JOURNAL OF COMPLEXITY 8, 203–215 (1992)

Test Complexity of Generic Polynomials

PETER BÜRGISSER AND THOMAS LICKTEIG

Institut für Informatik V, Universität Bonn, Römerstrasse 164, D-5300 Bonn, Germany

AND

MICHAEL SHUB

IBM Thomas J. Watson Research Center, Department of Mathematical Sciences, P.O. Box 218, Yorktown Heights, New York 10598

Received July 3, 1991

We investigate the complexity of algebraic decision trees deciding membership in a hypersurface $X \subset \mathbf{C}^m$. We prove an optimal lower bound on the number of additions, subtractions, and comparisons and an asymptotically optimal lower bound on the number of multiplications, divisions, and comparisons that are needed to decide membership in a generic hypersurface $X \subset \mathbf{C}^m$. Over the reals, where in addition to equality branching also $\leq$-branching is allowed, we prove an analogous statement for irreducible "generic" hypersurfaces $X \subset \mathbf{R}^m$. In the case $m = 1$ we give also a lower bound for finite subsets $X \subset \mathbf{R}$.

1. INTRODUCTION

Given a polynomial f: $\mathbf{C}^m \to \mathbf{C}$ we may check whether $f(\xi) = 0$ by evaluating f at ξ. But testing for zero may be easier than evaluating. We show in this paper that this is not the case if f is sufficiently general.

The complexity of evaluating polynomials has been extensively studied in the last decades, starting with Ostrowski, Motzkin, Belaga, Pan, Winograd, and Strassen. (See Borodin and Munro, 1975, von zur Gathen, 1988, and Strassen, 1984, 1990, for a review of this work.) Recently, interest has begun to focus on the complexity of testing for zero. Strassen (1981) contains a lower bound on decision complexity in terms of the degree of an algebraic set. (For an application see Schuster, 1980.) Ben-Or (1983) proves lower bounds on the decision complexity of semialgebraic sets in

0885-064X/92 $5.00

terms of the number of connected components, generalizing previous results by Dobkin and Lipton (1978) and Steele and Yao (1982). In turn Yao (1989) extends these results back to the discrete setting. Recio and Pardo (1987) give lower bounds based on the width of a semialgebraic set continuing work by Rabin (1972) and Jaromczyk (1981). Montaña, Pardo, and Recio (1990) replace the number of connected components by intersection numbers and improve Ben-Or (1983) in various cases of connected semialgebraic sets. In Lickteig (1990) lower bounds on decision complexity are proved via differential methods from algebraic complexity theory (Baur and Strassen, 1983; Strassen, 1973) and approximative complexity (see the references in Lickteig, 1990) which for instance allow lower bounds for various decision problems from linear algebra to be given in terms of the complexity of the two fundamental problems of solving a system of linear equations and matrix multiplication.

In this paper we investigate the decision complexity of a generic hypersurface $X \subset \mathbf{C}^m$ employing the dimension or transcendence degree bound. This technique for proving lower bounds on the complexity of rational functions was introduced by Motzkin (1955), Belaga (1961), Paterson and Stockmeyer (1971), Reingold and Stocks (1972), and later was improved by Baur and Rabin (1982). They show in particular that for a polynomial $f \in \mathbf{C}[x_1, \ldots, x_m]$ of degree d with algebraically independent coefficients over $\mathbf{Q}$ one has

$$L_+(f) \geq \binom{d+m}{m} - 1, \tag{1}$$

$$L_*(f) \geq \left[\binom{d+m}{m} - 1\right]/2, \tag{2}$$

where $L_+(f)$, $L_*(f)$ denote the additive, respectively the multiplicative complexity of f.

We briefly recall the definitions. We study straight line programs that compute rational functions in $\mathbf{C}(x_1, \ldots, x_m)$ from some input of the form $(\xi_1, \ldots, \xi_n; x_1, \ldots, x_m)$, where $\xi \in \mathbf{C}^n$, $n \in \mathbf{N}$, using operations from $\Omega := \mathbf{Q} \sqcup \{+, -, *, /\}$. Here $\mathbf{C}(x_1, \ldots, x_m)$ is considered as a $\mathbf{Q}$-algebra and $\lambda \in \mathbf{Q}$ stands for scalar multiplication by λ. Allowing arbitrarily many constants $\xi_i \in \mathbf{C}$ is sometimes referred to as "coefficient preparation." The minimum number of nonscalar multiplications and divisions sufficient to compute f by an Ω-straight line program from some input $(\xi_1, \ldots, \xi_n; x_1, \ldots, x_m)$ is called the *multiplicative complexity* $L_*(f)$. By counting only additions and subtractions we get the *additive complexity* $L_+(f)$. The bound in (1) is obviously sharp.

Let $X \subset \mathbf{C}^m$ be a hypersurface, $X = X_1 \cup \cdots \cup X_t$ its decomposition into irreducible components, and

$$X_i = Zeroset(f_i), \quad f_i \in \mathbf{C}[x_1, \ldots, x_m] \text{ irreducible},$$
$$\deg f_i = d_i \ (i = 1, \ldots, t).$$

(For definitions and results from classical algebraic geometry see, e.g., Shafarevich, 1974.) We call X **Q**-*generic of degree format* $(d_1, \ldots, d_t)$ if the polynomials $f_1, \ldots, f_t$ may be chosen such that all their coefficients are algebraically independent over **Q**. If T is an algebraic decision tree using the operation symbols in Ω, the relation symbol "=," and as constants a finite subset of **C** we denote by $C_{+,=}(T)$ the maximum number of additions, subtractions, and comparisons occuring in a path from the root to a leaf of T. By minimizing $C_{+,=}(T)$ over all such decision trees deciding membership in X we obtain the *additive branching decision complexity* $C_{+,=}(X)$ of X. The *multiplicative branching decision complexity* $C_{*,=}(X)$ is defined analogously.

Our main result is

THEOREM 1. *Let $X \subset \mathbf{C}^m$ be a* **Q**-*generic hypersurface of degree format $(d_1, \ldots, d_t) \in \mathbf{N}^t$. Then we have for the additive branching decision complexity $C_{+,=}(X)$ of X*

$$C_{+,=}(X) = \sum_{i=1}^{t} \left[\binom{d_i + m}{m} - 1 \right], \tag{3}$$

and the multiplicative branching decision complexity $C_{*,=}(X)$ of X satisfies

$$C_{+,=}(X) \geq \frac{1}{2} \sum_{i=1}^{t} \left[\binom{d_i + m}{m} - 1 \right]. \tag{4}$$

We further show that the lower bound in (4) is asymptotically sharp as $\min_{1 \leq i \leq t} d_i \to \infty$, keeping m, t fixed.

In the special case of zero-dimensional hypersurfaces we get

COROLLARY 1. *Let X be a finite subset of* **C** *with t elements that are algebraically independent over* **Q**. *Then*

$$C_{+,=}(X) = t,$$
$$t/2 \leq C_{*,=}(X) \leq t/2 + 3.$$

We compare this with the situation over the reals where we also allow $\leq$-comparisons to be performed. For a subset $X \subset \mathbf{R}^m$ the additive and multiplicative decision complexities $C_{+,\leq}(X)$ and $C_{*,\leq}(X)$ are defined in an obvious way.

THEOREM 2. *Let $X \subset \mathbf{R}^m$ be an irreducible hypersurface. Assume that*

$$X = Zeroset(f), \qquad f \in \mathbf{R}[x_1, \ldots, x_m] \text{ irreducible}, \qquad deg\, f = d$$

and that the coefficients of f are algebraically independent over $\mathbf{Q}$. Then

$$C_{+,\leq}(X) = \binom{d+m}{m} - 1, \tag{5}$$

$$C_{*,\leq}(X) \geq \left[\binom{d+m}{m} - 1\right]/2. \tag{6}$$

So for an *irreducible* "generic" hypersurface $X \subset \mathbf{R}^m$ the lower bounds (3), (4) remain valid for the complexities $C_{+,\leq}(X)$ and $C_{*,\leq}(X)$. However, if the hypersurface X has several irreducible components, the situation may drastically change. We demonstrate this fact in the case where X is zero-dimensional.

PROPOSITION 1. *For every finite subset $X \subset \mathbf{R}$ with t elements the following hold* ($\log = \log_2$):

$$\tfrac{1}{3}\sqrt{\log t} \leq C_{+,\leq}(X) \leq \lceil \log t \rceil + 1, \tag{7}$$

$$\log(t/3)/\log 6 \leq C_{*,\leq}(X) \leq \lceil \log t \rceil + 1. \tag{8}$$

If the elements of X are algebraically independent over $\mathbf{Q}$ we even have

$$\log t - \log\log(t+1) \leq C_{+,\leq}(X).$$

2. TRANSCENDENCE DEGREE BOUNDS

For $u_1, \ldots, u_r \in \mathbf{C}[x_1, \ldots, x_m]$ let us denote by $T(u_1, \ldots, u_r)$ the subfield of $\mathbf{C}$ generated by the coefficients of the polynomials u_i. The following lemma is based on the fact that prime factorization in $\mathbf{C}[x_1, \ldots, x_m]$ is unique up to scaling.

LEMMA 1. *Let $u_1, \ldots, u_r \in \mathbf{C}[x_1, \ldots, x_m]$ be polynomials different from zero. Then*

$$trdeg_{\mathbf{Q}} T(u_1 \cdots u_r) \geq trdeq_{\mathbf{Q}} T(u_1, \ldots, u_r) - (r-1).$$

Proof. By Kronecker's trick we may assume w.l.o.g. that $m = 1$ (replace $x_1, \ldots, x_m$ by $x_1, x_1^N, \ldots, x_1^{N^{m-1}}$ with $N > deg(u_1 \cdots u_r)$). Let $u_1, \ldots, u_r$ be monic. Using the fact that the splitting field of u_i is a

finite algebraic extension of $T(u_i)$ we see that

$$trdeg_{\mathbf{Q}} T(u_1 \cdot \cdot \cdot u_r) = trdeg_{\mathbf{Q}} T(u_1, \ldots, u_r).$$

Taking into account that for $\alpha_i \in \mathbf{C}$

$$trdeg_{\mathbf{Q}} T(u_i) \geq trdeg_{\mathbf{Q}} T(\alpha_i u_i) - 1$$

the lemma follows. ■

The proof of Theorem 1 rests on an observation in Lickteig (1990) stating that the bound (2) also holds when one is allowed to perform any $\mathbf{Q}$-rational operation of arity two at unit cost. So we not only focus on Ω-straight line programs computing a rational function $f \in \mathbf{F}(x_1, \ldots, x_m)$ but also consider straight line programs where a basic computation step is any $\mathbf{Q}$-rational operation of arity less than or equal to a given natural number a, i.e., given by a rational function in $\mathbf{Q}(t_1, \ldots, t_a)$. For $a \in \mathbf{N}$ we put $\Omega_{(a)} := \{\mathbf{Q}\text{-rational operations of arity} \leq a\}$. We define the *complexity* $L_{(a)}(f)$ *of* f *with respect to arity* a as the minimum number of nonlinear $\mathbf{Q}$-rational operations of arity less than or equal to a sufficient to compute f from some input of the form $(\xi_1, \ldots, \xi_n; x_1, \ldots, x_m)$ where $n \in \mathbf{N}$, $\xi_i \in \mathbf{C}$ by an $\Omega_{(a)}$-straight line program. (Compare Schnorr, 1981; Ben-Or, 1983; Lickteig, 1990.) Obviously

$$L_{(2)}(f) \leq L_*(f).$$

For example, a rational function $f = x_1^{e_1} x_2^{e_2} \cdot \cdot \cdot x_m^{e_m}$ $(e_i \in \mathbf{Z})$ can be computed from $(x_1, \ldots, x_m)$ with only $m - 1$ rational operations of arity ≤ 2, namely with operations of the form $(t_1, t_2) \longmapsto t_1^{\mu_1} t_2^{\mu_2}$ $(\mu_i \in \mathbf{Z})$, no matter how big the $|e_i|$ are. So

$$L_{(2)}(x_1^{e_1} x_2^{e_2} \cdot \cdot \cdot x_m^{e_m}) \leq m - 1.$$

The next theorem will be our main tool.

THEOREM 3. (*Motzkin*, 1955; *Belaga*, 1961; *Reingold and Stocks*, 1972; *Baur and Rabin*, 1982; *Lickteig*, 1990). *Let* $a \in \mathbf{N}$, $a \geq 1$, *and* $f \in \mathbf{C}(x_1, \ldots, x_m)$. *Then there exist* $\alpha, \tilde{\alpha} \in \mathbf{C}$, $u, \tilde{u} \in \mathbf{C}[x_1, \ldots, x_m]$, $v, \tilde{v} \in \mathbf{C}[x_1, \ldots, x_m] \backslash \{0\}$ *satisfying*

$$f = \tilde{\alpha} \frac{\tilde{u}}{\tilde{v}}, \qquad trdeg_{\mathbf{Q}} T(\tilde{u}, \tilde{v}) \leq L_+(f),$$

$$f = \alpha + \frac{u}{v}, \qquad trdeg_{\mathbf{Q}} T(u, v) \leq aL_{(a)}(f).$$

Proof. We prove the following statement by induction on s: If $\beta = (\beta_1, \ldots, \beta_s)$ is an Ω-straight line program with s instructions executable on the input $(\xi_1, \ldots, \xi_n; x_1, \ldots, x_m)$, $\xi \in \mathbf{C}^n$ with result sequence

$$(b_{-n-m+1}, \ldots, b_0, b_1, \ldots, b_s),$$

where $b_{-n-m+1} = \xi_1, \ldots, b_0 = x_m$, then there are

$$\tilde{u}_i, \tilde{v}_i \in \mathbf{C}[x_1, \ldots, x_m], \tilde{\alpha}_i \in \mathbf{C} \qquad (i = 1, \ldots, s)$$

satisfying the two conditions

$$b_i = \tilde{\alpha}_i \tilde{u}_i / \tilde{v}_i, \quad \tilde{v}_i \neq 0,$$

$$trdeg_{\mathbf{Q}} T(\tilde{u}_1, \ldots, \tilde{u}_s, \tilde{v}_1, \ldots, \tilde{v}_s) \leq |\{i \leq s : \beta_i \text{ instruction for an addition or subtraction}\}|.$$

Let us sketch the induction step "$s > 0$": If $\beta_s = (+; i, j)$ with $i, j < s$ then (w.l.o.g. $b_i \neq 0$)

$$b_s = b_i + b_j = \tilde{\alpha}_i (\tilde{u}_i \tilde{v}_j + \frac{\tilde{\alpha}_j}{\tilde{\alpha}_i} \tilde{u}_j \tilde{v}_i)/(\tilde{v}_i \tilde{v}_j);$$

if $\beta_s = (*; i, j)$ with $i, j < s$ then

$$b_s = b_i * b_j = (\tilde{\alpha}_i \tilde{\alpha}_j)(\tilde{u}_i \tilde{u}_j)/(\tilde{v}_i \tilde{v}_j).$$

In the case of the other operations one has analogous representations for b_s. From these the definition of $\tilde{\alpha}_s$, $\tilde{u}_s$, and $\tilde{v}_s$ is evident.

Analogously, Let $\beta = (\beta_1, \ldots, \beta_s)$ be an $\Omega_{(a)}$-straight line program. Assume that β is executable on some input of the form $(\xi_1, \ldots, \xi_n; x_1, \ldots, x_m)$ with $\xi \in \mathbf{C}^n$ and result sequence

$$(b_{-n-m+1}, \ldots, b_0, b_1, \ldots, b_s).$$

Then there are

$$u_i, v_i \in \mathbf{C}[x_1, \ldots, x_m], \alpha_i \in \mathbf{C} \qquad (i = 1, \ldots, s)$$

satisfying the two conditions

$$b_i = \alpha_i + u_i / v_i, \qquad v_i \neq 0,$$

$$trdeg_{\mathbf{Q}} T(u_1, \ldots, u_s, v_1, \ldots, v_s) \leq a|\{i \leq s : \beta_i \text{ instruction for a nonlinear } \mathbf{Q}\text{-rational operation}\}|.$$

The theorem is an immediate consequence of these statements. ∎

3. Proofs

In the following let $ord_p : \mathbf{C}(x_1, \ldots, x_m)^\times \to \mathbf{Z}$ denote the discrete valuation associated with an irreducible polynomial $p \in \mathbf{C}[x_1, \ldots, x_m]$, i.e., $f = p^{ord_p(f)} A/B$, where p does not divide A and B.

Proof of Theorem 1. Let $X \subset \mathbf{C}^m$ be a $\mathbf{Q}$-generic hypersurface of degree format $(d_1, \ldots, d_t) \in \mathbf{N}^t$. Then we may assume for the decomposition $X = X_1 \cup \cdots \cup X_t$ of X into irreducible components that

$$X_i = Zeroset(f_i), \qquad f_i \in \mathbf{C}[x_1, \ldots, x_m] \text{ irreducible},$$
$$deg\, f_i = d_i \ (i = 1, \ldots, t),$$

and the coefficients of $f_1, \ldots, f_t$ are algebraically independent over $\mathbf{Q}$.

For the upper bound we compute all the $f_i - f_i(0)$ with

$$\sum_{i=1}^{t} \left[\binom{d_i + m}{m} - 2 \right] \text{ additions}$$

and then compare them with $-f_i(0)$.

To prove the lower bounds assume T to be a tree deciding membership in X. We denote by π_i the typical path of X_i $(i = 1, \ldots, t)$ (i.e., the path taken by Zariski-almost all elements of X_i) and by π_0 the typical path of $\mathbf{C}^m$. The node where π_i and π_0 separate will be called ν_i. After permuting $X_1, \ldots, X_t$ we can assume that the sequence of nodes $(\nu_1, \ldots, \nu_t)$ is ordered according to the partial order $\prec$ defined by the tree T (predecessor relation), say

$$\nu_1 = \cdots = \nu_{t_1} \prec \nu_{t_1+1} = \cdots = \nu_{t_2} \prec \cdots \prec \nu_{t_{s-1}+1} = \cdots = \nu_t,$$

where $t_0 := 0 < t_1 < t_2 < \cdots < t_s = t$. By following the path π_0 up to the node ν_{t_i} $(i = 1, \ldots, s)$ we obtain rational functions $g_i^{(1)}, g_i^{(2)} \in \mathbf{C}(\underline{x})$ such that

$$g_i^{(1)} = g_i^{(2)}?$$

is tested at node ν_{t_i} and

$$L_+(g_1^{(1)}, g_1^{(2)}, \ldots, g_s^{(1)}, g_s^{(2)}) \leq C_{+,=}(T) - s,$$
$$L_*(g_1^{(1)}, g_1^{(2)}, \ldots, g_s^{(1)}, g_s^{(2)}) \leq C_{*,=}(T) - s.$$

The $g_i := g_i^{(1)} - g_i^{(2)}$ are obviously not zero. Furthermore, for every $i \in \{1, \ldots, s\}$ the rational function g_i is defined almost everywhere on $X_{t_{i-1}+1}, \ldots, X_t$ and, among these sets, vanishes exactly on $X_{t_{i-1}+1}, \ldots, X_{t_i}$. By the Nullstellensatz we have for all $i \in \{1, \ldots, s\}, j \in \{1, \ldots, t\}$,

$$ord_{f_j}(g_i) > 0 \qquad \text{if } t_{i-1} < j \leq t_i,$$
$$ord_{f_j}(g_i) = 0 \qquad \text{if } t_i < j.$$

The matrix $[ord_{f_j}(g_i)]_{i,j} \in \mathbf{Z}^{s \times t}$ is therefore a blockwise lower triangular matrix where the block diagonal entries are elementwise positive. Hence it is possible to choose $m_1, \ldots, m_s \in \mathbf{N}$ such that

$$\sum_{i=1}^{s} m_i ord_{f_j}(g_i) > 0 \qquad \text{for all } j \in \{1, \ldots, t\}.$$

So the nonzero rational function $h := g_1^{m_1} g_2^{m_2} \cdots g_s^{m_s}$ satisfies the condition $ord_{f_j}(h) > 0$ for all j. Since h may be obtained from $g_1^{(1)}, \ldots, g_s^{(2)}$ with s subtractions and $s - 1$ operations $(t_1, t_2) \mapsto t_1^{e_1} t_2^{e_2}$ of arity 2 we have

$$L_+(h) \leq C_{+,=}(T), \qquad L_{(2)}(h) \leq C_{*,-}(T) - 1.$$

Theorem 3 implies now that there exist

$$\alpha, \tilde{\alpha} \in \mathbf{C}, \qquad u, \tilde{u} \in \mathbf{C}[x_1, \ldots, x_m], \qquad v, \tilde{v} \in \mathbf{C}[x_1, \ldots, x_m] \backslash \{0\}$$

satisfying

$$h = \tilde{\alpha} \frac{\tilde{u}}{\tilde{v}}, \qquad trdeg_{\mathbf{Q}} T(\tilde{u}, \tilde{v}) \leq L_+(h),$$

$$h = \alpha + \frac{u}{v}, \qquad trdeg_{\mathbf{Q}} T(u, v) \leq 2L_{(2)}(h).$$

The polynomials $f_1, \ldots, f_t$ are prime factors of $\tilde{u}$ and of $\alpha v + u$. Lemma 1 implies therefore that

$$trdeg_{\mathbf{Q}} T(f_1, \ldots, f_t) - t \leq trdeg_{\mathbf{Q}} T(\tilde{u}),$$
$$trdeg_{\mathbf{Q}} T(f_1, \ldots, f_t) - t \leq trdeg_{\mathbf{Q}} T(\alpha v + u).$$

Since we assume the algebraic independence over $\mathbf{Q}$ of the coefficients of the polynomials f_i we have

$$trdeg_{\mathbf{Q}} T(f_1, \ldots, f_t) = \sum_{i=1}^{t} \binom{d_i + m}{m}.$$

This proves the asserted lower bounds. ∎

Proof of Theorem 2. Let T be a tree deciding membership in a proper algebraic subset $X \subset \mathbf{R}^m$. Without loss of generality we can assume that for every path π from the root to a leaf in T the set

$$D_\pi := \{\xi \in X : \text{the input } \xi \text{ defines the path } \pi \text{ in } T\}$$

is nonempty. Obviously $X = \bigcup\{D_\pi : \pi \text{ path leading to a yes-leaf}\}$. Consider a path π that leads to a yes-leaf as being fixed for a moment. Let us denote by $V_\leq$ the set of $\leq$-branching nodes of π and let $g_\nu^{(1)}, g_\nu^{(2)}$ be rational functions for $\nu \in V_\leq$ such that

$$g_\nu^{(1)} \leq g_\nu^{(2)} \ ?$$

is the test performed at node ν. The set $V_=$ and the rational functions $g_\nu^{(1)}$, $g_\nu^{(2)}$ for $\nu \in V_=$ are defined similarly. We have $g_\nu^{(1)} \neq g_\nu^{(2)}$ for every $\nu \in V_\leq \cup V_=$ since the D_π are nonempty. Furthermore

$$L_+(g_\nu^{(1)}, g_\nu^{(2)}) \leq C_{+,\leq}(T) - 1, \; L_*(g_\nu^{(1)}, g_\nu^{(2)}) \leq C_{*,\leq}(T) - 1$$

for all $\nu \in V_\leq \cup V_=$. There are partitions

$$V_\leq = V_{\leq,\text{true}} \cup V_{\leq,\text{false}}, \qquad V_= = V_{=,\text{true}} \cup V_{=,\text{false}}$$

with the property that an element ξ lies in D_π if and only if the following conditions are satisfied:

$$\forall \nu \in V_{\leq,\text{true}} \; g_\nu^{(1)}(\xi) \leq g_\nu^{(2)}(\xi), \qquad \forall \nu \in V_{\leq,\text{false}} \; g_\nu^{(1)}(\xi) > g_\nu^{(2)}(\xi),$$
$$\forall \nu \in V_{=,\text{true}} \; g_\nu^{(1)}(\xi) = g_\nu^{(2)}(\xi), \qquad \forall \nu \in V_{=,\text{false}} \; g_\nu^{(1)}(\xi) \neq g_\nu^{(2)}(\xi).$$

We show now that

$$D_\pi \subset \bigcup \{\{\xi \in \mathbf{R}^m : g_\nu^{(1)}(\xi) = g_\nu^{(2)}(\xi)\} : \nu \in V_{\leq,\text{true}} \cup V_{=,\text{true}}\}. \tag{9}$$

If $V_{=,\text{true}}$ is nonempty the statement (9) is obvious. So let us assume that $V_{=,\text{true}}$ is empty. If (9) were violated then D_π would contain a nonempty

open subset of $\mathbf{R}^m$ which would contradict the assumption that X is a proper algebraic subset of $\mathbf{R}^m$.

Now we use that X is an irreducible hypersurface. Therefore there exists a path π such that D_π is Zariski-dense in X. Moreover, also by the irreducibility of X, there is a $\nu \in V_{\leq,\text{true}} \cup V_{=,\text{true}}$ such that

$$D_\pi \subset \{\xi \in \mathbf{R}^m : g_\nu^{(1)}(\xi) = g_\nu^{(2)}(\xi)\}.$$

Because the vanishing ideal of X equals (f) (cf. Bochnak, Coste, and Roy, 1987, Théorème 4.5.1, p. 85) we get $ord_f(g_\nu^{(1)} - g_\nu^{(2)}) > 0$. The rest of the proof is identical to the one of Theorem 1. ■

Remark. Assume $k = \mathbf{R}$ or $k = \mathbf{C}$. Eve's algorithm (Eve, 1964) shows for a univariate polynomial $f \in k[x]$ of degree d the upper bound

$$L_{*,k[x]}(f) \leq d/2 + 2. \tag{10}$$

From this can be easily concluded that for fixed $m \in \mathbf{N}'$ there is a sequence $(\rho_d) = o(1)$ $(d \to \infty)$ such that for any polynomial $f \in k[x_1, \ldots, x_m]$ of degree d

$$L_{*,k[x]}(f) \leq \frac{d^m}{2(m!)}(1 + \rho_d). \tag{11}$$

Assume now that $m, t \in \mathbf{N}'$ are fixed. The estimate (11) implies immediately that there is a sequence $(\sigma_{(d_1,\ldots,d_t)}) = o(1)$ $(\min_{1\leq i\leq t} d_i \to \infty)$ such that for all hypersurfaces $X \subset \mathbf{C}^m$ of degree format $(d_1, \ldots, d_t)$

$$C_{*,=}(X) \leq \frac{1}{2(m!)} \sum_{i=1}^{t} d_i^m (1 + \sigma_{(d_1,\ldots,d_t)}).$$

The lower bounds (4), (6) in Theorem 1 and 2 are therefore asymptotically sharp.

Proof of Proposition 1. The upper bounds in Proposition 1 follow from the obvious bisection algorithm. The lower bound in (8) is a consequence of Ben-Or's result (Ben-Or, 1983). Our proof of statement (7) is based on the following theorem due to Grigoriev (1982) and Risler (1985) (see Benedetti and Risler, 1990):

For all $f \in \mathbf{R}(x)^*$ we have for the additive complexity $k = L_+(f)$ of f

$$|\{\xi \in \mathbf{R} : f(\xi) = 0\}| \leq (k + 2)^{2k+1} 2^{2k^2+2k+1}. \tag{12}$$

We now show the lower bound in (7). Let T be a tree deciding membership in X. By the first part of the proof of Theorem 2, applied to the finite subset $X \subset \mathbf{R}$, we have from relation (9) for each path π of T leading to a yes-leaf

$$D_\pi \subset \bigcup \{\{\xi \in \mathbf{R} : g_\nu^{(1)}(\xi) = g_\nu^{(2)}(\xi)\} : \nu \in V_{\leq,\text{true}} \cup V_{=,\text{true}}\} \qquad (13)$$

(with the notation adopted from there). We put $\rho := C_{+,\leq}(T)$. As the right-hand side of (13) is the zeroset of

$$h_\pi := \prod_{\nu \in V_{\leq,\text{true}} \cup V_{=,\text{true}}} (g_\nu^{(1)} - g_\nu^{(2)})$$

and $L_+(h_\pi) \leq \rho$ we conclude from statement (12) that

$$|D_\pi| \leq (\rho + 2)^{2\rho+1} 2^{2\rho^2+2\rho+1}.$$

Since there are at most 2^ρ paths π we see that

$$|X| \leq 2^\rho (\rho + 2)^{2\rho+1} 2^{2\rho^2+2\rho+1},$$

and a routine calculation shows that

$$\tfrac{1}{3} \sqrt{\log |X|} \leq \rho = C_{+,\leq}(X)$$

(if $\rho = 1$ one sees directly that $|X| \leq 3$).

Assume now that the elements of X are algebraically independent over $\mathbf{Q}$. Theorem 3 and Lemma 1 imply

$$|D_\pi| - 1 \leq L_+(h_\pi)$$

as $D_\pi \subset \mathit{Zeroset}(h_\pi)$. If there is a path π leading to a yes-leaf such that $|D_\pi| > \log t$ we are done. Otherwise the tree T has at least $t/\log t$ yes-leaves, and there is a path π with at least $\log(t/\log t)$ comparisons.

ACKNOWLEDGMENTS

We thank Robby Robson for useful conversations, a referee for suggesting a simplified proof of Lemma 1, and Marie-Françoise Coste-Roy for communicating to us the reference Montaña *et al.* (1990). Research was done while the authors visited the International Computer Science Institute, Berkeley, and was sponsored by the Verein zur Förderung der deutsch-amerikanischen Zusammenarbeit auf dem Gebiet der Informatik und ihrer Anwendungen. The third author was also supported in part by NSF grants.

REFERENCES

BAUR, W., AND RABIN, M. O. (1982), Linear disjointness and algebraic complexity, *in* "Logic and Algorithmic: An International Symposium Held in Honour of Ernst Specker," Monographies de l'Enseignement Mathématique, No. 30, pp. 35–46, Geneva.

BAUR, W., AND STRASSEN, V. (1982), The complexity of partial derivatives, *Theoret. Comput. Sci.* **22,** 317–330.

BELAGA, E. G., (1961), Evaluation of polynomials of one variable with preliminary processing of the coefficients, *Problemy Kibernet.* **5,** 7–15.

BENEDETTI, R., AND RISLER, J.-J. (1990), "Real Algebraic and Semi-algebraic Sets," Actualités Mathématiques, Hermann, Paris.

BEN-OR, M. (1983), Lower bounds for algebraic computation trees, *in* "Proceedings, 15th ACM STOC, Boston," pp. 80–86.

BOCHNAK, J., COSTE, M., AND ROY, M.-F. (1987), "Géométrie algébrique réelle," Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band 12, Springer-Verlag, Berlin, New York.

BORODIN, A., AND MUNRO, I. (1975), The Computational Complexity of Algebraic and Numeric Problems, American Elsevier, New York.

DOBKIN, D., AND LIPTON, R. J. (1978), A lower bound of $n^2/2$ on linear search programs for the knapsack problem, *J. Comput. System Sci.* **16,** 413–417.

EVE, J. (1964), The evaluation of polynomials, *Numer. Math.* **6,** 17–21.

VON ZUR GATHEN, J. (1988), Algebraic complexity theory, *Annu. Rev. Comput. Sci.* **3,** 317–347.

GRIGORIEV, D. YU. (1982), Preprinty LOMI No. **118,** pp. 25–82.

JAROMCZYK, J. W. (1981), An extension of Rabin's complete proof concept, *in* "Lecture Notes in Computer Science," Vol. **118,** pp. 321–326, Springer, Berlin/New York.

LICKTEIG, T. (1990), On semialgebraic decision complexity, Tech. Rep. TR-90-052 Int. Comp. Science Inst., Berkeley, and Univ. Tübingen, Habilitationsschrift, to appear.

MONTAÑA, J. L., PARDO, L. M., AND RECIO, T. (1990), The non-scalar model of complexity in computational geometry, *in* "Proceedings of the Symposium 'MEGA-90—Effective Methods in Algebraic Geometry,' Castiglioncello, Livorno, Italy," pp. 347–361.

MOTZKIN, T. S. (1955), Evaluation of polynomials, *Bull. Amer. Math. Soc.* **61,** 163.

PATERSON, M. S., AND STOCKMEYER, L. (1971), Bounds on the evaluation time of rational polynomials, *in* "IEEE Conference Record 12th Annual Symp. on Switching and Automata Theory," pp. 140–143.

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

RECIO, T., AND PARDO, L. M. (1989), Rabin's width of a complete proof and the width of a semialgebraic set, *in* "Proceedings, EUROCAL '87, Leipzig, Lecture Notes in Computer Science, vol. 378, pp. 456–462, Springer, Berlin/New York.

REINGOLD, E. M., AND STOCKS, I. (1972), Simple proofs for polynomial evaluation, *in* "Complexity of Computer Computations," (R. Miller and J. Thatcher, Eds.), pp. 21–30, Plenum, New York.

RISLER, J.-J. (1985), Additive complexity and zeros of real polynomials, *SIAM J. Comput.* **14,** 178–183.

SCHNORR, C. P. (1981), An extension of Strassen's degree bound, *SIAM J. Comput.* **10,** 371–382.

SCHUSTER, P. (1980), Interpolation und Kettenbruchentwicklung. Die Komplexität einiger Berechnungsaufgaben, Dissertation, Universität Zürich.

SHAFAREVICH, I. R. (1974), "Basic Algebraic Geometry," Grundlehren der Mathematischen Wissenschaften, Vol. 213, Springer, Berlin/New York.

STEELE, J. M., AND YAO, A. C. (1982), Lower bounds for algebraic decision trees, *J. Algorithms* **3,** 1–8.

STRASSEN, V. (1973), Vermeidung von Divisionen, *Crelles J. Reine Angew. Math.* **264,** 184–202.

STRASSEN, V. (1983), The computational complexity of continued fractions, *in* "Proceedings, 1981 ACM Symposium on Symbolic and Algebraic Computation" and *SIAM J. Comput* **12,** 1–27.

STRASSEN, V. (1984), Algebraische Berechnungskomplexität, *in* "Perspectives in Mathematics, Anniversary of Oberwolfach 1984" (W. Jäger, J. Moser, and R. Remmert, Eds.), pp. 509–550, Birkhäuser Verlag, Basel.

STRASSEN, V. (1990), Algebraic complexity theory, *in* "Handbook of Theoretical Computer Science" (J. van Leeuwen, A. Meyer, M. Nivat, M. Paterson, and D. Perrin, Eds.), Vol. A, pp. 635–672, Elsevier, Amsterdam/New York.

YAO, A. C. (1989), Lower bounds for algebraic computation trees with integer inputs, *in* "Proceedings 30th IEEE Symposium FOCS, Research Triangle Park, North Carolina," pp. 308–313.