On randomized algebraic test complexity*

Peter Bürgisser†
Dept. of Computer Science
University of Bonn
5300 Bonn 1

Marek Karpinski ‡
Dept. of Computer Science
University of Bonn
5300 Bonn 1
and
International Computer Science Institute
Berkeley, California

Thomas Lickteig§
Dept. of Computer Science
University of Bonn
5300 Bonn 1

Abstract. We investigate the impact of randomization on the complexity of deciding membership in a (semi-)algebraic subset $X \subset \mathbb{R}^m$. Examples are exhibited where allowing for a certain error probability ϵ in the answer of the algorithms the complexity of decision problems decreases. A randomized $(\Omega^k, \{=, \leq\})$-decision tree ($k \subseteq \mathbb{R}$ a subfield) over m will be defined as a pair (T, μ) where μ a probability measure on some $\mathbb{R}^n$ and T is a $(\Omega^k, \{=, \leq\})$-decision tree over $m + n$. We prove a general lower bound on the average decision complexity for testing membership in an irreducible algebraic subset $X \subset \mathbb{R}^m$ and apply it to k-generic complete intersection of polynomials of the same degree, extending results in [4, 6]. We also give applications to nongeneric cases, such as graphs of elementary symmetric functions, $\mathrm{SL}(m, \mathbb{R})$, and determinant varieties, extending results in [Li 90].

Key words. Algebraic complexity theory, decision trees, randomization, straight line programs, real spectrum.
Subject classification. 68C20, 68C25, 14P10.

---

*Submitted to *Journal of Complexity*
†Sponsored by the Schweizerischer Nationalfonds
‡Supported in part by Leibniz Center for Research in Computer Science, by the DFG Grant KA 673/4-1 and by the SERC Grant GR-E 68297
§Sponsored by DFG Heisenberg-Grant Li 405/2-1

1 Introduction

We are concerned with the computational task of testing membership in a semi-algebraic subset $X \subseteq \mathbb{R}^m$. The starting point of our investigation is the observation that for membership problems of certain $X \subseteq \mathbb{R}^m$ there are randomized algorithms that run much faster than any deterministic one. We illustrate this by two examples.

Example 1. Let
$$X := \{(A,B,C) : AB = C\} \subset (\mathbb{R}^{m\times m})^3$$
be the graph of matrix multiplication. It is conceivable – although not proven so far – that deciding membership in X is as hard as matrix multiplication. Freivalds [Fr 89] proposed the following randomized algorithm: choose a vector $\rho \in \{0,1\}^m$ at random with probability 2^{-m}, compute $A(B\rho)$ and $C\rho$, test whether $A(B\rho) = C\rho$, and if this is the case answer "yes", otherwise reply "no". The answer given by the algorithm can only be wrong if $AB \neq C$, but then the error probability is at most $1/2$ since for every affine hyperplane $H \subset \mathbb{R}^m$ one has $|\{0,1\}^m \cap H| \leq 2^{m-1}$.

This algorithm uses only $O(m^2)$ arithmetical operations and comparisons. Furthermore, by repeating this procedure t times we can achieve an error probability of at most 2^{-t} with an amount of $O(tm^2)$ steps, whereas the complexity of matrix multiplication is not believed to be of order m^2.

Example 2. Let
$$X := \{(\xi,\zeta) : \zeta = \sigma(\xi)\} \subset \mathbb{R}^{2m}$$
denote the graph of the mapping given by all elementary symmetric functions $\sigma_1,\ldots,\sigma_m$. By Strassen [St 83] (over $\mathbb{C}$) and the extension by Montaña-Pardo-Recio [MRR 90] of Ben-Or [Be 83] the number of multiplications, divisions and comparisons necessary to test membership in X (deterministically) is at least of order of magnitude $m \log m$.

However, when allowing for a certain error probability, one can proceed in the following way. Given an input $(\xi,\zeta) \in \mathbb{R}^{2m}$, choose a number $\rho \in \mathbb{R}$ at random according to some probability distribution μ on $\mathbb{R}$, compute (using Horner's rule)
$$\rho^m + \sum_{i=1}^{m} (-1)^i \zeta_i \rho^{m-i} \text{ and } \prod_{i=1}^{m} (\rho - \xi_i),$$
and test whether they are equal. If this is the case answer "yes", otherwise answer "no". If $(\xi,\zeta) \in X$, the correct answer is given, and for $(\xi,\zeta) \notin X$ the error probability equals

$\mu(\mathcal{Z}(f_{\xi,\zeta}))$ where $\mathcal{Z}(f_{\xi,\zeta})$ denotes the zeroset of

$$f_{\xi,\zeta} := \sum_{i=1}^{m} (-1)^i (\zeta_i - \sigma_i(\xi)) T^{m-i} \in \mathbb{R}[T] \setminus \{0\}.$$

Hence the error probability is at most

$$\epsilon := \sup\{\mu(M) : M \subset \mathbb{R} \ \ |M| = m-1\}.$$

(Taking for instance the uniform distribution on $2m-2$ points in $\mathbb{R}$ one obtains $\epsilon = 1/2$; if the probability measure has a density (e.g. the Gauss distribution) then even $\epsilon = 0$.)

This algorithm runs with only $O(m)$ arithmetical operations and comparisons and is therefore at least by a factor of order $\log m$ faster than an optimal deterministic one.

In this paper we show in particular that for hypersurfaces $X \subseteq \mathbb{R}^m$ randomization does not help much, irrespective of the chosen measure μ on some $\mathbb{R}^n$ provided that μ satisfies some mild "algebraicity" condition. We also give a lower bound on the $\mathbb{R}$-preconditioned (μ, ϵ)-average decision complexity of the membership problem of a k-generic complete intersection $X \subseteq \mathbb{R}^m$ of r polynomials of the same degree, $k \subseteq \mathbb{R}$ a subfield. This bound is by a factor of r smaller than the (deterministic) $\mathbb{R}$-preconditioned decision complexity which has been determined in Bürgisser [Bü 92]. In particular, the lower bounds in Bürgisser-Lickteig-Shub [BLS 90] on $\mathbb{R}$-preconditioned decision complexity of a $\mathbb{Q}$-generic hypersurface remain essentially true for $\mathbb{R}$-preconditioned (μ, ϵ)-average decision complexity.

Section 2 contains the definitions of randomized decision trees (T, μ), (μ, ϵ)-average complexity, and $\mathbb{R}$-preconditioning. In section 3 we give the main result on average decision complexity, and in section 4 the above mentioned applications.

Our result does also apply to nongeneric cases. For instance the (μ, ϵ)-average complexity of the membership problem of $\mathrm{SL}(m, \mathbb{R}) \subset \mathbb{R}^{m \times m}$ is about the same as the complexity of matrix multiplication, and the (μ, ϵ)-average complexity of the membership problem of determinant varieties

$$\{A \in \mathbb{R}^{p \times q} : \mathrm{rank} A \leq r\} \subset \{A \in \mathbb{R}^{p \times q} : \mathrm{rank} A \leq s\}$$

$(r < s \leq p \leq q)$ has a lower bound of order r^2. We will also show that the randomized algorithm described in Example 2 for testing *all* elementary symmetric functions for certain values is optimal up to a constant factor. In contrast to this, for the graph

$$\mathrm{graph}\sigma_{\lfloor m/2 \rfloor} \subset \mathbb{R}^{m+1}$$

of the *single* middle elementary symmetric $\sigma_{\lfloor m/2 \rfloor}$ the (μ, ϵ)-average decision complexity will be shown to be at least of order $m \log m$. These lower bounds remain even true for the membership problems of the respective sets of rational points, and extend results in Lickteig [Li 90]. (For decision complexity and rational points see also [Be 83, Hi 91, Ya 89].)

As in [Bü 92, BL 91] we follow the approach inititated in [Li 90] to prove lower bounds on decision complexity. We will use some real algebraic geometry, and the reader is assumed to be familiar with its basic concepts. For this theory we refer to the book by Bochnak, Coste and Roy [BCR 86]; see also Knebusch and Scheiderer [KS 89, chapt. III]. As far as complexity theory is concerned the reader is assumed to be familiar with [BL 91, sections 1-4]. For some overview on lower bounds on decision complexity see e.g. the introduction of [BL 91]. For general background on randomized algorithms see e.g. Karp [Ka 90], and Karpinski and Verbeek [KV 87] and the references given there.

2 Randomized decision trees

We recall some definitions following the terminology in [BL 91, Li 90]. Throughout this paper $k \subseteq \mathbb{R}$ denotes a fixed subfield. We consider (Ω^k, P)-decision trees T over $m \in \mathbb{N}$; these trees take as inputs elements from $\mathbb{R}^m$, use operations in $\Omega^k := k \sqcup \{0, 1, +, -, *, /\}$ ($\lambda \in k$ stands for the scalar multiplication with λ) and branch according to relations in $P := \{=, \leq\}$. To each leaf of such a tree T is assigned one of the symbols *yes* or *no*. For $\xi \in \mathbb{R}^m$ we denote by T_ξ the path in T defined by the input ξ (leading to a leaf or ending prior to an unexecutable division instruction, cf. [BL 91]).

Let $X \subseteq Y \subseteq \mathbb{R}^m$ be subsets (semi-algebraic or not). We say that T decides the partition $\{X, Y \setminus X\}$ of Y (or T decides membership in X relative to Y) if for all $\xi \in X$ the path T_ξ ends up with a *yes*-leaf and for all $\xi \in Y \setminus X$ the path T_ξ ends up with a *no*-leaf.

Let $c : \Omega^k \sqcup P \to \mathbb{N}$ be a cost function. The c-length $L(c, \pi)$ of a path π in T is defined as the sum of the costs along π; the c-cost of the tree T is the maximum of the $L(c, \pi)$ taken over all paths π in T (cf. [BL 91]). The *decision complexity* $C(c, \{X, Y \setminus X\})$ of a partition $\{X, Y \setminus X\}$ of Y with respect to (k and) c is defined as

$$C(c, \{X, Y \setminus X\}) := \min_T \max_{\xi \in Y} L(c, T_\xi)$$

where T varies over all (Ω^k, P)-decision trees over m deciding the partition $\{X, Y \setminus X\}$. One has $C(c, \{X, Y \setminus X\}) < \infty$ for semi-algebraic X and Y if and only if X is the trace in Y of a k-definable semi-algebraic subset of $\mathbb{R}^m$. In order to deal with arbitrary partitions $\{X, Y \setminus X\}$ one must allow preconditioning of certain real constants $\zeta_1, \ldots, \zeta_s \in \mathbb{R}$. So one minimizes the decision complexities of all partitions

$$\{\{\zeta\} \times X, \{\zeta\} \times (Y \setminus X)\}$$

of $\{\zeta\} \times Y \subseteq \mathbb{R}^{s+m}$; the $\mathbb{R}$-*preconditioned decision complexity* of $\{X, Y \setminus X\}$ with respect to c is defined as (cf. [Bü 92])

$$C_{\mathbb{R}}(c, \{X, Y \setminus X\}) := \min\{C(c, \{\{\zeta\} \times X, \{\zeta\} \times (Y \setminus X)\}) : s \in \mathbb{N}, \zeta \in \mathbb{R}^s\}.$$

Let us now formalize the notion of a randomized decision tree. We call a finite measure

$$\mu : \mathcal{B}(\mathbb{R}^n) \to [0, \infty)$$

on the Borel algebra of $\mathbb{R}^n$ *algebraic* if it can be written as a finite sum

$$\mu = \sum_{i=1}^{N} \mu_i$$

of Borel measures μ_i which are *pure*; i.e., they should satisfy the following conditions:

(P1) the Zariski closure $Zarsupp\mu_i \subseteq \mathbb{R}^n$ of the support of μ_i is irreducible,

(P2) $\mu_i(Z) = 0$ for all proper algebraic subsets $Z \subset Zarsupp\mu_i$.

(Example: a convex combination of a Gauss-distribution on $\mathbb{R}$ and some δ-"functions".)

Let T be an (Ω^k, P)-decision tree over $m + n$ and μ be an algebraic probability measure on $\mathbb{R}^n$. We call the pair (T, μ) a *randomized* (Ω^k, P)*-decision tree over* m.

The *average* c*-length of* (T, μ) *on input* $\xi \in \mathbb{R}^m$ is defined as

$$L(c, (T, \mu), \xi) := \int_{\mathbb{R}^n} L(c, T_{(\xi,\rho)}) d\mu(\rho).$$

(It measures the expected c-cost of the tree on input ξ. Any sort of costs to perform the random choice of ρ are not taken into account.)

We say that (T, μ) decides a partition $\{X, Y \setminus X\}$ of $Y \subseteq \mathbb{R}^m$ (or (T, μ) decides membership in X relative to Y) with error probability $\epsilon \in [0, 1)$ if

(R1) the path $T_{(\xi,\rho)}$ ends up with a leaf for all $(\xi, \rho) \in Y \times \mathbb{R}^n$,

(R2) wrong answers are rare:

$$\begin{array}{lll} \forall \xi \in X : & \mu\{\rho \in \mathbb{R}^n : T_{(\xi,\rho)} \text{ ends up with a } \textit{no}\text{-leaf}\} & \leq \epsilon, \\ \forall \xi \in Y \setminus X : & \mu\{\rho \in \mathbb{R}^n : T_{(\xi,\rho)} \text{ ends up with a } \textit{yes}\text{-leaf}\} & \leq \epsilon. \end{array}$$

Let an algebraic measure $\mu : \mathcal{B}(\mathbb{R}^n) \to [0,1]$ and $\epsilon \in [0,1)$ be given. We define the (μ,ϵ)-*average decision complexity* $C^{(\mu,\epsilon)}(c,\{X, Y \setminus X\})$ of $\{X, Y \setminus X\}$ with respect to a cost function $c : \Omega^k \sqcup P \to \mathbb{N}$ as

$$C^{(\mu,\epsilon)}(c,\{X, Y \setminus X\}) := \min_T \max_{\xi \in \mathbb{R}^m} L(c,(T,\mu),\xi)$$

where T varies over all (Ω^k, P)-decision trees over $m+n$ such that (T,μ) decides membership in X relative to Y with error probability ϵ. The $\mathbb{R}$-*preconditioned* (μ,ϵ)-*average decision complexity* $C_{\mathbb{R}}^{(\mu,\epsilon)}(c,\{X, Y \setminus X\})$ of $\{X, Y \setminus X\}$ with respect to c is defined as

$$C_{\mathbb{R}}^{(\mu,\epsilon)}(c,\{X, Y \setminus X\}) := \min_{s \in \mathbb{N}} \min_{\zeta \in \mathbb{R}^s} C^{(\mu,\epsilon)}(c,\{\{\zeta\} \times X, \{\zeta\} \times (Y \setminus X)\}).$$

We remark that if $\epsilon \in [0,1)$ is given there is always an algebraic probability distribution μ on $\mathbb{R}$ such that

$$C^{(\mu,\epsilon)}(c,\{X, Y \setminus X\}) \leq (1-\epsilon) C(c,\{X, Y \setminus X\}) + \min\{c(=), c(\leq)\}.$$

(Take for instance $\mu = \epsilon\delta_0 + (1-\epsilon)\delta_1$ and proceed in the following way: check first whether $\zeta > 0$; if yes continue deterministically, otherwise answer "no", say.) This shows that randomization may lead to at least a certain decreasing of the decision complexity. Our analysis will show that in several cases not much more decreasing is possible.

In the sequel we will apply some real algebraic geometry (cf. [BCR 86]). Let

$$\alpha = (p, \leq_\alpha) \in \mathrm{Spec}_r \mathbb{R}[x_1,\ldots,x_m]$$

be given. Following [BL 91, Li 90] we consider α as an input of (Ω^k, P)-decision trees T over m by identifying α with

$$(\kappa(p)_{\leq_\alpha}, (x_1(p),\ldots,x_m(p)));$$

by T_α we denote the path distinguished by the input α (leading to a leaf or ending prior to an unexecutable division instruction). $\mathrm{Ex}T \subseteq \mathrm{Spec}_r \mathbb{R}[x_1,\ldots,x_m]$ denotes the constructible subset of all α such that T is executable on α, i.e., T_α ends up with a leaf. $T_{\alpha,\beta}$ denotes the common piece of T_α and T_β for $\alpha, \beta \in \mathrm{Spec}_r \mathbb{R}[x_1,\ldots,x_m]$.

For any path π in T we denote by $\Gamma(\pi)$ the Ω^k-straight line program over m assigned to π by "forgetting" the comparison instructions. An input for an Ω^k-straight line program Γ over m is a pair (A, x) where A is a k-algebra and $x \in A^m$. A localization A of a residue class ring of $\mathbb{R}[x_1,\ldots,x_m]$ defines (via $k \to \mathbb{R}$) canonically a *standard input* for Ω^k-straight line programs over m, denoted by (A, x), which is induced by the vector of coordinate functions $x = (x_1,\ldots,x_m)$, i.e., x has to be interpreted in A^m.

Finally let us recall that for an irreducible algebraic subset $V \subseteq \mathbb{R}^m$ the central points $\xi \in \mathrm{Cent}V := \overline{\mathrm{Reg}V}$ are characterized by

$$\dim_\xi V = \dim V$$

where $\dim_\xi V$ is the (local) dimension of V in the point ξ (cf. [BCR 86, 7.6.1]).

3 A general lower bound

Before stating our main result we need to recall a definition from [Li 90]. Let $X \subset Y \subseteq \mathbb{R}^m$ be irreducible algebraic subsets. The *exclusion complexity* $\mathrm{EC}(c, X, Y)$ of X in Y with respect to a cost function $c : \Omega^k \to \mathbb{N}$ is defined as

$$\mathrm{EC}(c, X, Y) := \min\{L_{k \to \mathcal{O}_{X,Y}}(c, x, f) : f \in \mathcal{M}_{X,Y} \setminus \{0\}\};$$

here $\mathcal{O}_{X,Y}$ denotes the localization of the coordinate ring $\mathcal{P}(Y)$ of Y in the vanishing ideal of X, $\mathcal{M}_{X,Y}$ its maximal ideal, and $L_{k \to \mathcal{O}_{X,Y}}(c, x, f)$ denotes the minimum c-length of an Ω^k-straight line program over m that computes f on the standard input $(\mathcal{O}_{X,Y}, x)$. The $\mathbb{R}$-*preconditioned exclusion complexity* of X in Y with respect to c is defined as

$$\mathrm{EC}_{\mathbb{R}}(c, X, Y) := \min\{\mathrm{EC}(c, \{\zeta\} \times X, \{\zeta\} \times Y) : s \in \mathbb{N}, \zeta \in \mathbb{R}^s\}.$$

(By definition $\mathrm{EC}(c, X, Y) \geq \mathrm{EC}_{\mathbb{R}}(c, X, Y)$, and equality holds if $k = \mathbb{R}$ and c is nonscalar.)

Let

$$\begin{array}{ccc} X' & \subset & Y' \\ \downarrow & & \downarrow \\ X & \subset & Y \end{array}$$

be an inclusion of pairs of semi-algebraic subsets of $\mathbb{R}^m$, X and Y being irreducible algebraic subsets. Under certain conditions on the pair (X', Y') the decision complexity of $\{X', Y' \setminus X'\}$ and exclusion complexity of X in Y are related as

$$C(c, \{X', Y' \setminus X'\}) \geq \mathrm{EC}(c|_{\Omega^k}, X, Y) - c(-),$$

and this lower bound remains even true if one replaces the pair (X', Y') by a pair (X'', Y'') of (arbitrary) subsets with X'' dense in X' and Y'' dense in Y' (cf. [Li 90, section E], resp. Lemmas 3.5, 3.6, 3.7 below).

Our main result is that $\mathbb{R}$-preconditioned exclusion complexity provides also a lower bound on average decision complexity.

Theorem 3.1 *Let $k \subseteq \mathbb{R}$ be a subfield, $c : \Omega^k \sqcup P \to \mathbb{N}$ a cost function, and*

$$\begin{array}{ccc} X' & \subset & Y' \\ \downarrow & & \downarrow \\ X & \subset & Y \end{array}$$

be an inclusion of pairs of semi-algebraic subsets of $\mathbb{R}^m$ where $X \subset Y \subseteq \mathbb{R}^m$ are irreducible algebraic subsets, $\dim X' = \dim X$ *and*

$$\forall \xi \in Y' : \quad \dim_\xi Y' = \dim Y.$$

If $X'' \subseteq X'$, $Y'' \subseteq Y'$ are dense subsets, $X'' \subset Y''$, and (T, μ) is a randomized (Ω^k, P)-decision tree over m deciding $\{X'', Y'' \backslash X''\}$ with error probability ϵ, then there is an algebraic subset $W \subset X$ with $\dim W < \dim X$ *such that*

$$\forall \xi \in X' \setminus W : \quad L(c, (T, \mu), \xi) \geq (1 - 2\epsilon)(\mathrm{EC}_{\mathbb{R}}(c|_{\Omega^k}, X, Y) - c(-)).$$

Remark 3.2 *Let $F \subseteq \mathbb{R}$ be a subfield. If the F-rational points $X(F)$ resp. $Y(F)$ of F-definable X resp. Y lie dense in X resp. Y and* $\mathrm{Cent}X \subset \mathrm{Cent}Y$ *then for instance*

$$\begin{aligned} X'' &:= X(F) \cap \mathrm{Cent}X \subset \mathrm{Cent}X =: X', \\ Y'' &:= Y(F) \cap \mathrm{Cent}Y \subset \mathrm{Cent}Y =: Y' \end{aligned}$$

satisfy the assumptions of the theorem (e.g. determinant varieties; see section 4).

If $X \subset Y \subseteq \mathbb{R}^m$ are irreducible algebraic subsets then we call $\mathcal{I}(X) \in \mathrm{Spec}\mathcal{P}(Y)$ *central* if one of the following equivalent conditions are satisfied (cf. [BCR 86, 7.6.2, 10.2.4]):

(C1) $\mathcal{I}(X)$ is the center in $\mathcal{P}(Y)$ of a real place of $\mathcal{K}(Y)$ which is finite over $\mathcal{P}(Y)$,

(C2) $\exists \alpha \in \mathrm{Spec}_r\mathcal{K}(X)\ \exists \beta \in \mathrm{Spec}_r\mathcal{K}(Y) :\ \ \beta$ generalization of α in $\mathrm{Spec}_r\mathcal{O}_{X,Y}$,

(C3) $\dim(X \cap \mathrm{Cent}Y) = \dim X$,

(C4) $\dim(\mathrm{Cent}X \cap \mathrm{Cent}Y) = \dim X$,

(C5) $\dim(\mathrm{Reg}X \cap \mathrm{Cent}Y) = \dim X$.

(Note that this condition is always satisfied if $Y = \mathrm{Reg}Y$. If $Y \subset \mathbb{R}^3$ is the Cartan umbrella (see [BCR 86, 3.1.2 d), p. 53]) then it is not satisfied for $X = \mathrm{Sing}Y$; it is satisfied in the case of [BCR 86, 3.1.2 e), p. 53].)

COROLLARY 3.3 *If $X \subset Y \subseteq \mathbb{R}^m$ are irreducible algebraic subsets, $\mathcal{I}(X) \in \mathrm{Spec}\mathcal{P}(Y)$ central, then for algebraic probability measures $\mu : \mathcal{B}(\mathbb{R}^n) \to [0,1]$, $\epsilon \in [0,1)$, and arbitrary cost functions $c : \Omega^k \sqcup P \to \mathbb{N}$*

$$C_{\mathbb{R}}^{(\mu,\epsilon)}(c, \{X, Y \setminus X\}) \geq (1-2\epsilon)(\mathrm{EC}_{\mathbb{R}}(c|_{\Omega^k}, X, Y) - c(-)).$$

The proof of this corollary follows from Theorem 3.1 taking into account that for $\zeta \in \mathbb{R}^s$

$$\mathrm{EC}_{\mathbb{R}}(c, X, Y) = \mathrm{EC}_{\mathbb{R}}(c, \{\zeta\} \times X, \{\zeta\} \times Y).$$

The proof of Theorem 3.1 is based on the subsequent four lemmas.

LEMMA 3.4 *Let $S \subseteq U \subseteq V \subseteq \mathbb{R}^m$ be semi-algebraic subsets. Then the following two conditions are equivalent:*

(a) $\forall \alpha \in \tilde{S}\ \forall \beta \in \tilde{V} :\ \ \alpha \supseteq \beta,\ \mathrm{dim}\alpha = \mathrm{dim}S \Rightarrow \beta \in \tilde{U}$,

(b) $\exists$ *semi-algebraic* $W \subset S : \mathrm{dim}W < \mathrm{dim}S, S \setminus W \subseteq \mathrm{int}_V U$.

PROOF. (a) $\Rightarrow$ (b): Put $W := S \cap \overline{V \setminus U}$. Obviously, we have $S \setminus W \subseteq \mathrm{int}_V U$. By the way of contradiction we assume that $\mathrm{dim}W = \mathrm{dim}S$. Then by [BCR 86, 7.5.8] there is an $\alpha \in \tilde{W}$ with $\mathrm{dim}\alpha = \mathrm{dim}S$. As $\alpha \in \overline{\tilde{V} \setminus \tilde{U}}$ we conclude by [BCR 86, 7.1.20] that there is a generalization β of α in $\tilde{V} \setminus \tilde{U}$, contradicting (a).

(b) $\Rightarrow$ (a): Assume $S \setminus W \subseteq \mathrm{int}_V U$ for some $W \subset S$ with $\mathrm{dim}W < \mathrm{dim}S$. If $\alpha \in \tilde{S}$, $\mathrm{dim}\alpha = \mathrm{dim}S$ then by [BCR 86, 7.5.8] $\alpha \in \tilde{S} \setminus \tilde{W} \subseteq \mathrm{int}_{\tilde{V}}\tilde{U}$. As open constructible sets are stable under generalization (cf. [BCR 86, 7.1.21]) every generalization $\beta \in \tilde{V}$ of α lies also in $\tilde{U}$. □

LEMMA 3.5 *Let $X \subseteq Y \subseteq \mathbb{R}^m$ be irreducible algebraic subsets, $c : \Omega^k \to \mathbb{N}$ a cost function. Then the following hold:*

(a) If $Z \subseteq \mathbb{R}^m$ is a irreducible algebraic subset, $Y \subseteq Z$ then

$$\mathrm{EC}(c, X, Y) \geq \mathrm{EC}(c, X, Z).$$

(b) If $V \subseteq \mathbb{R}^n$ is an irreducible algebraic subset then

$$\mathrm{EC}_{\mathbb{R}}(c, X, Y) = \mathrm{EC}_{\mathbb{R}}(c, X \times V, Y \times V).$$

PROOF. (a): This follows from the trivial fact that the canonical epimorphism of k-algebras $\mathcal{O}_{X,Z} \to \mathcal{O}_{X,Y}$ is local. Indeed, every Ω^k-straight line program over m executable on the standard input $(\mathcal{O}_{X,Y}, x)$ is also executable on the standard input $(\mathcal{O}_{X,Z}, x)$.

(b): For the inequality

$$\mathrm{EC}(c, X, Y) \geq \mathrm{EC}(c, X \times V, Y \times V)$$

consider the canonical local monomorphism of k-algebras $\mathcal{O}_{X,Y} \to \mathcal{O}_{X \times V, Y \times V}$. Hence also $\mathrm{EC}_{\mathbb{R}}(c, X, Y) \geq \mathrm{EC}_{\mathbb{R}}(c, X \times V, Y \times V)$. The argument for the reverse inequality

$$\mathrm{EC}_{\mathbb{R}}(c, X, Y) \leq \mathrm{EC}_{\mathbb{R}}(c, X \times V, Y \times V)$$

is of *transfer* type: factor the above morphism as

$$\mathcal{O}_{X,Y} \to (\mathcal{O}_{X,Y} \otimes_{\mathbb{R}} \mathcal{P}(V))_d \to \mathcal{O}_{X \times V, Y \times V}$$

where $d \in \mathcal{O}_{X,Y} \otimes_{\mathbb{R}} \mathcal{P}(V)$ is a suitably chosen denominator, and use the Artin-Lang Theorem [BCR 86, 4.1.2] to construct a retraction of the first morphism mapping the coordinate ring $\mathcal{P}(V)$ of V into $\mathbb{R}$. □

LEMMA 3.6 *Let T be an (Ω^k, P)-decision tree over m, $X \subseteq \mathbb{R}^m$ be an irreducible algebraic subset and let $X' \subseteq X$ be a semi-algebraic subset such that* $\dim X' = \dim X$. *Then the following hold:*

(a) There is a proper algebraic subset $Z \subset X$ with $X' \setminus Z \subseteq \mathrm{Ex}T$ if and only if $\tilde{X'} \cap \mathrm{Spec}_r \mathcal{K}(X) \subseteq \mathrm{Ex}T$.

(b) If $X'' \subseteq X'$ is an arbitrary but dense subset of X' then

$$X'' \subseteq \mathrm{Ex}T \Rightarrow \tilde{X'} \cap \mathrm{Spec}_r \mathcal{K}(X) \subseteq \mathrm{Ex}T.$$

PROOF. (a): $X' \cap \mathrm{Ex}T$ is a semi-algebraic subset of X'; so the statement follows from [BCR 86, 7.5.8] applied to its complement in X'.

(b): Let $\alpha \in \tilde{X'} \cap \mathrm{Spec}_r \mathcal{K}(X)$ and consider the locally closed

$$\mathrm{Cell}(T, \alpha) := \{\beta : T_\beta = T_\alpha\} \subseteq \mathrm{Spec}_r \mathbb{R}[x_1, \ldots, x_m].$$

Its trace in X' contains an open nonempty subset of X', therefore it contains also points from X''. Hence $\mathrm{Cell}(T, \alpha) \subseteq \mathrm{Ex}T$ under the condition that $X'' \subseteq \mathrm{Ex}T$. □

LEMMA 3.7 *Let T be an (Ω^k, P)-decision tree over m, $c : \Omega^k \sqcup P \to \mathbb{N}$ a cost function, and $X \subset Y \subseteq \mathbb{R}^m$ be irreducible algebraic subsets. If $\alpha \in \mathrm{Spec}_r\mathcal{K}(X)$ is a specialization in $\mathrm{Spec}_r\mathcal{O}_{X,Y}$ of $\beta \in \mathrm{Spec}_r\mathcal{K}(Y)$ and $T_\alpha \neq T_\beta$ then*

$$L(c, T_\alpha) \geq L(c, T_{\alpha,\beta}) \geq \mathrm{EC}(c|_{\Omega^k}, X, Y) - c(-).$$

PROOF. Consider the common path $T_{\alpha,\beta}$ of α and β in T. Let $\Gamma(T_{\alpha,\beta})$ denote the Ω^k-straight line program over m assigned to $T_{\alpha,\beta}$, and let $(k[x]_d, x)$ be its universal input (cf. [BL 91]). Consider the canonical morphisms of k-algebras

$$\begin{array}{ccc} & k[x]_d & \\ & \downarrow & \\ \mathcal{K}(X)_{\leq\alpha} \leftarrow & \mathcal{O}_{X,Y} & \rightarrow \mathcal{K}(Y)_{\leq\beta}. \end{array}$$

If $T_{\alpha,\beta}$ ends up with a comparison vertex then there are results $f_1, f_2 \in k[x]_d$ of $\Gamma(T_{\alpha,\beta})$ on input $(k[x]_d, x)$ satisfying one of the following four alternatives:

$$\begin{array}{lcl} f_1(\alpha) \leq f_2(\alpha) & \text{and} & f_1(\beta) > f_2(\beta), \\ f_1(\alpha) > f_2(\alpha) & \text{and} & f_1(\beta) \leq f_2(\beta), \\ f_1(\alpha) = f_2(\alpha) & \text{and} & f_1(\beta) \neq f_2(\beta), \\ f_1(\alpha) \neq f_2(\alpha) & \text{and} & f_1(\beta) = f_2(\beta). \end{array}$$

By assumption β is a generalization of α, so by [BCR 86, 7.1.18] the second and fourth one are impossible, and in the remaining cases

$$(f_1 - f_2)(\alpha) = 0, \quad (f_1 - f_2)(\beta) \neq 0$$

and we are done.

If $T_{\alpha,\beta}$ does not end up with a comparison vertex then necessarily $T_\alpha = T_{\alpha,\beta}$ is an initial segment of T_β since by $\alpha \supseteq \beta$ the path T_β cannot be an initial segment of T_α. In this case the assertion follows from the fact that $\Gamma(T_\beta)$ is not executable on standard input $(\mathcal{K}(X), x)$. (Note that T is neither required to be executable on α nor on β.) □

PROOF. (of Theorem 3.1) Throughout the following we will use the notation $Z_\xi := \{\rho : (\xi, \rho) \in Z\}$ for the fiber over $\xi \in \mathbb{R}^m$ of the restriction of the canonical projection $\mathbb{R}^m \times \mathbb{R}^n \to \mathbb{R}^m$ to some semialgebraic subset $Z \subseteq \mathbb{R}^m \times \mathbb{R}^n$.

We define a semialgebraic subset

$$\mathcal{S} := \{(\xi, \rho) : L(c, T_{(\xi,\rho)}) < \mathrm{EC}_{\mathbb{R}}(c|_{\Omega^k}, X, Y) - c(-)\} \subseteq Y' \times \mathbb{R}^n$$

of "T-short" points. For all $\xi \in Y'$ we have

$$L(c,(T,\mu),\xi) = \int_{\mathbb{R}^n} L(c,T_{(\xi,\rho)})d\mu(\rho) \geq (1-\mu\mathcal{S}_\xi)(\mathrm{EC}_{\mathbb{R}}(c|_{\Omega^k},X,Y)-c(-)).$$

Hence it is sufficient to prove that $\mu\mathcal{S}_\xi \leq 2\epsilon$ for all $\xi \in X'$ outside a lower dimensional semi-algebraic subset of X'.

Let $\mu = \Sigma_{i=1}^N \mu_i$, μ_i pure and write $V_i := \mathrm{Zarsupp}\mu_i$. $Y' \times \mathbb{R}^n$ is partitioned into the following three semi-algebraic subsets:

$$\begin{aligned}
\mathcal{Y} &:= \{(\xi,\rho) : T_{(\xi,\rho)} \text{ ends up with a } \textit{yes}\text{-leaf}\},\\
\mathcal{N} &:= \{(\xi,\rho) : T_{(\xi,\rho)} \text{ ends up with a } \textit{no}\text{-leaf}\},\\
\mathcal{U} &:= (Y' \times \mathbb{R}^n) \setminus \mathrm{Ex}T.
\end{aligned}$$

We put furthermore

$$\begin{aligned}
\mathcal{Y}_i &:= \mathcal{Y} \cap (Y' \times V_i),\\
\mathcal{N}_i &:= \mathcal{N} \cap (Y' \times V_i),\\
\mathcal{S}_i^{\mathcal{Y}} &:= \mathcal{S} \cap (X' \times V_i) \cap \mathcal{Y},\\
\mathcal{S}_i^{\mathcal{N}} &:= \mathcal{S} \cap (X' \times V_i) \cap \mathcal{N},\\
\mathcal{S}_i^{\mathcal{U}} &:= \mathcal{S} \cap (X' \times V_i) \cap \mathcal{U},
\end{aligned}$$

having

$$\mathcal{S}_i^{\mathcal{Y}} \subseteq \mathcal{Y}_i \subseteq Y' \times V_i, \;\; \mathcal{S}_i^{\mathcal{N}} \subseteq \mathcal{N}_i \subseteq Y' \times V_i \quad (i=1,\ldots,N). \tag{1}$$

If $\beta \in \widetilde{Y \times V_i}$ is a generalization of some $\alpha \in \mathrm{Spec}_r\mathcal{K}(X \times V_i)$ with $T_\alpha \neq T_\beta$ we may conclude from Lemma 3.7 and Lemma 3.5 that

$$\begin{aligned}
L(c,T_\alpha) &\geq \mathrm{EC}_{\mathbb{R}}(c|_{\Omega^k}, X \times V_i, \mathcal{Z}(\mathrm{supp}\beta)) - c(-)\\
&\geq \mathrm{EC}_{\mathbb{R}}(c|_{\Omega^k}, X, Y) - c(-).
\end{aligned}$$

This intermediate reasoning thus shows

$$\forall \alpha \in \tilde{\mathcal{S}} \cap \mathrm{Spec}_r\mathcal{K}(X \times V_i)\; \forall \beta \in \widetilde{Y \times V_i} \;: \alpha \supseteq \beta \Rightarrow T_\alpha = T_\beta.$$

This allows to apply Lemma 3.4 to the triples in (1). Therefore we can find lower dimensional algebraic subsets

$$\mathcal{W}_i^{\mathcal{Y}}, \mathcal{W}_i^{\mathcal{N}} \subset X \times V_i$$

such that

$$\mathcal{S}_i^{\mathcal{Y}} \setminus \mathcal{W}_i^{\mathcal{Y}} \subset \mathrm{int}_{Y' \times V_i}\mathcal{Y}_i, \quad \mathcal{S}_i^{\mathcal{N}} \setminus \mathcal{W}_i^{\mathcal{N}} \subset \mathrm{int}_{Y' \times V_i}\mathcal{N}_i. \tag{2}$$

By Lemma 3.6 we also know that $\mathcal{S}_i^{\mathcal{U}} \subset X' \times V_i$ is lower dimensional. Hence it is possible to choose a lower dimensional algebraic subset W of X such that for all $i = 1,\ldots,N$

$$\forall \xi \in X' \setminus W : \quad \dim(\mathcal{W}_i^{\mathcal{Y}})_\xi, \dim(\mathcal{W}_i^{\mathcal{N}})_\xi, \dim(\mathcal{S}_i^{\mathcal{U}})_\xi < \dim V_i.$$

This implies by the purity of the μ_i

$$\forall \xi \in X' \setminus W: \quad \begin{array}{lcl} \mu_i(\mathcal{S}_i^{\mathcal{Y}} \setminus \mathcal{W}_i^{\mathcal{Y}})_\xi & = & \mu_i(\mathcal{S}_i^{\mathcal{Y}})_\xi, \\ \mu_i(\mathcal{S}_i^{\mathcal{N}} \setminus \mathcal{W}_i^{\mathcal{N}})_\xi & = & \mu_i(\mathcal{S}_i^{\mathcal{N}})_\xi, \\ \mu_i(\mathcal{S}_i^{\mathcal{U}})_\xi & = & 0. \end{array} \tag{3}$$

Now let us fix some $\xi_0 \in X' \setminus W$. We must show that for every $\epsilon' > 0$

$$\mu \mathcal{S}_{\xi_0} - 2\epsilon' \le 2\epsilon.$$

It is easy to verify that

$$\begin{array}{rcl} \mu \mathcal{S}_{\xi_0} & = & \sum_{i=1}^N \mu_i \mathcal{S}_{\xi_0} \\ & = & \sum_{i=1}^N \mu_i(\mathcal{S}_{\xi_0} \cap V_i) \\ & = & \sum_{i=1}^N \mu_i(\mathcal{S} \cap (X' \times V_i))_{\xi_0} \\ & = & \sum_{i=1}^N \mu_i(\mathcal{S}_i^{\mathcal{Y}})_{\xi_0} + \sum_{i=1}^N \mu_i(\mathcal{S}_i^{\mathcal{N}})_{\xi_0} + \sum_{i=1}^N \mu_i(\mathcal{S}_i^{\mathcal{U}})_{\xi_0} \\ & = & \sum_{i=1}^N \mu_i(\mathcal{S}_i^{\mathcal{Y}} \setminus \mathcal{W}_i^{\mathcal{Y}})_{\xi_0} + \sum_{i=1}^N \mu_i(\mathcal{S}_i^{\mathcal{N}} \setminus \mathcal{W}_i^{\mathcal{N}})_{\xi_0}, \end{array} \tag{4}$$

the latter equality coming from (3). Since every Borel measure on $\mathbb{R}^n$ is regular (cf. [Ha 74, chap. X, § 52]) we can find for $\epsilon' > 0$ *compact* subsets $\mathcal{C}_i^{\mathcal{Y}} \subseteq (\mathcal{S}_i^{\mathcal{Y}} \setminus \mathcal{W}_i^{\mathcal{Y}})_{\xi_0}$, $\mathcal{C}_i^{\mathcal{N}} \subseteq (\mathcal{S}_i^{\mathcal{N}} \setminus \mathcal{W}_i^{\mathcal{N}})_{\xi_0}$ such that

$$\begin{array}{rcl} \sum_{i=1}^N \mu_i \mathcal{C}_i^{\mathcal{Y}} & \ge & \sum_{i=1}^N \mu_i(\mathcal{S}_i^{\mathcal{Y}} \setminus \mathcal{W}_i^{\mathcal{Y}})_{\xi_0} - \epsilon', \\ \sum_{i=1}^N \mu_i \mathcal{C}_i^{\mathcal{N}} & \ge & \sum_{i=1}^N \mu_i(\mathcal{S}_i^{\mathcal{N}} \setminus \mathcal{W}_i^{\mathcal{N}})_{\xi_0} - \epsilon'. \end{array} \tag{5}$$

It remains to bound both left-hand sides by ϵ. Let for $i = 1, \ldots, N$

$$\delta_i^{\mathcal{Y}} := \mathrm{dist}(\{\xi_0\} \times \mathcal{C}_i^{\mathcal{Y}}, (Y' \times V_i) \setminus \mathrm{int}_{Y' \times V_i} \mathcal{Y}_i),$$

$$\delta_i^{\mathcal{N}} := \mathrm{dist}(\{\xi_0\} \times \mathcal{C}_i^{\mathcal{N}}, (Y' \times V_i) \setminus \mathrm{int}_{Y' \times V_i} \mathcal{N}_i)$$

(where by definition $\mathrm{dist}(\emptyset, M) := \mathrm{dist}(M, \emptyset) := \infty$ for $M \subseteq \mathbb{R}^n$), and set

$$\delta := \min \bigcup_{i=1}^N \{\delta_i^{\mathcal{Y}}, \delta_i^{\mathcal{N}}\}.$$

As the distance between a compact set and a closed set is positive if they are disjoint, we conclude from (2) that $\delta > 0$. Hence for all $i = 1, \ldots, N$

$$\forall \xi \in B_{\delta/2}(\xi_0) \cap Y': \ \mathcal{C}_i^{\mathcal{Y}} \subseteq (\mathcal{Y}_i)_\xi, \ \mathcal{C}_i^{\mathcal{N}} \subseteq (\mathcal{N}_i)_\xi. \tag{6}$$

Next observe that $Y'' \setminus X''$ is dense in Y'. Otherwise there were a nonempty open subset U of Y' such that $Y'' \cap U \subseteq X'' \cap U$, hence $U \subseteq X$ since Y'' is dense in Y'. So

$$\dim_\xi Y' \le \dim U \le \dim X$$

for some $\xi \in U$, in contradiction to our assumption $\dim_\xi Y' = \dim Y > \dim X$. Therefore we can choose some $\xi \in B_{\delta/2}(\xi_0) \cap (Y'' \setminus X'')$. For such a point

$$\sum_{i=1}^{N} \mu_i \mathcal{C}_i^{\mathcal{Y}} \leq \sum_{i=1}^{N} \mu_i (\mathcal{Y}_i)_\xi = \sum_{i=1}^{N} \mu_i \mathcal{Y}_\xi = \mu \mathcal{Y}_\xi \leq \epsilon$$

by (6) and the assumption on the tree T.

Likewise, since X'' is dense in X' there is also a point $\xi \in B_{\delta/2}(\xi_0) \cap X''$, hence

$$\sum_{i=1}^{N} \mu_i \mathcal{C}_i^{\mathcal{N}} \leq \sum_{i=1}^{N} \mu_i (\mathcal{N}_i)_\xi = \sum_{i=1}^{N} \mu_i \mathcal{N}_\xi = \mu \mathcal{N}_\xi \leq \epsilon$$

by (6) and the assumption on the tree T. Therefore by (4) and (5)

$$\mu \mathcal{S}_{\xi_0} \leq 2(\epsilon + \epsilon'),$$

as asserted. □

4 Applications

First we compare deterministic and average decision complexity in the situation of k-generic complete intersections ($k \subseteq \mathbb{R}$).

Let $X \subset \mathbb{R}^m$ be an irreducible algebraic subset, $r := \operatorname{codim}_{\mathbb{R}^m} X < m$. We call X a *k-generic complete intersection of r polynomials of degrees $d_1, \ldots, d_r$* if $X = \mathcal{Z}(f_1, \ldots, f_r)$ for some $f_1, \ldots, f_r \in \mathbb{R}[x_1, \ldots, x_m]$ of degrees $d_1, \ldots, d_r$ whose total system of all coefficients is algebraically independent over k (cf. [Bü 92]). In [Bü 92] the (deterministic) additive and multiplicative $\mathbb{R}$-preconditioned branching decision complexity of X have been determined; for instance if $d_1 = \ldots = d_r = d$ then

$$\begin{aligned} C_{\mathbb{R}}(c_{+,\leq}, \{X, \mathbb{R}^m \setminus X\}) &= r \binom{d+m}{m} - r^2, \\ C_{\mathbb{R}}(c_{*,\leq}, \{X, \mathbb{R}^m \setminus X\}) &\sim \frac{1}{2} r \binom{d+m}{m} \quad r, m \text{ fixed}, \ d \to \infty \end{aligned}$$

where the cost functions $c_{+,\leq}, c_{*,\leq} : \Omega^k \sqcup P \to \mathbb{N}$ are defined as $1_{\{+,-,=,\leq\}}$, $1_{\{*,/,=,\leq\}}$, respectively. We compare this now with the average complexity with respect to $c_+ = 1_{\{+,-\}}$ and $c_* = 1_{\{*,/\}}$.

Corollary 4.1 *Let $X \subset \mathbb{R}^m$ be a k-generic complete intersection of r polynomials of the same degree d, $r < m$, $k \subseteq \mathbb{R}$ a subfield. If $\mu : \mathcal{B}(\mathbb{R}^n) \to [0,1]$ is an algebraic probability measure and $\epsilon \in [0,1)$ then*

$$C_{\mathbb{R}}^{(\mu,\epsilon)}(c_+, \{X, \mathbb{R}^m \setminus X\}) \gtrsim (1-2\epsilon)\begin{pmatrix} d+m \\ m \end{pmatrix},$$

$$C_{\mathbb{R}}^{(\mu,\epsilon)}(c_*, \{X, \mathbb{R}^m \setminus X\}) \gtrsim \frac{1}{2}(1-2\epsilon)\begin{pmatrix} d+m \\ m \end{pmatrix}$$

as $d \to \infty$.

Proof. We show the first inequality. Let $\mathcal{O}_{X,\mathbb{R}^m}$ denote the local ring of X, and let $f \in \mathcal{M}_{X,\mathbb{R}^m}$ be nonzero. It follows from [Ma 86, p. 112, Thm. 14.14] that

$$\sqrt{(f, g_2, \ldots, g_r)} = \mathcal{M}_{X,\mathbb{R}^m}$$

if $g_2, \ldots, g_r$ are sufficiently general k-linear combinations of $f_1, \ldots, f_r$. Assume a sequence $\zeta \in \mathbb{R}^s$ to contain all the coefficients of the polynomials $g_2, \ldots, g_r$. Then

$$L_{k\to\mathcal{O}_{X,\mathbb{R}^m}}(c_+, \zeta x, \{f, g_2, \ldots, g_r\}) \leq L_{k\to\mathcal{O}_{X,\mathbb{R}^m}}(c_+, \zeta x, f) + (r-1)\begin{pmatrix} d+m \\ m \end{pmatrix}.$$

The quantity on the left-hand side is bounded from below by the so called verification complexity $\mathrm{VC}_{k\to\mathcal{O}_{X,\mathbb{R}^m}}(c_+, \zeta x, \mathcal{M}_{X,\mathbb{R}^m})$ (cf. [BL 91, Li 90]) which is in [Bü 92] shown to be at least $r(\begin{pmatrix} d+m \\ m \end{pmatrix} - r)$. As $f \in \mathcal{M}_{X,\mathbb{R}^m} \setminus \{0\}$ may be arbitrary this implies

$$\mathrm{EC}_{\mathbb{R}}(c_+, X, \mathbb{R}^m) \geq \begin{pmatrix} d+m \\ m \end{pmatrix} - r^2.$$

So the assertion follows together with Corollary 3.3.

The second inequality follows analogously, using [Bü 92, Thm. 2.5, Prop. 4.3, Lemma 4.7]. □

We are going to design a randomized (Ω^k, P)-decision tree (T, μ) over some $s+m$ for some $\{\zeta\} \times X \subset \{\zeta\} \times \mathbb{R}^m (\subset \mathbb{R}^s \times \mathbb{R}^m)$. Let $\epsilon \in (0,1)$ be given, put $M := \lceil (r-1)\epsilon^{-1} \rceil$ and choose sufficiently general k-linear combinations $F_1, \ldots, F_M$ of the polynomials $f_1, \ldots, f_r$ with the property that every choice of r polynomials among $F_1, \ldots, F_M$ has X as its zeroset. As probability measure μ we take the uniform distribution on $\{1, \ldots, M\} \subset \mathbb{R}$ which is algebraic. Choose $s \in \mathbb{N}$ and $\zeta \in \mathbb{R}^s$ such that for all $i = 1, \ldots, M$

$$L_{k\to\mathbb{R}[x]}(c_+, \zeta x, F_i) \leq \begin{pmatrix} d+m \\ m \end{pmatrix} - 1.$$

We describe the action of T over $s+m+1$ in an informal way: Given an input $(\zeta, \xi, \rho) \in \{\zeta\} \times \mathbb{R}^m \times \mathbb{R}$, it is first decided whether $\rho \in \{1, \ldots, M\}$, and if so, $i \in \{1, \ldots, M\}$ with $\rho = i$ is found. (This can be done using a bisection subtree with $M+1$ leaves, one leaf for the case $\rho \notin \{1, \ldots, M\}$, and M leaves for the cases $\rho \in \{1, \ldots, M\}$.) If $\rho \notin \{1, \ldots, M\}$ is found the algorithm stops and answers "yes"(say). If $\rho \in \{1, \ldots, M\}$ is found the algorithm computes $F_\rho(\xi)$, checks whether $F_\rho(\xi) = 0$, replies "yes" if so and "no" if not.

By construction each $\xi \notin X$ is a zero of at most $r-1$ of the $F_1, \ldots, F_M$. Therefore (T, μ) decides membership in $\{\zeta\} \times X$ relative to $\{\zeta\} \times \mathbb{R}^m$ with error probability $(r-1)M^{-1} \leq \epsilon$. So

$$C_{\mathbb{R}}^{(\mu,\epsilon)}(c_{+,\leq}, \{X, \mathbb{R}^m \setminus X\}) \leq \log_2 \frac{r-1}{\epsilon} + 2 + \begin{pmatrix} d+m \\ m \end{pmatrix}.$$

In a similar way one obtains for $d \to \infty$

$$C_{\mathbb{R}}^{(\mu,\epsilon)}(c_{*,\leq}, \{X, \mathbb{R}^m \setminus X\}) \leq \log_2 \frac{r-1}{\epsilon} + (1+o(1))\frac{1}{2} \begin{pmatrix} d+m \\ m \end{pmatrix}.$$

Thus randomization may reduce decision complexity by about a factor of r in this case, and the lower bound in Corollary 4.1 cannot essentially be improved if no further condition on (μ, ϵ) is imposed, even if one replaces the cost functions c_+ resp. c_* by $c_{+,\leq}$ resp. $c_{*,\leq}$.

For the rest of this section we assume $k = \mathbb{R}$. The next result is inspired by [BS 83] and is similar to [Li 90, (V.3)]:

Proposition 4.2 *Let $X \subseteq \mathbb{R}^m$ be an irreducible algebraic subset with the property that every restriction to X of any coordinate projection $\mathbb{R}^m \to H$ onto a coordinate plane H of dimension d dominates H. Then*

$$\mathrm{EC}(c_{+,*}, X, \mathbb{R}^m) \geq d$$

where $c_{+,*} = 1_{\{+,-,*,/\}}$.

Proof. It suffices to show that

$$L_{k \to \mathcal{O}_{X,\mathbb{R}^m}}(c_{+,*}, x, f) \geq |\{i \in \{1, \ldots, m\} : \partial_i f \neq 0\}| - 1$$

for every $f \in \mathcal{M}_{X,\mathbb{R}^m} \setminus \{0\}$.

In doing so, let $A := \mathbb{R}[x_1, \ldots, x_m]$ and $S \subset A \setminus \{0\}$ be an arbitrary multiplicative system. Let $\Gamma = (\Gamma_1, \ldots, \Gamma_t)$ be an Ω^k-straight line program over m which is executable on the standard input (A_S, x) having result sequence

$$(x_1, \ldots, x_m, r_1, \ldots, r_t) \in A_S^{m+t}.$$

We show by induction on t the following: If Γ computes some $f \in A_S$ on input (A_S, x) then

$$c_{+,*}\text{-length of } \Gamma \geq |\{i \in \{1, \dots, m\} : \partial_i f \neq 0\}| - 1. \tag{7}$$

This is true for $t = 0$. For $t \geq 1$ let $\Gamma' = (\Gamma'_2, \dots, \Gamma'_t)$ denote the Ω^k-straight line program over $m + 1$ obtained from Γ by deleting the first instruction Γ_1 and replacing in all successor instructions calls to the result of the first instruction by calls to a additional new input component. Let $A' := \mathbb{R}[x_0, \dots, x_m]$, and let $S' \subset A' \setminus \{0\}$ denote the preimage of $A_S^\times$ under the substitution

$$\sigma : A' \to A_S, \quad x_0 \mapsto r_1$$

extending $A \to A_S$. By construction Γ' is executable on the standard input $(A'_{S'}, x')$ of length $m + 1$ and computes some $f' \in A'_{S'}$ with $\sigma_{S'}(f') = f$; here $\sigma_{S'} : A'_{S'} \to A_S$ denotes the k-algebra morphism induced by σ. By the inductive hypothesis

$$c_{+,*}\text{-length of } \Gamma' \ \geq |\{i \in \{0, \dots, m\} : \partial_i f' \neq 0\}| - 1. \tag{8}$$

Observe that by the chain rule

$$\partial_i f = \sigma_{S'}(\partial_i f') + \sigma_{S'}(\partial_0 f') \cdot (\partial_i r_1) \quad (i \geq 1) \tag{9}$$

and that

$$c_{+,*}\text{-length of } \Gamma \in (c_{+,*}\text{-length of } \Gamma') + \{0, 1\}.$$

Now (7) follows from (8) by discussing for every $\omega_1 \in \Omega^k$ the case that r_1 results in instruction Γ_1 from an application of ω_1. If $\partial_0 f' = 0$ then all $\partial_1 f, \dots, \partial_m f$ are the images of $\partial_1 f', \dots, \partial_m f'$ under $\sigma_{S'}$ (by (9)), and (8) implies (7). If $\partial_0 f' \neq 0$ then at least $m - \mathrm{ar}(\omega_1)$ many among $\partial_1 f, \dots, \partial_m f$ are nevertheless images of the respective ones among $\partial_1 f', \dots, \partial_m f'$ due to the fact that $m - \mathrm{ar}(\omega_1)$ many among the $\partial_1 r_1, \dots, \partial_m r_1$ are zero. In this case (7) follows from (8) using $\partial_0 f' \neq 0$ and

$$c_{+,*}\text{-length of } \Gamma = c_{+,*}\text{-length of } \Gamma' + 1 \Leftrightarrow \mathrm{ar}(\omega_1) = 2. \ \square$$

This result allows us to determine the exclusion complexity $\mathrm{EC}(c_{+,*}, X, \mathbb{R}^{2m})$ of the graph X of *all* elementary symmetric functions exactly: If

$$x_{i_1}, \dots, x_{i_s}, \sigma_{i_{s+1}}, \dots, \sigma_{i_m} \in \mathbb{R}[x_1, \dots, x_m]$$

is any choice of m elements in

$$\{x_1, \dots, x_m, \sigma_1, \dots, \sigma_m\}$$

then they are algebraically independent over $\mathbb{R}$. To see this, note that both

$$\{x_1, \ldots, x_m\} \text{ and } \{\sigma_1, \ldots, \sigma_m\}$$

constitute transcendence bases of $\mathbb{R}(x)$ over $\mathbb{R}$. So if $\sigma_{i_{s+1}}, \ldots, \sigma_{i_m}$ are chosen then there are $x_{j_1}, \ldots, x_{j_s}$ extending these to a trancendence basis. Now, by the action of the symmetric group $S_m \subset \mathrm{Aut}(\mathbb{R}(x)/\mathbb{R})$ we may assume that

$$j_1 = i_1, \ldots, j_s = i_s.$$

Therefore by Proposition 4.2 $\mathrm{EC}(c_{+,*}, X, \mathbb{R}^{2m}) \geq m$. By looking at the graph of σ_1 we see that this is even an equality.

COROLLARY 4.3 *For every algebraic probability measure μ on some $\mathbb{R}^n$ and $\epsilon \in [0,1)$ we have for the graph $X \subset \mathbb{R}^{2m}$ of all elementary symmetric functions*

$$C_{\mathbb{R}}^{(\mu,\epsilon)}(c_{+,*}, \{X, \mathbb{R}^{2m} \setminus X\}) \geq (1-2\epsilon)(m-1).$$

So the procedure in Example 2 cannot essentially be improved. By contrast, the membership problem of the graph of one single middle elementary symmetric function is more difficult, already for the cost function $c_* = 1_{\{*,/\}}$. In the case of hypersurfaces exclusion complexity and verification complexity coincide (cf. [Li 90, (E.1.5.1), p. 107]). The proof of the subsequent two corollaries is an immediate consequence of Corollary 3.3 and the lower bounds on verification complexity proved in [Li 90, p. 136, (D.5) and p. 174, (L.4), respectively].

COROLLARY 4.4 *Let*

$$X := \{(\xi, \zeta) : \zeta = \sigma_{\lfloor m/2 \rfloor}(\xi)\} \subset \mathbb{R}^{m+1}$$

be the graph of the middle elementary symmetric function. Then for every algebraic probability measure μ on some $\mathbb{R}^n$ and $\epsilon \in [0,1)$ we have

$$C_{\mathbb{R}}^{(\mu,\epsilon)}(c_*, \{X, \mathbb{R}^{m+1} \setminus X\}) \geq \mathrm{const.}\,(1-2\epsilon) m \log m.$$

COROLLARY 4.5 *For every algebraic probability measure μ on some $\mathbb{R}^n$ and $\epsilon \in [0,1)$ we have*

$$C_{\mathbb{R}}^{(\mu,\epsilon)}(c_*, \{\mathrm{SL}(m,\mathbb{R}), \mathbb{R}^{m\times m} \setminus \mathrm{SL}(m,\mathbb{R})\}) \geq \mathrm{const.}\,(1-2\epsilon) m^{\omega},$$

$$C_{\mathbb{R}}^{(\mu,\epsilon)}(c_+, \{\mathrm{SL}(m,\mathbb{R}), \mathbb{R}^{m\times m} \setminus \mathrm{SL}(m,\mathbb{R})\}) \geq \mathrm{const.}\,(1-2\epsilon) m^{\omega}$$

where ω denotes the asymptotic exponent of matrix multiplication.

We remark that by Theorem 3.1 the lower bounds in the above three corollaries remain true if the partitions $\{X, \mathbb{R}^N \setminus X\}$ (N suitable) are replaced by the partitions $\{X(\mathbb{Q}), \mathbb{Q}^N \setminus X(\mathbb{Q})\}$ of respective $\mathbb{Q}$-rational points. This also holds for determinant varieties: Let $r < s \leq p \leq q$, and let $X_r \subset X_s \subseteq \mathbb{R}^{p\times q}$ denote the subsets of matrices of rank $\leq r$ resp. $\leq s$. Note that

$$\overline{X_r(\mathbb{Q})} = X_r = \mathrm{Cent} X_r \subset \mathrm{Cent} X_s = X_s = \overline{X_r(\mathbb{Q})}.$$

COROLLARY 4.6 *Let $r < s \leq p \leq q$, and let $X_r(\mathbb{Q}) \subset X_s(\mathbb{Q}) \subseteq \mathbb{Q}^{p\times q}$ denote the subsets of matrices of rank $\leq r$ resp. $\leq s$. Then for every algebraic probability measure μ on some $\mathbb{R}^n$ and $\epsilon \in [0,1)$ we have*

$$C_{\mathbb{R}}^{(\mu,\epsilon)}(c_*, \{X_r(\mathbb{Q}), X_s(\mathbb{Q}) \setminus X_r(\mathbb{Q})\}) \geq \mathrm{const.}\,(1-2\epsilon)r^2.$$

The proof follows from Theorem 3.1 together with [Li 90, (E.1.7.1), p. 112 and (V.3), p. 167].

Acknowledgements

The first and the third author wish to express their sincere thanks to the Schweizerischer Nationalfonds and the Deutsche Forschungsgemeinschaft (Heisenberg-Grant Li 405/2-1) for their financial supports.

References

[BS 83] W. BAUR AND V. STRASSEN, The complexity of partial derivatives, Theoret. Comput. Sci.**22** (1983), pp. 317–330.

[Be 83] M. BEN–OR, Lower bounds for algebraic computation trees, *Proc. 15th ACM STOC*, Boston (1983), pp. 80–86.

[BCR 86] J. BOCHNAK, M. COSTE, AND M.-F. ROY, *Géométrie algébrique réelle*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band **12**, Springer Verlag, 1987.

[Bü 92] P. BÜRGISSER, Decision complexity of generic complete intersections, Research Report No. 8578-CS, Univ. Bonn, 1992; submitted to *Computational Complexity*.

[BL 91] P. Bürgisser and T. Lickteig, Verification complexity of linear prime ideals, to appear in *J. Pure and Applied Algebra*, 1992.

[BLS 90] P. Bürgisser, T. Lickteig, and M. Shub, Test complexity of generic polynomials, to appear in *Journal of Complexity*, 1992.

[Fr 89] R. Freivalds, Fast Probabilistic Algorithms, *LNCS* **74** (1979), Springer Verlag, pp. 57–69.

[Ha 74] P. R. Halmos, *Measure Theory*, Graduate Texts in Mathematics **18**, Springer Verlag, 1974.

[Hi 91] M. D. Hirsch, Lower bounds for the non-linear complexity of algebraic computation trees with integer inputs, *Computational Complexity* **1** (1991), pp. 257–268.

[Ka 90] R. M. Karp, An introduction to randomized algorithms, Tech. Rep. TR-90-024, Int. Comp. Science Inst., Berkeley (1990).

[KV 87] M. Karpinski and R. Verbeek, Randomness, provability and the separation of the Monte Carlo time and space, *LNCS* **270** (1987), pp. 189–207.

[KS 89] M. Knebusch and C. Scheiderer, *Einführung in die reelle Algebra*, Vieweg-Studium 63: Aufbaukurs Mathematik, Vieweg, 1989.

[Li 90] T. Lickteig, On semialgebraic decision complexity, Tech. Rep. TR-90-052 Int. Comp. Science Inst., Berkeley (1990), and Univ. Tübingen, Habilitationsschrift.

[Ma 86] H. Matsumura, *Commutative ring theory*, Cambridge studies in advanced mathematics **8**, Cambridge University Press, 1986.

[MRR 90] J. L. Montaña, L. M. Pardo, and T. Recio, The non-scalar model of complexity in computational geometry, in: *Proceedings of the symposium "MEGA-90 – Effective Methods in Algebraic Geometry"* (1990), Castiglioncello (Livorno, Italy), pp. 347–361.

[St 83] V. Strassen, The computational complexity of continued fractions, *SIAM J. Comp.* **12/1** (1983), pp. 1–27.

[Ya 89] A. C. C. Yao, Lower bounds for algebraic computation trees with integer inputs, *SIAM J. Comp.* **20** (1989), pp. 655–668.