}{2}})$ describing the semialgebraic set

$$\begin{aligned} E =& \{(t_1, \ldots, t_{\frac{d}{2}}) \in \mathbb{R}^{\frac{d}{2}} : \exists x \in \mathbb{R} \text{ such that } P(t_1, \ldots, t_{\frac{d}{2}}, x) = 0\} \\ =& \{t_1 \leq 0\} \cup \ldots \cup \{t_{\frac{d}{2}} \leq 0\}. \end{aligned}$$

The number of polynomials involved in φ is bigger than the decisional complexity of E. Finally,

$$C_D(E, \mathbb{R}^{\frac{d}{2}}) = C_D(E^c, \mathbb{R}^{\frac{d}{2}}) \geq \omega_{gen}(\{t_1 > 0, \ldots, t_{\frac{d}{2}} > 0\}, \mathbb{R}^{\frac{d}{2}}) = \frac{d}{2}. \ \square$$

4.5. Rabin's Theorem Revisited. Finally, we remark that Theorem 3.8 and Proposition 4.1 above yield as a consequence Rabin's claim in a particular case: one may use the minimum width of complete proofs as a lower bound under the strong restriction of *linear functions and sign independence*.

As in [10], a collection $p_1, \ldots, p_m : \mathbb{R}^n \longrightarrow \mathbb{R}$ of polynomial mappings is said to be *sign independent* in an open semialgebraic set $U \subseteq \mathbb{R}^n$ if, for every sequence of sign conditions $\mu_1, \ldots, \mu_m \in \{<, =, >\}$, the set $\{x \in U : p_1(x)\mu_1 0, \ldots, p_m(x)\mu_m 0\}$ is non–empty.

COROLLARY 4.7. *Under the conventions of Section 3 and Definition 3.1, let $SP(X)$ be the formula $L_1(X) \geq 0 \wedge \cdots \wedge L_m(X) \geq 0$ and W the convex set $W = \{x \in \mathbb{R}^n : L_1(x) \geq 0, \ldots, L_m(x) \geq 0\}$. Then,*

i) for every complete proof $\mathcal{P}$ of $SP(X)$ relative to some non–zero polynomial $Q(X)$, $\omega_{gen}(W, \mathbb{R}^n) \leq Width(\mathcal{P})$,

ii) if, in addition to the above hypothesis, $L_1(X), \ldots, L_m(X)$ are sign independent in $\mathbb{R}^n$, then we have

$$\omega_{gen}(W, \mathbb{R}^n) = \varpi(W, \mathbb{R}^n) = m = C_D(W).$$

OBLEM 4.3. *Decide whether x_1 verifies $f(x_1) = \max f(\mathcal{F})$.*

is is the membership problem for a semialgebraic subset of $M \subseteq \mathbb{R}^{nN}$. are going to describe this subset. Let us denote by $(X_1, \ldots, X_{nN})$ the rdinates of the elements of $\mathbb{R}^{nN}$. Let us also define the set of polynomials:

$$g_i(X_1, \ldots, X_{nN}) = f(X_1, \ldots, X_n) - f(X_{in+1}, \ldots, X_{(i+1)n}),$$

re $1 \leq i \leq N-1$. Clearly, we have

$$M = \{x \in \mathbb{R}^{nN} : g_1(x) \geq 0, \ldots, g_{N-1}(x) \geq 0\}.$$

f is a non-constant polynomial, the polynomial $g(X_1, \ldots, X_n, Y_1, \ldots, Y_n) =$ $X_1, \ldots, X_n) - f(Y_1, \ldots, Y_n)$ changes sign in $\mathbb{R}^{2n}$. Now, applying the Change Sign Criterion for real hypersurfaces (see [3], 4.5.1), we know there is a nt $(\alpha, \beta) \in \mathbb{R}^{2n}$ such that $g(\alpha, \beta) = 0$ and $\frac{\partial g}{\partial X_j}(\alpha, \beta) \neq 0$ or $\frac{\partial g}{\partial Y_j}(\alpha, \beta) \neq$ or some j, $1 \leq j \leq n$. Finally, consider the point $A = (\alpha, \beta, \ldots, \beta) \in \mathbb{R}^{nN}$ ifying $g_1(A) = \cdots = g_{N-1}(A) = 0$ and $\operatorname{rank} J(g_1, \ldots, g_{N-1})_A = N-1$. Then, $-1 \leq \omega_{gen}(M, \mathbb{R}^{nN})$, which is smaller than the decisional complexity of M, wanted. □

. **Direct oriented–convex hull.** As was observed in the Introduction, problem was motivated by the work of J. Jaromczyk [8], who applied the th directly to get lower bounds for the DO-CH problem. The limitations his approach are those of [10], which we have discussed in Section 3. Now, provide lower bounds for the problem using Theorem 3.8 and, specifically, ollary 3.10.

ROLLARY 4.4. *The problem DO–CH has complexity at least $\Omega(N)$.*

OOF. Given $z_i = (x_i, y_i), z_j = (x_j, y_j), z_k = (x_k, y_k)$, define

$$\det(z_i, z_k, z_j) = x_k.(y_i - y_j) + y_k.(x_j - x_i) + y_j.x_i - y_i.x_j.$$

decisional problem DO–CH is the membership problem for a semialgebraic set of $\mathbb{R}^{2.N}$ given by

$$D = \{(z_1, \ldots, z_N) \in \mathbb{R}^{2.N} : \det(z_1, z_2, z_3) \geq 0, \ldots, \det(z_{N-2}, z_{N-1}, z_N) \geq 0, \det(z_{N-1}, z_N, z_1) \geq 0, \det(z_N, z_1, z_2 \geq 0)\}.$$

From Corollary 3.10, it is enough to observe that the point $A \in \mathbb{R}^{2 \cdot N}$ given by

$$A = ((1,0), (2,0), \ \ldots, (N-1, 0), (N, -1))$$

verifies the following equations:

$$\begin{aligned} &\det((i,0), (i+1,0), (i+2,0)) = 0 \quad \text{for } 1 \leq i \leq N-3, \\ &\det((N-2,0), (N-1,0), (N,-1)) > 0, \\ &\det((N-1,0), (N,-1), (1,0)) > 0, \\ &\det((N,0), (1,0), (2,0)) > 0, \\ &\operatorname{rank} J(\det(z_1, z_2, z_3), \ldots, \det(z_{N-3}, z_{N-2}, z_{N-1}))_A = N-3. \end{aligned}$$

Thus, we conclude that $N - 3 \leq \omega_{gen}(D, \mathbb{R}^{2N}) \leq C_D(D)$, which is smaller than the complexity of DO–CH. □

4.3. Finite subset and finite selection in real complete intersections. These problems arise naturally in computational geometry. We have some fixed subset $\mathcal{A} \subseteq \mathbb{R}^n$ and a property $\mathcal{R}$ on points of $\mathbb{R}^n$. Then, we consider the following questions.

FINITE SUBSET DECISION. *Given a finite set $\mathcal{F} = \{x_1, \ldots, x_N\} \subseteq \mathbb{R}^n$, decide whether $\mathcal{F} \subseteq \mathcal{A}$.*

FINITE SELECTION. *Given a finite set $\mathcal{F} = \{x_1, \ldots, x_N\} \subseteq \mathbb{R}^n$, find a point $x_i \in \mathcal{F}$ such that x_i verifies property $\mathcal{R}$.*

The model of algebraic computation trees can only be applied when $\mathcal{A}$ is a semialgebraic set or $\mathcal{R}$ is a property described by a first order formula over the reals. Our lower bound method applies, for instance, under the following conditions:

> Assume $\{f_1, \ldots, f_d\} \subseteq \mathbb{R}[X_1, \ldots, X_n]$ to be a collection of polynomials such that the ideal $\mathcal{I} = (f_1, \ldots, f_d)$ is real of height d. Let us also assume for $\mathcal{A}$ and $\mathcal{R}$ the following hypotheses:
>
> $$\mathcal{A} = \{x \in \mathbb{R}^n : f_1(x) \geq 0, \ldots, f_d(x) \geq 0\},$$
>
> $$\mathcal{R} \leftrightarrow [f_1(X_1, \ldots, X_n) \geq 0] \vee \cdots \vee [f_d(X_1, \ldots, X_n) \geq 0].$$

Observe that in the case $d = 1$, the above hypotheses simply mean that f_1 changes its sign in $\mathbb{R}^n$ or equivalently that $\mathcal{R}$ is not the trivial property $[1 \geq 0]$ (see [3], 4.5.1, for more detailed descriptions). Now we want to show the following.

)LLARY 3.10. *Let $f_1, \ldots, f_m \in \mathbb{R}[X_1, \ldots, X_n]$ be a collection of poly-*
als for which there is a point $\alpha \in \mathbb{R}^n$ and a non-negative integer k,
$\leq m$, such that

$$f_1(\alpha) = \ldots = f_k(\alpha) = 0, f_{k+1}(\alpha) > 0, \ldots, f_m(\alpha) > 0$$

he rank of the jacobian matrix verifies rank $J(f_1, \ldots, f_k)_\alpha = k$. Then, the
ing inequality holds:

$$k \leq \omega_{gen}(\{x \in \mathbb{R}^n : f_1(x) \geq 0, \ldots, f_m(x) \geq 0\}, \mathbb{R}^n).$$

)F. First observe that the point α is a k-corner point in the semialgebraic
$f_1 \geq 0, \ldots, f_m \geq 0\}$. Consider a semialgebraic open neighborhood U of α
ined in the open set $\{x \in \mathbb{R}^n : f_{k+1}(x) > 0, \ldots, f_m(x) > 0\}$.
observe that the generic width of a set S in U is that of $S \cap U$ in U. Since
llowing set equality holds:

$$\begin{aligned} &\{x \in \mathbb{R}^n : \ f_1(x) \geq 0, \ldots, f_m(x) \geq 0\} \cap U \\ = &\{x \in \mathbb{R}^n : \ f_1(x) \geq 0, \ldots, f_k(x) \geq 0\} \cap U, \end{aligned}$$

rollary 3.9, we conclude that

$$\omega_{gen}(\{x \in \mathbb{R}^n : f_1(x) \geq 0, \ldots, f_m(x) \geq 0\}, U) = k.$$

tatement follows since for every semialgebraic set $S \subseteq \mathbb{R}^n$ and every open
lgebraic subset U of $\mathbb{R}^n$ we have $\omega_{gen}(S, U)$ is at most $\omega_{gen}(S, \mathbb{R}^n)$. □

)LLARY 3.11. *Let $f_1, \ldots, f_d \in \mathbb{R}[X_1, \ldots, X_n]$ be a collection of polyno-*
such that the ideal $\mathcal{I} = (f_1, \ldots, f_d)$ is real and of height d. Then, the
ing inequality holds:

$$d \leq \omega_{gen}(\{f_1 \geq 0, \ldots, f_d \geq 0\}, \mathbb{R}^n).$$

ie proof follows from the observation that $\mathcal{I}$ is a real complete intersection
here must exist a simple point $\alpha \in \mathbb{R}^n$ of the algebraic set described
e equations $\{f_1 = 0, \ldots, f_d = 0\}$. This point is a d-corner point of
$0, \ldots, f_d \geq 0\}$ and Theorem 3.8 applies.

4. Applications of the Generic Width

We have mentioned previously that the main Theorem in [10] can not be immediately applied to obtain lower bounds of decisional complexity as done by Rabin. Actually, Theorem 3.8 and its corollaries are very useful in this sense because of the following Proposition.

PROPOSITION 4.1. *Let W be a semialgebraic subset of $\mathbb{R}^n$. Then,*

$$\omega_{gen}^{\mathcal{N}}(W, \mathbb{R}^n) \leq \omega_{gen}(W, \mathbb{R}^n) \leq C_D(W).$$

PROOF. Let T be an ACT solving the membership problem for W. Let $\Gamma_1, \ldots, \Gamma_r$ be the oriented paths in T from the root to some leaf, ending at an affirmative label (i.e., paths followed by inputs belonging to W).

We have $W = W(T) = \bigcup_{i=1}^{r} W(\Gamma_i)$, where $W(\Gamma_i)$ is the semialgebraic set given by the sequence of polynomial sign conditions occuring in Γ_i. After a renumbering, let $r' \leq r$ be such that there is no equation among the sign conditions describing $W(\Gamma_i)$ if and only if $i \leq r'$. Let W' be the semialgebraic set given as $W' = \bigcup_{j=1}^{r'} W(\Gamma_j)$. Clearly, W' is generically equal to W in $\mathbb{R}^n$.

Let $W''(\Gamma_j)$ be the closed semialgebraic set obtained after replacing the strict sign conditions occuring in Γ_j, "> 0", by the relaxed sign conditions "≥ 0". Then, let W'' be the union of those $W''(\Gamma_j)$. The proof is complete once one observes that the following conditions hold:

i) W'' is generically equal to W in $\mathbb{R}^n$ and thus $\omega_{gen}(W, \mathbb{R}^n) \leq \omega(W'', \mathbb{R}^n)$,

ii) $\omega(W'', \mathbb{R}^n) \leq h_D(T)$. □

4.1. Finite polynomial optimization. Problems 1.1 to 1.3 of the Introduction are particular cases of finite polynomial maximization and minimization. Now, we observe that our analyses in Section 3 and Proposition 4.1 provide linear lower bounds for all of them regardless of the fixed, non-constant polynomial $f \in \mathbb{R}[X_1, \ldots, X_n]$.

COROLLARY 4.2. *Both problems, finite maximization and finite minimization, have complexity at least $\Omega(N) = \Omega(\#(\mathcal{F}))$.*

PROOF. We do the proof only for maximization. First of all, note that lower bounds for the complexity of maximization can be immediately obtained from lower bounds of the following problem.

an affirmative answer. Observe that the subsets accepted by some ACT he class of semialgebraic sets coincide. As in algebraic complexity theory, tal complexity of a semialgebraic set W is defined as the minimum height ACT accepting W (see [1], [9], [14], or [15]).

order to deal with the problems stated in Section 1, [10] introduces a r measure of the complexity that takes arithmetic operations for free.

NITION 2.1. *Let T be an algebraic computation tree and W a semialge- subset of $\mathbb{R}^n$.*

The decisional height of a path Γ from the root to some leaf in T, $h_D(\Gamma)$, is the number of branching nodes occuring in Γ.

Likewise, the decisional height of T, $h_D(T)$, is the maximum of all the decisional heights of all paths Γ in T.

The decisional complexity of W, $C_D(W)$, is the minimum decisional height of all ACT's solving the membership problem for W.

OSITION 2.2. *The decisional complexity of any semialgebraic set of di- on d can be bounded by an effective function of d.*

F. Given a semialgebraic set W of dimension d it can be decomposed union of a semialgebraic set which is open in the Zariski closure of is a semialgebraic set of strictly smaller dimension. Now, every open gebraic set in an algebraic set of dimension d can be written using at $s(d) \times t(d)$ polynomials, where $s(d)$ and $t(d)$ are the upper bounds of the r invariants (see [5] and [6]), and are some effective functions of d. In (d) is defined as the minimum number of polynomial strict inequalities) needed to represent an open basic semialgebraic set in an algebraic set limension d. In the same way, $t(d)$ is the minimum number of unions of losed semialgebraic sets needed to represent an open semialgebraic set lgebraic set V of dimension d. Bröcker's work shows that these bounds l only on the dimension d and not on the particular algebraic variety one considers the semialgebraic sets. More concretely, it is shown in [5] (d) equals d and

$$t(d) \leq t(d-1) + \binom{4^{d-1}}{2 \cdot 4^{d-2} - 2^{d-2}}.$$

ore the decisional complexity of this open set is at most $s(d) \times t(d) + 1$: ay construct an ACT that tests, using just one branching node, the

membership in the Zariski closure of W, and then concatenate the $s(d) \times t(d)$ polynomials to test membership in the open set. Since the zero dimensional case involves only decisional height one, we use induction on the dimension of the semialgebraic set W to complete the proof. □

REMARK 2.3. *The decisional complexity is clearly a lower bound for the total complexity of any semialgebraic set (counting also the number of involved arithmetic operations, as in [1] and [9]). But Proposition 2.2 above shows that decisional complexity fails in most cases to approximate total complexity; in fact, one can exhibit semialgebraic sets in $\mathbb{R}^n$ of arbitrarily high total complexity while the decisional complexity is always bounded by a function of $d \leq n$. For example, an algebraic subset of $\mathbb{R}$ always has decisional complexity one, but the total complexity depends on the number of its components. Another example is that of regular polygons in $\mathbb{R}^2$ having decisional complexity two, regardless of the number of vertices—which determines the total complexity (see [9]). Notice that every regular polygon Q in $\mathbb{R}^2$ is given as $Q = \{(x,y) \in \mathbb{R}^2 : P(x,y) \geq 0, Q(x,y) \geq 0\}$, where $P(X,Y)$ is the equation of the circle passing through all the vertices of Q, while $Q(X,Y)$ is the polynomial given as the product of the equations of all lines passing through the sides of the polygon Q. This behavior can explain in precise terms the comment of Ben-Or in [1] about the failure of the methods of Rabin and Jaromczyk, using algebraic decision trees, to give non-linear lower bounds for some problems.*

We can observe that the decisional complexity is not necessarily a lower bound in terms of the input size. For instance, in [1] Ben-Or analyzed lower bounds for the total complexity of the following problem.

ELEMENT DISTINCTNESS PROBLEM. *Given $x_1, \ldots, x_N \in \mathbb{R}$, is there a pair i,j with $i \neq j$ and $x_i = x_j$?*

A $\Omega(N log_2 N)$ lower bound for the total complexity of this problem is given in [1]. However, the decisional complexity of ELEMENT DISTINCTNESS is clearly 1.

3. Generic Width of a Semialgebraic Set

Nevertheless, the decisional complexity provides a useful lower bound for some other problems (where topological methods as in [1] and [9] fail), when combined with the analysis of the concept of width according to the following definition: denote by $SP(X)$ the formula given by the conjunction

$$L_1(X) \geq 0 \wedge \cdots \wedge L_m(X) \geq 0$$

this last set is closed and $g(\alpha_k) = x_{km}^r \cdot h(\alpha_k) \neq 0$, then

$$\alpha \in \bigcup_{j=1}^{t} \{x \in U : q_{1,j}(x) \geq 0, \ldots, q_{m-1,j}(x) \geq 0\} \setminus \{x \in U : g(x) = 0\},$$

h gives the inclusion. □

ow, for every $1 \leq j \leq t$, reordering the indices i if necessary, define $s(j)$ that $r_{i,j} = 0$ if and only if $i \leq s(j)$. We have the following cases.

If $s(j) = m-1$ then the set

$$\{x \in U : x_m \geq 0, q'_{1,j}(x) \geq 0, \ldots, q'_{m-1,j}(x) \geq 0\} \setminus \{\pi(x) = 0\}$$

has no common point with the hyperplane $\{x \in \mathbb{R}^n : x_m = 0\}$ since otherwise, by continuity, there would be a point x in Δ_m with m–coordinate $x_m < 0$.

If $s(j) = m-2$ the condition $q'_{m-1,j} \geq 0$ always holds over the set of points $\{x \in U : x_m = 0, q'_{1,j}(x) \geq 0, \ldots, q'_{m-2,j}(x) \geq 0\} \setminus \{x \in U : \pi(x) = 0\}$ since otherwise, by continuity, there would be a point $x \in \{x \in U : q_{1,j}(x) > 0, \ldots, q_{m-2,j}(x) > 0, q'_{m-1,j}(x) < 0\} \setminus \{x \in U : \pi(x) = 0\}$ with m–coordinate $x_m < 0$. Since $q_{m-1,j}(x) = x_m \cdot q'_{m-1,j}(x) > 0$ and $g(x) = x_m^r \cdot h(x) \neq 0$, by equality (3.7.1) this point would be in Δ_m.

Finally, if $0 \leq s(j) < m-2$, let us define the following Nash functions

$$Q_{i,j} = \begin{cases} q'_{i,j} & \text{if } 1 \leq i \leq s(j), \\ q'_{s(j)+1,j} q'_{i,j} & \text{if } s(j)+2 \leq i \leq m-1. \end{cases}$$

Then, we have the following set equality:

$$\begin{aligned} \{x \in U : \ & x_m = 0, q'_{1,j}(x) \geq 0, \ldots, q'_{m-1,j}(x) \geq 0, \pi(x) \neq 0\} = \\ \{x \in U : \ & x_m = 0, q'_{1,j}(x) \geq 0, \ldots, q'_{s(j),j}(x) \geq 0, \\ & Q_{s(j)+2,j}(x) \geq 0, \ldots, Q_{m-1,j}(x) \geq 0, \pi(x) \neq 0\}. \end{aligned}$$

Otherwise, there would be a point $x \in U$ satisfying the system of equations and inequalities

$$x_m = 0, q'_{1,j}(x) \geq 0, \ldots, q'_{s(j),j}(x) \geq 0,$$
$$q'_{s(j)+1,j} \cdot q'_{s(j)+2,j}(x) \geq 0, \ldots, q'_{s(j)+1,j} \cdot q'_{m-1,j}(x) \geq 0, \pi(x) \neq 0,$$

so that $q'_{i,j}(x) < 0$ for some i, $s(j)+1 \leq i \leq m-1$. This would imply that $q'_{i,j}(x) < 0$ for every $s(j)+1 \leq i \leq m-1$. Now, by continuity, one can choose a point y satisfying the following system:

$$y_m < 0, q'_{1,j}(y) > 0, \ldots, q'_{s(j),j}(y) > 0,$$
$$q'_{s(j)+1,j}(y) < 0, \ldots, q'_{m-1,j}(y) < 0, \pi(y) \neq 0.$$

Now, observe that we have $q_{i,j}(y) = y_m \cdot q'_{i,j}(y) > 0$ for $s(j)+1 \leq i \leq m-1$. On the other hand, for $1 \leq i \leq s(j)$, $q'_{i,j}(y) = q_{i,j}(y) > 0$ and $g(y) = y_m^r \cdot h(y) \neq 0$. Finally, by equality (3.7.1), this point y would be in Δ_m and we would arrive to a contradiction since $y_m < 0$.

Identifying $\mathbb{R}^{n-1}$ with the linear hyperplane $\{x \in \mathbb{R}^n : x_m = 0\}$, it follows from 1 to 3 above that the Nash generic width of Δ_{m-1} in $\mathbb{R}^{n-1}$ is at most $m-2$, which contradicts the induction hypothesis; thus, the proof of Proposition 3.7 is complete. □

From the classical literature, we define *Nash m–corner points* (see for instance [13], p. 15) in semialgebraic sets $W \subseteq \mathbb{R}^n$ as those points $\alpha \in W$ such that there is a Nash diffeomorphism of a neighborhood U of α onto a neighborhood U' of the origin, such that under this diffeomorphism $W \cap U$ looks like $\{x_1 \geq 0, \ldots, x_m \geq 0\}$.

THEOREM 3.8. *For a semialgebraic subset $W \subseteq \mathbb{R}^n$, if there is an m–corner point $\alpha \in W$, then $m \leq \omega_{gen}(W, \mathbb{R}^n)$.*

The proof follows in a straightforward manner from Proposition 3.7. The following corollaries deal with more concrete instances where the hypothesis of Theorem 3.8 holds.

COROLLARY 3.9. *Let $p_1(X), \ldots, p_m(X) \in \mathbb{R}[X_1, \ldots, X_n]$ be a collection of polynomials, and let α be a point in $\mathbb{R}^n$ such that $p_1(\alpha) = 0, \ldots, p_m(\alpha) = 0$ and the rank of the Jacobian matrix defined by $p_1(X), \ldots, p_m(X)$ at α is m, i.e., rank $J(p_1, \ldots, p_m)_\alpha = m$. Then,*

$$\omega_{gen}^{\mathcal{N}}(\{x \in \mathbb{R}^n : p_1(x) \geq 0, \ldots, p_m(x) \geq 0\}, U) = m$$

for every open neighborhood U of α in $\mathbb{R}^n$.

PROOF. The hypothesis means that $\{p_1, \ldots, p_m\}$ is a subset of a regular system of parameters near α. Thus, using the local (Nash) coordinates of the Implicit Function Theorem for Nash functions (see [3]) we can identify W, near α, with an m–corner, and the Corollary is then a consequence of Theorem 3.8. □

e conclude that $C \subseteq \{(x,y) \in \mathbb{R}^2 : \prod_{i=1}^t P_i(x,y) = 0\}$ and $X^3 - X^2 - Y^2$ s $\prod_{i=1}^t P_i(X,Y)$. Then, since $X^3 - X^2 - Y^2$ is irreducible, $X^3 - X^2 - Y^2$ s $P_i(X,Y)$ for some i, which finally implies $P_i(0,0) = 0$, $(0,0) \in W$, and ve arrived at a contradiction.

n the other hand, it is easy to find examples where the last two values in equality of (3.6.1) differ. For instance, consider the semialgebraic subset $\mathbb{R}^3$ given by

$$S = \{(x,y,z) \in \mathbb{R}^3 : x \geq 0, y \geq 0, -z^2 \geq 0\}.$$

Proposition 3.7 below, we can prove that $\omega(S, \mathbb{R}^3) = 2$, but $-1 \geq 0$ is a lete proof of S relative to $Z \in \mathbb{R}[X,Y,Z]$.

OSITION 3.7. *For every open semialgebraic neighborhood $U \subseteq \mathbb{R}^n$ of the $0 \in \mathbb{R}^n$, we have*

$$\omega_{gen}^{\mathcal{N}}(\{x \in \mathbb{R}^n : x_1 \geq 0, \ldots, x_m \geq 0\}, U) = m.$$

F. We show that for every open semialgebraic neighborhood U of the $0 \in \mathbb{R}^n$, there are no Nash functions g, $q_{i,j} \in \mathcal{N}(U) \setminus \{0\}$ such that the ing equality holds.

$$\in U : x_1 \geq 0, \ldots, x_m \geq 0\} \setminus \{x \in U : g(x) = 0\}$$
$$\bigcup_{j=1}^t \{x \in U : q_{1,j}(x) \geq 0, \ldots, q_{m-1,j}(x) \geq 0\} \setminus \{x \in U : g(x) = 0\} \quad (3.7.1)$$

may assume that U is an open ball centered at the origin and proceed luction on m $(\leq n)$. The case $m = 1$ follows from the observation $x \in U : x_1 < 0\}$ is a non-empty open semialgebraic set, hence the gebraic set $\{x \in U : x_1 \geq 0\}$ can be generically equal neither to $\mathbb{R}^n$ nor empty set.

ppose that the induction hypothesis is true for $m-1$ and suppose that are Nash functions g, $q_{i,j} \in \mathcal{N}(U) \setminus \{0\}$ such that the equality (3.7.1) The strategy we follow in this inductive step will be to get from the ty (3.7.1) a description of $\{x_1 \geq 0, \ldots, x_{m-1} \geq 0\}$ as a subset of $\mathbb{R}^{n-1}$ Nash generic width at most $m-2$. The rest of the proof shows the lure that generates this description.

te that if $f, h \in \mathcal{N}(U) \setminus \{0\}$, the semialgebraic set $\{x \in U : q^2 \cdot h(x) \geq 0\}$ rically equal to the semialgebraic set $\{x \in U : h(x) \geq 0\}$. Then, without generality, we can assume that the factorizations in $\mathcal{N}(U)$ of the Nash

functions g and $q_{i,j}$ occuring in the equality (3.7.1) are square free. Now, for each pair of indices (i,j) there is an $r_{i,j} \in \{0,1\}$ such that $q_{i,j} = x_m^{r_{i,j}} \cdot q'_{i,j}$ and $q'_{i,j}$ is not in the ideal $(x_m)\mathcal{N}(U)$. In the same way, there is an $r \in \{0,1\}$ such that $g = x_m^r \cdot h$ and $h \notin (x_m)\mathcal{N}(U)$. Let B be the subset of U given by

$$B = \bigcup_{j=1}^t \{x \in U : x_m \geq 0, \ \ q'_{1,j}(x) \geq 0, \ldots, q'_{m-1,j}(x) \geq 0\}$$

and let π be the Nash function $\pi = h \prod_{i,j} q'_{i,j}$. For simplicity, let us write $\Delta_m = \{x \in U : x_1 \geq 0, \ldots, x_m \geq 0\}$.

CLAIM. *Under the above notation, the following equality holds:*

$$\Delta_m \setminus \{x \in U : \pi(x) = 0\} = B \setminus \{x \in U : \pi(x) = 0\}.$$

PROOF. For the first inclusion, let us consider a point α in the semialgebraic set $\Delta_m \setminus \{x \in U : \pi(x) = 0\}$. Note that it is the limit of a sequence of points $\{\alpha_k = (x_{k1}, \ldots, x_{kn})\}_{k \in \mathbb{N}}$ contained in $\Delta_m \setminus \{x \in U : \pi(x) = 0\}$ such that for every $k \in \mathbb{N}$, x_{km} is strictly positive. Then, $g(\alpha_k) = x_{km}^r \cdot h(\alpha_k) \neq 0$ and from the equality (3.7.1) we conclude that

$$\{\alpha_k\}_{k \in \mathbb{N}} \subseteq \bigcup_{j=1}^t \{x \in U : \ q_{1,j}(x) \geq 0, \ldots, q_{m-1,j}(x) \geq 0\} \setminus \{x \in U : g(x) = 0\}.$$

Since $x_{km} > 0$, if $\alpha_k \in \{x \in U : q_{1,j}(x) \geq 0, \ldots, q_{m-1,j}(x) \geq 0\}$, we conclude that $q'_{i,j}(\alpha_k) \geq 0$ for $1 \leq i \leq m-1$. This implies that

$$\alpha_k \in \{x \in U : x_m \geq 0, q'_{1,j}(x) \geq 0, \ldots, q'_{m-1,j}(x) \geq 0\}.$$

Hence, $\{\alpha_k\}_{k \in \mathbb{N}} \subseteq B$ and, taking the limit of the sequence, the inclusion follows.

As for the converse, assume an element $\alpha = (x_1, \ldots, x_m, x_{m+1}, \ldots, x_n)$ in $B \setminus \{\pi(x) = 0\}$ to be given. There must be a j, $1 \leq j \leq t$, such that

$$\alpha \in \{x \in U : x_m \geq 0, q'_{1,j}(x) \geq 0, \ldots, q'_{m-1,j}(x) \geq 0\} \setminus \{x \in U : \pi(x) = 0\}$$

and α is the limit of a sequence of points $\{\alpha_k = (x_{k1}, \ldots, x_{kn})\}_{k \in \mathbb{N}}$ contained in the open set

$$\{x \in U : x_m > 0, q'_{1,j}(x) > 0, \ldots, q'_{m-1,j}(x) > 0\} \setminus \{x \in U : \pi(x) = 0\}.$$

Then, $q_{i,j}(\alpha_k) = x_{mk}^{r_{i,j}} \cdot q'_{i,j}(\alpha_k) \geq 0$ and

$$\{\alpha_k\}_{k \in \mathbb{N}} \subseteq \bigcup_{j=1}^t \{x \in U : \ q_{1,j}(x) \geq 0, \ldots, q_{m-1,j}(x) \geq 0\}.$$

when the Zariski closure of F is irreducible, that there is a polynomial $q \in \mathbb{R}[X_1, \dots, X_n]$, non-identically zero on F, such that

$$W \cap F \setminus \{x \in F : q(x) = 0\} = W' \cap F \setminus \{x \in F : q(x) = 0\}.$$

The relation 'generically equal in F' is an equivalence relation.

While complete proofs relative to a non-zero polynomial are in fact complete proofs in non-trivial cases, the property of being "generically equal" does not mean "equal" in these cases. Consider for instance the closed semialgebraic sets $W_1 = \{(x,y) \in \mathbb{R}^2 : x \geq 0, y \geq 0\}$ and

$$W_2 = \{(x,y) \in \mathbb{R}^2 : x \geq 0, y \geq 0\} \cup \{(x,y) \in \mathbb{R}^2 : -y^2 \geq 0\}.$$

Both sets are generically equal in $\mathbb{R}^2$ but are not equal.

If U is an open connected semialgebraic subset of $\mathbb{R}^n$, a proper Nash set is a semialgebraic subset of dimension smaller than the dimension of U. Two semialgebraic subsets of $\mathbb{R}^n$, W and W', are generically equal in U if and only if there is a Nash function $h \in \mathcal{N}(U)$, non-identically zero on U, such that $W \cap U \setminus \{x \in U : h(x) = 0\} = W' \cap U \setminus \{x \in U : h(x) = 0\}$.

ur analysis will combine the widths of open and closed sets generically to the given one. This improves the performance of the width as a lower l, but the computation of these generic widths requires a result stronger the Main Theorem in [10].

NITION 3.5. *Given two semialgebraic subsets W and F of $\mathbb{R}^n$, we define eneric width of W in F, $\omega_{gen}(W,F)$, as follows:*

$$\begin{aligned} {}_n(W,F) &= \min\{\omega(C,F) : C \text{ is closed, generically equal to } W \text{ in } F\} \\ &= \min\{\omega(O,F) : O \text{ is open, generically equal to } W \text{ in } F\}. \end{aligned}$$

nalogously, the Nash generic width of W in an open set U, $\omega^{\mathcal{N}}_{gen}(W,U)$, is ed by replacing "width" by "Nash width" in the equalities above. Obvi-, as polynomials are also Nash functions, we have

$$\omega^{\mathcal{N}}_{gen}(W,U) \leq \omega_{gen}(W,U) \leq n.$$

last inequality is from Bröcker's works [5] and [6].

REMARK 3.6. *Let us denote by $\varpi(W,\mathbb{R}^n)$ the minimum of the widths of any complete proof of W relative to some polynomial $Q(X)$. We observe that the parameters $\omega_{gen}(W,\mathbb{R}^n)$, $\varpi(W,\mathbb{R}^n)$ (used in [10]), and $\omega(W,\mathbb{R}^n)$ (used in [8]) are different. First, we have the obvious relation*

$$\omega_{gen}(W,\mathbb{R}^n) \leq \varpi(W,\mathbb{R}^n) \leq \omega(W,\mathbb{R}^n). \qquad (3.6.1)$$

Second, for semialgebraic subsets $W \subseteq \mathbb{R}^n$ whose interior points are dense, we have the following equality:

$$\varpi(W,\mathbb{R}^n) = \omega(W,\mathbb{R}^n).$$

However, both of them can be different from the generic width. Consider, for instance, examples of basic closed semialgebraic sets where the dimension falls beyond a smooth boundary. More concretely, consider the closed semialgebraic subset of $\mathbb{R}^2$ described by the cubic with an isolated point:

$$\begin{aligned} W &= \{(x,y) \in \mathbb{R}^2 : x^3 - x^2 - y^2 \geq 0, x - 1/2 \geq 0\} \\ &= \{(x,y) \in \mathbb{R}^2 : x^3 - x^2 - y^2 > 0\} \\ &\quad \cup \{(x,y) \in \mathbb{R}^2 : x^3 - x^2 - y^2 = 0, x \neq 0\}. \end{aligned}$$

It is clear that W is generically equal to the open semialgebraic set given by $\{(x,y) \in \mathbb{R}^2 : x^3 - x^2 - y^2 > 0\}$, thus $\omega_{gen}(W,\mathbb{R}^2) = 1$.

On the other hand, let $\mathcal{P}$ be a complete proof of W relative to a non-zero polynomial $Q(X,Y) \in \mathbb{R}[X,Y] \setminus \{0\}$. Since the interior points of W are dense, we have that $W(\mathcal{P}) = W$ and $\mathcal{P}$ is a complete proof of W. Now, we have the following inequality:

$$2 \leq \omega(W,\mathbb{R}^2).$$

Assume there are polynomials $P_1(X,Y), \dots, P_t(X,Y) \in \mathbb{R}[X,Y]$ such that

$$W = \{(x,y) \in \mathbb{R}^2 : P_1(x,y) \geq 0\} \cup \dots \cup \{(x,y) \in \mathbb{R}^2 : P_t(x,y) \geq 0\}.$$

The set $B = \{(x,y) \in \mathbb{R}^2 : x^3 - x^2 - y^2 = 0, x \neq 0\}$ is the set of regular points of the irreducible curve $C = \{(x,y) \in \mathbb{R}^2 : x^3 - x^2 - y^2 = 0\}$. Then, B is Zariski dense in C and the ideal of C is $(X^3 - X^2 - Y^2)$. Now, observe that B is the boundary of W which implies that no $P_i(X,Y)$ can be strictly positive on points of B. Since $B \subseteq W$, we must have the following inclusion:

$$B \subseteq \{P_1(x,y) = 0\} \cup \dots \cup \{P_t(x,y) = 0\} = \{(x,y) \in \mathbb{R}^2 : \prod_{i=1}^{t} P_i(x,y) = 0\}.$$

Now, following the arguments of Rabin we should be able to obtain a com-
e proof $\mathcal{P}$ of $\{x \in \mathbb{R} : x \geq 0\}$ relative to $Q(X) = X(X+1)f^2(X)$, just
‹ing some sign changes, but preserving the family of polynomials occuring in
ACT. However, note that a complete proof consists only of non-strict "≥ 0"
ı inequalities. Moreover, the semialgebraic set $W(\mathcal{P})$ must be included in
$\in \mathbb{R} : x \geq 0\}$ (see condition (i) of Definition 3.1 above). Nevertheless,
ᵓ uses only the polynomials $\{Xf^2(X), (X+1)f^2(X)\}$ and sign conditions
0", $W(\mathcal{P})$ contains all negative roots of $f(X)$, and it would never be posible
ıave the following inclusion:

$$W(\mathcal{P}) \subseteq \{x \in \mathbb{R} : x \geq 0\}.$$

Γhis difficulty can be avoided if we include some new polynomials. For
ance, consider including with the given family all the derivatives of these
·nomials as in Thom's Lemma (see [3], 2.5.4, and [7]), or consider adding
·parating polynomial $g(X)$, which is strictly negative on the roots of $f(X)$
positive on $\{x \in \mathbb{R} : x \geq 0\}$. With this bigger collection we can find a
ıplete proof of the given set.

Γhis example shows that obtaining a complete proof, even if it is relative to
ıe non–zero polynomial, is not simply a matter of sign changes but requires
ing some new polynomials to the family occuring in the given ACT.

Γhere are algorithmic procedures to get these new polynomials; this is the
ı behind all the known proofs of the Finiteness Theorem (see [3], [7], and
for details). Given a description (a formula or an ACT) of a semialgebraic
W known to be closed, we can construct from the given description a
ırating family of polynomials using Thom's Generalized Lemma as in [7]
[11]. This family is big enough to produce a complete proof of the set.
ʋever, the method is based on a cylindrical algebraic decomposition and it
ɔduces all the partial derivatives of all polynomials occuring in the tree.
ꜱ technique leads to complete proofs of width $O(2^h)$ where h is the height
ḷe tree.

Γhere is another method based on Lojasiewicz's inequality [3]. This method
ery accurate for open semialgebraic sets, but not so good for closed ones.
ıtroduces $O(N2^{h-1})$ new polynomials, where N is the number of NO leaves
h is the height of the tree. The complete proofs of closed sets obtained by
method also have width of order $O(N2^{h-1})$.

Γhese features lead to enormous changes on the complexity and we cannot
ıperate the height of the original tree as a linear function of the width of
obtained complete proof.

Nevertheless, we observe that the conclusion in [10] (i.e., that the width is

a lower bound for the decisional complexity) remains true in the example of Figure 1 above: $1 \leq h_D(T) = 2$ (see Corollary 4.6 below). In order to show how this relation holds, we proceed by slightly changing the concept of width, without explicitly using the procedures to construct complete proofs.

DEFINITION 3.2. *Let F, W be two semialgebraic subsets of $\mathbb{R}^n$, W closed. The width of W in F, $\omega(W,F)$, is the minimum non-negative integer $k \in \mathbb{N}$ such that there are an integer $t \in \mathbb{N}$ and polynomials $p_{i,j} \in \mathbb{R}[X_1, \ldots, X_n]$ for $1 \leq i \leq k$, $1 \leq j \leq t$, verifying*

$$W \cap F = \bigcup_{j=1}^{t} \{x \in F : p_{1,j}(x) \geq 0, \ldots, p_{k,j}(x) \geq 0\}. \tag{3.2.1}$$

By convention, we assume $\omega(\mathbb{R}^n, F) = 0$ and $\omega(\emptyset, F) = 0$.

Similarly, if W' is an open semialgebraic subset of $\mathbb{R}^n$, we define the concept of the width of W' in F by replacing "≥ 0" by "> 0" in the equality (3.2.1) above.

For technical reasons, we will work in the realm of Nash function theory throughout the remainder of this section: a Nash function defined on an open semialgebraic subset U of $\mathbb{R}^n$ is an analytic function $f : U \longrightarrow \mathbb{R}$ which is algebraic over the polynomials (see [3], Ch. 8, for more detailed descriptions). We shall denote by $\mathcal{N}(U)$ the ring of Nash functions defined on U. A Nash set in U is the zero set of a finite collection of Nash functions in $\mathcal{N}(U)$. An important property of Nash functions is that sets given by a Boolean formula of sign conditions on Nash functions defined on U are also semialgebraic subsets of $\mathbb{R}^n$. Another important property we shall apply below is that $\mathcal{N}(U)$ is a factorial domain whenever U is an open ball (see [4] and [12]).

Analogously to Definition 3.2 above, for an open semialgebraic subset U of $\mathbb{R}^n$ we define the *Nash width* of a closed (respectively open) semialgebraic subset W in F, $\omega^{\mathcal{N}}(W,U)$, by replacing the polynomials $p_{i,j}$ by Nash functions defined on U in equality (3.2.1) above.

DEFINITION 3.3. *Let W, W', F be three semialgebraic subsets of $\mathbb{R}^n$. We say that W and W' are* generically equal *in F if and only if* $\dim(W \bigtriangleup W') \cap F < \dim F$, *where $W \bigtriangleup W'$ is the symmetric difference of W and W'.*

REMARK 3.4. *i) Since the dimension of F as a semialgebraic set is the dimension of its Zariski closure, "W generically equal to W' in F" means,*

$L_j : \mathbb{R}^n \longrightarrow \mathbb{R}$ are affine linear functions for $1 \leq j \leq m$.

NITION 3.1. *([10]) Let $Q(X) = Q(X_1, \cdots, X_n)$ be a polynomial and F a x subset of $\mathbb{R}^n$. We say that the $t \times k$ array $\mathcal{P}$ of polynomials*

$$\mathcal{P} = \begin{pmatrix} p_{1,1}(X) & \dots & p_{1,k}(X) \\ \vdots & \ddots & \vdots \\ p_{t,1}(X) & \dots & p_{t,k}(X) \end{pmatrix}$$

omplete proof *in F of $SP(X)$, relative to $Q(X)$, if*

for every $1 \leq i \leq t$ and every $x_0 \in \mathbb{R}^n$,

$$[x_0 \in F \wedge 0 \leq p_{i,1}(x_0) \wedge \cdots \wedge 0 \leq p_{i,k}(x_0)] \Longrightarrow SP(x_0), \text{ and}$$

for every $x_0 \in F$ satisfying $SP(x_0)$ and $Q(x_0) \neq 0$, there exists an i, $1 \leq i \leq t$, such that

$$0 \leq p_{i,1}(x_0) \wedge \cdots \wedge 0 \leq p_{i,k}(x_0).$$

hermore, we define $Width(\mathcal{P}) = k$.

abin simply used the term *complete proof* of $SP(X)$ to refer to those lete proofs $\mathcal{P}$ relative to the constant polynomial $1 \in \mathbb{R}[X_1, \dots, X_n]$. ollowing the underlying ideas of [10], we can extend the concept of a com- proof of any closed semialgebraic subset $W \subseteq \mathbb{R}^n$ in the following manner. Ve can understand a complete proof $\mathcal{P}$ as a description, in matricial pre- ation, of a semialgebraic closed set $W(\mathcal{P}) \subseteq \mathbb{R}^n$, as in the Finiteness orem:

$$W(\mathcal{P}) = \bigcup_{i=1}^{t} \{x \in \mathbb{R}^n : p_{i,1}(x) \geq 0, \dots, p_{i,k}(x) \geq 0\}.$$

Ve shall say that one of such matrices, $\mathcal{P}$, is a complete proof of a semi- raic subset $W \subseteq \mathbb{R}^n$ relative to $Q(X)$ when the following two conditions :

$W(\mathcal{P}) \subseteq W$,

$W \setminus \{x \in \mathbb{R}^n : Q(x) \neq 0\} \subseteq W(\mathcal{P}) \setminus \{x \in \mathbb{R}^n : Q(x) \neq 0\}$.

When $F = \mathbb{R}^n$, complete proofs relative to $Q(X)$ of the syntactic expression $SP(X)$ (as in Definition 3.1) are just complete proofs relative to $Q(X)$ of the following subset W of $\mathbb{R}^n$:

$$W = \{x \in \mathbb{R}^n : L_1(x) \geq 0, \dots, L_m(x) \geq 0\}.$$

Again, we simply use the term *complete proofs of a semialgebraic subset* $W \subseteq \mathbb{R}^n$ to refer to those complete proofs relative to the constant polynomial 1, i.e., $\mathcal{P}$ is a complete proof of W if and only if $W = W(\mathcal{P})$.

In [10], Proposition 6, Rabin states that for all those non–trivial $SP(X)$ (i.e., those with non-empty interior) the clause "relative to $Q(X)$ " can always be dropped. In our terminology this result can be translated as follows. Given a closed semialgebraic set $W \subseteq \mathbb{R}^n$ whose interior points are dense in W, for every complete proof $\mathcal{P}$ of W relative to a non-zero $Q(X)$, we have $W(\mathcal{P}) = W$, i.e., $\mathcal{P}$ is in fact a complete proof of W and the clause "relative to $Q(X)$" can also be dropped. The proof follows the same arguments as Proposition 6 in [10].

In [10], Rabin claimed that "after certain sign changes" in an ACT solving the membership problem for a set $\{x \in \mathbb{R}^n : L_1(x) \geq 0, \dots, L_m(x) \geq 0\}$, one can obtain a complete proof of that set. This assertion is not clear for the authors. Take the semialgebraic subset $\{x \in \mathbb{R} : x \geq 0\}$ of $\mathbb{R}$ and a polynomial $f(X) \in \mathbb{R}[X]$ with only negative roots, say $f(X) = X + 2$. In Figure 1 below, we exhibit an ACT, T, solving the membership problem for $\{x \in \mathbb{R} : x \geq 0\}$ in $\mathbb{R}$.

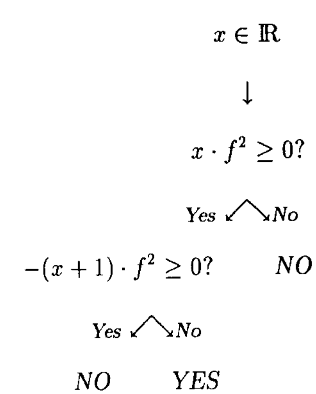

Figure 1: An algebraic decision tree that does not produce a complete proof.

ɔOF. The first statement is clear from our discussions in Section 3. As he second statement, observe that given affine linear functions $L_1, \ldots, L_m$: $\longrightarrow \mathbb{R}$, the L_i's are sign independent if and only if the rank of the Jacobian ıed by $\{L_1, \ldots, L_m\}$ at some point $\alpha \in \mathbb{R}^n$, verifying $L_1(\alpha) = 0, \ldots,$ $\alpha) = 0$, is m. Then, Theorem 3.8 and Proposition 4.1 allow us to conclude $\omega_{gen}(W, \mathbb{R}^n) = \omega(W, \mathbb{R}^n) = m = C_D(W)$.
)n the other hand, Theorem 3.8 and Remark 3.6 yield the main Theorem 0], i.e., $m = \omega_{gen}(W, \mathbb{R}^n) \leq \varpi(W, \mathbb{R}^n) \leq m = C_D(W)$, which completes proof. □

ıARK 4.8. *The statement of Corollary 4.6 does not hold under the weaker othesis of sign independence on the polynomials* $p_1, \ldots, p_m$ *if they are not ır forms: consider in* $\mathbb{R}^2$ *the linear functions* $L_1 = X_1$, $L_2 = X_2$, $L_3 =$ $- X_1$ *and* $L_4 = X_1 + X_2$ *and the polynomial mappings* $p_1 = L_1L_2$ *and* L_3L_4. *Clearly, the polynomial mappings* p_1 *and* p_2 *are sign independent ny open semialgebraic neighborhood* $U \subseteq \mathbb{R}^2$ *of the origin* $0 \in \mathbb{R}^2$, *but* $\geq 0, p_2 \geq 0\} = \{L_2L_3 \geq 0\}$.
)n the other hand, sign independence for conditions in $\{>, <\}$ *is a necessary lition for Corollary 4.6 to hold. Actually, if for some sequence* $\mu_1, \ldots, \mu_m \in$ $>\}$ *the set* $\{x \in U : p_1(x)\mu_1 0, ldots, p_m(x)\mu_m 0\} = \emptyset$, *then* $w_{gen}(\{x \in U :$ $)\mu_1 0, \ldots, p_m(x)\mu_m 0\}, U) \leq m - 1$. *In order to see this, let us suppose that* $\cdots = \mu_l =$ "$>$" *and* $\mu_{l+1} = \cdots = \mu_m =$ "$<$"; *then, the following equality s:*

$$\{x \in U : \ p_1(x) \geq 0, \ldots, p_m(x) \geq 0\} \setminus \{x \in U : \Pi_{i=1}^m p_i(x) = 0\} =$$
$$\{x \in U : \ p_1(x) \geq 0, \ldots, p_l(x) \geq 0, p_{l+1} \cdot p_{l+2}(x) \geq 0,$$
$$\ldots, p_{l+1} \cdot p_m(x) \geq 0\} \setminus \{x \in U : \Pi_{i=1}^m p_i(x) = 0\}.$$

Acknowledgements

authors are partially supported by DGICyT PB 92/0498 and "POSSO", RIT-BRA 6846.

References

M. BEN-OR, Lower bounds for algebraic computation trees. In *Proc. Fifteenth Ann. ACM Symp. Theor. Comput.*, 1983, 80–86.

R. BENEDETTI AND J. J. RISLER, *Real algebraic and semialgebraic geometry.* Hermann, Paris, 1990.

[3] J. BOCHNAK, M. COSTE AND M.-F. ROY, *Géométrie algébrique réelle.* Ergebnisse der Math., 3.Folge, Band **12**, Springer–Verlag, Berlin, Heidelberg, New York, 1987.

[4] J. BOCHNAK, Sur la factorialité des anneaux de fonctions de Nash. *Comment. Math. Helv.* **52** (1977), 211–218.

[5] L. BRÖCKER, Minimale Erzeugung von Positivbereich. *Geom. Dedicata* **16** (1984), 335–350.

[6] L. BRÖCKER, Spaces of orderings and semialgebraic sets. In *Quadratic and Hermitian Forms, CMS Conf. Proc.* **4**, Providence, Amer. Math. Soc. (1984), 231–248.

[7] M. COSTE, Ensembles Semi-algébriques. In *Géométrie Algébrique Réelle et Formes Quadratiques*, ed. J. L. COLLIOT-THÉLENE, M. COSTE, L. MAHÉ, AND M.-F. ROY. Lecture Notes in Mathematics **959**, Springer–Verlag, Berlin, Heidelberg, New York, 1982, 109–139.

[8] J. JAROMCZYK, An extension of Rabin's complete proof concept. In *Math. Found. of Comp. Sci. 1981*, ed. J. GRUSKA AND M. CHYTILL. Lecture Notes in Computer Science **118**, Springer–Verlag, Berlin, Heidelberg, New York, 1981, 321–326.

[9] J. L. MONTAÑA, L. M. PARDO AND T. RECIO, The non-scalar model of complexity in computational geometry. In *Proc. MEGA'90*, ed. C. TRAVERSO AND T. MORA. Progress in Mathematics **94**, Birkhäuser Boston, 1991, 347–362.

[10] M. O. RABIN, Proving simultaneous positivity of linear forms. *J. Comput. System Sci.* **6** (1972), 639–650.

[11] T. RECIO, Una Descomposición de un Conjunto Semialgebraico. In *Actas del* **V** *Congreso de la Agrupación de Matemáticos de Expresión Latina*, CSIC, Publicaciones del Instituto Jorge Juan, Madrid, 1978, 217–221.

[12] J. J. RISLER, Sur l'anneau des fonctions de Nash globales. *Ann. Scien. Ecole Norm. Sup.*, $4^{\text{éme}}$ *série*, **8** (1975), 365–378.

[13] J.T. SCHWARTZ, *Differential Geometry and Topology.* Notes on Mathematics and its Applications, Gordon and Breach, 1968.

[14] V. STRASSEN, Algebraic Complexity Theory. In *Handbook of Theoretical Computer Science*, ed. J. VAN LEEUWEN. Elsevier, Amsterdam, 1990, 633–673.

[15] F.F. YAO, Computational Geometry. In *Handbook of Theoretical Computer Science*, ed. J. VAN LEEUWEN. Elsevier, Amsterdam, 1990, 343–391.

Manuscript received 2 January 1992

José L. Montaña
Dept. de Matemáticas, Est. y Comp.
Facultad de Ciencias
Universidad de Cantabria
Santander, 39071 SPAIN
montana1@ccucvx.unican.es

Luis M. Pardo
Dept. de Matemáticas, Est. y Comp.
Facultad de Ciencias
Universidad de Cantabria
Santander, 39071 SPAIN
pardo@ccucvx.unican.es

Tomás Recio
Dept. de Matemáticas, Est. y Comp.
Facultad de Ciencias
Universidad de Cantabria
Santander, 39071 SPAIN
recio@ccucvx.unican.es