ELSEVIER

Journal of Pure and Applied Algebra 110 (1996) 131–184

JOURNAL OF PURE AND APPLIED ALGEBRA

Semi-algebraic decision complexity, the real spectrum, and degree

Thomas Lickteig *

Institut für Informatik, Universität Bonn, 53117 Bonn, Germany

Communicated by M.F. Roy; received 5 September 1994; revised 15 April 1995

Abstract

Semi-algebraic decision complexity introduces a quantitative finiteness aspect into semi-algebraic geometry. In this paper we combine methods from abstract real algebraic geometry and complexity theory in order to show lower bounds on the arithmetical cost of semi-algebraic decision trees. In contrast to the topological combinatorial methods the approach is local and based on the relations computed along paths distinguished by certain well defined points in the real spectrum of the polynomial ring $R[X_1,\ldots,X_n]$. We describe the theme of semi-algebraic decision trees entirely from the point of view of the concept of the real spectrum which extracts the local "quintessence" of the behavior of decision trees. Together with the degree argument – introduced into complexity theory by Strassen [46] – we obtain bounds that apply to concrete natural problems, and their range of application complements the one of topologically based lower bounds. Various new applications to test problems around interpolation (solvability of overdetermined interpolation tasks) and Chinese remaindering are included.

Having a lower bound on decision complexity of a semi-algebraic subset $E \subset R^n$ a further question naturally arises: Is the set of inputs from R^n producing a long path in a decision tree "significant," or is it only an unspecified exceptional set of possibly very low dimension? Unlike the topological combinatorial methods the real spectrum approach provides such information. For instance, if E is an irreducible algebraic set then the subset of points in E producing a short path has dimension strictly less than the dimension of E.

We discuss complexity questions throughout from the variable and relative standpoint.

Keywords: Straight line programs; Decision trees; Real spectrum; Degree method; Derivations

1991 Math. Subj. Class.: 68Q05, 68Q25, 68Q40, 14P10

* E-mail: lickteig@cs.uni-bonn.de. Supported by DFG Heisenberg Grant Li-405/2-1.
Dedicated to the memories of Siegfried Breitsprecher and Jacques Morgenstern.

SSDI 0022-4049(95)00105-0

1. Introduction

In a paper of great originality, Strassen [46] introduced the concept of geometric degree into the field of numerical and algebraic algorithms to prove *lower bounds* on the complexity of computing polynomials and rational functions (see also [41, 39, 1]). His method (cf. [47]) also gives lower bounds $\log_2 \deg E$ on testing membership in an irreducible algebraic subset $E \subset R^n$ (R an algebraically closed field) with algebraic decision trees (only $=$-branching); for an interesting application see [42].

If R is a real closed field $\leq$-branching can be included too, and then the situation is different. Ben-Or [4] pointed out a way to use the degree argument for semi-algebraic decision trees ($\leq$-branching included) and proved a lower bound on the decision complexity in terms of $\log_2 \sharp E$ where $\sharp E$ denotes the number of semi-algebraically connected components of the semi-algebraic subset $E \subset R^n$; here the degree argument comes in via a result by Milnor [29] and Thom [48] which has been already used in previous work by Steele and Yao [43]. Throughout this paper the term *decision tree* (algebraic or semi-algebraic) is always understood in the unrestricted sense of a computation tree with a Boolean output alone.

Subsequently the work of several authors has concentrated on generalizing and refining Ben-Or's method to connected but nevertheless *topologically complicated* sets E. Montaña et al. [32] use intersections with low-degree polynomials to produce many connected components. Björner and Lovász [6], Björner, et al. [7], and Yao [51, 52] relate ranks of higher homology groups to the decision complexity (see also [20]). For topological lower-bound methods in the parallel model the reader is referred to the new developments by Montaña and Pardo [31] and Montaña et al. [30]. In [16] Grigoriev, et al. give a new "number of cases" lower bound for testing membership in a polyhedron based on the number of facets.

As pointed out in [24] all lower-bound results known so far are grosso-modo based on degree and differential techniques (see [29, 48], and the bounds based on transcendence degree and on the rank of an imperfection module in [12, 11] under this aspect). In this paper, which presents part of [24], we also use these basic concepts, degree and derivations, the latter in the complexity theoretic form of the remarkable theorem of Linnainmaa [26] (communicated to the author by Erich Kaltofen), Baur and Strassen [2] (see also Morgenstern [34]; for a parallel complexity analysis see [21]). In this way extensions of Strassen's degree method to semi-algebraic decision trees are possible.

The classical scenario in algebraic complexity theory is as follows. Assume a fixed R-algebra A (traditionally a rational function field), $x \in A^n$, and $f \in A^m$ to be given. The question is: Which are the straight line programs computing f from the input vector x, and what can be said about their number of computational steps (or result sequence)? Hereby the straight line programs are assumed to be executable on x, that is, no divisions by non-units in A occur. Considering paths in decision trees leads to a "dual" scenario turning the straight line program into the object of departure, the input vector into the "varying quantity," and assumptions about executability into questions:

How does the outcome of the tests along a path vary if for different ordered extension fields $(K, \leq)$ of R vectors $x \in K^n$ (rather than $x \in R^n$) are taken as inputs? Having such an information, which R-algebras A and $x \in A^n$ can be assigned such that the computational steps along the path are executable on x, and which sort of elements in A is computed? Which paths are "informative," assuming the decision tree to decide membership in a semi-algebraic subset $E \subset R^n$?

These questions suggest a line for proving lower bounds consisting of two main steps:

(a) Establish a transition from the set $E \subset R^n$ and the decision tree to certain well-defined R-algebras and computations in these algebras producing elements of particular type.

(b) Use algebraic methods to prove lower bounds on the cost of computing such elements.

The main tool for achieving the first goal is the notion of the *real spectrum*, the fundamental concept for real algebraic geometry introduced by M. Coste and M.F. Roy. Like for the Zariski spectrum, real geometry and real algebra appear in this concept as two sides of one thing. The real spectrum can also play the role of a "dictionary" between geometric and algebraic properties, and for that reason it is central in our treatment of semi-algebraic decision trees.

Since the theme of algorithmic complexity is situated on the border line between mathematics and computer science we now first give some explanations about this very young and so far not widely known notion. It establishes a fusion of ideas from the Zariski spectrum of a ring and from Artin–Schreier theory. (More comments on main ideas, their geometric signification and examples with illustrations can be found in the appendix. For a detailed introduction to this chic theory due to Coste and Roy the reader is referred to the books by Bochnak et al. [8], Knebusch and Scheiderer [22], and the article by Becker [3].) Let A be a commutative ring. A subset $\alpha \subset A$ is called a *prime cone* if it satisfies the following conditions:

(i) $a \in \alpha, b \in \alpha \Rightarrow a + b \in \alpha$,
(ii) $a \in \alpha, b \in \alpha \Rightarrow a \cdot b \in \alpha$,
(iii) $a \in A \Rightarrow a^2 \in \alpha$,
(iv) $-1 \notin \alpha$,
(v) $a \cdot b \in \alpha \Rightarrow a \in \alpha$ or $-b \in \alpha$.

(Note that this definition generalizes the notion of a positive cone of an ordering of a field. It also generalizes the notion of a point in R^n; see below). Prime cones are the real counterpart of prime ideals and form the points of the *real spectrum* $\mathrm{Spec}_r A$ of the ring A. Analogously as for the Zariski spectrum $\alpha \in \mathrm{Spec}_r A$ is called a *generization* of $\beta \in \mathrm{Spec}_r A$, and β a *specialization* of α, if $\alpha \subseteq \beta$. It is not hard to see from the definition that α is a prime cone if and only if

$$\alpha + \alpha \subseteq \alpha, \quad \alpha \cdot \alpha \subseteq \alpha, \quad \alpha \cup (-\alpha) = A,$$

$\mathfrak{p} = \alpha \cap (-\alpha)$ is a prime ideal of A.

The prime ideal $\mathfrak{p} = \alpha \cap (-\alpha)$ is called the *support* of α and is denoted $\operatorname{supp}\alpha$. This gives rise to an equivalent representation of prime cones. Let $r_\mathfrak{p} : A \to k(\mathfrak{p}) = Fr(A/\mathfrak{p})$ denote the canonical homomorphism to the residue field of $\mathfrak{p}$. Then α induces an ordering $\leq_\alpha$ on the residue field $k(\mathfrak{p})$ defined by

$$r_\mathfrak{p}(a)/r_\mathfrak{p}(b) \geq_\alpha 0 \iff ab \in \alpha \quad \text{for } a, b \in A, b \notin \mathfrak{p}.$$

(Note that if A is already a field then $\mathfrak{p} = 0$, and α is exactly the positive cone of an ordering on A.) Reversely, any ordering $\leq$ on $k(\mathfrak{p})$ defines uniquely a prime cone

$$\alpha = r_\mathfrak{p}^{-1}(\{\kappa \in k(\mathfrak{p}) : \kappa \geq 0\}).$$

Hence, a prime cone α can be identified with the pair $(\operatorname{supp}\alpha, \leq_\alpha)$. Using this second representation of prime cones allows to consider elements $a \in A$ as functions

$$\alpha \mapsto a(\alpha) = r_{\operatorname{supp}\alpha}(a)$$

on the real spectrum $\operatorname{Spec}_r A$ with values in all possible ordered residue fields $(k(\operatorname{supp}\alpha), \leq_\alpha)$; one writes $a(\alpha) \geq 0$ if $r_{\operatorname{supp}\alpha}(a) \geq_\alpha 0$, or equivalently, if $a \in \alpha$. Finally, the topology of the real spectrum of A is given by the basis open sets

$$\tilde{\mathcal{U}}(a_1, \ldots, a_k) = \{\alpha \in \operatorname{Spec}_r A : a_1(\alpha) > 0, \ldots, a_k(\alpha) > 0\},$$

where $a_1, \ldots, a_k$ is an arbitrary finite family of elements in A. A subset $\mathscr{C} \subseteq \operatorname{Spec}_r A$ is called *constructible* if it is a Boolean combination of such basis open sets $\tilde{\mathcal{U}}(a_1, \ldots, a_k)$. $\mathscr{C}$ is open (closed) iff it is stable under generization (specialization). A point (prime cone) $\alpha \in \mathscr{C}$ is said to be a minimal point of $\mathscr{C}$ (cf. [22]) if $\mathscr{C}$ contains no proper generization $\beta \subset \alpha$, a maximal point of $\mathscr{C}$ if $\mathscr{C}$ contains no proper specialization $\beta \supset \alpha$. Since in this paper the word "point" will be used in a different context we will speak throughout of minimal (maximal) prime cones rather than of minimal (maximal) points.

We now pass to the geometric situation when $A = R[X_1, \ldots, X_n]$ is a polynomial ring. The evaluation of polynomials in a point $\xi \in R^n$ defines the maximal ideal

$$\mathfrak{m}_\xi = \{f \in R[X] : f(\xi) = 0\} \in \operatorname{Spec} R[X]$$

with real closed residue field $k(\mathfrak{m}_\xi) = R$ and therefore a uniquely determined prime cone

$$\alpha_\xi = \{f \in R[X] : f(\xi) \geq 0\} \in \operatorname{Spec}_r R[X].$$

Since $\mathfrak{m}_\xi$ is a maximal ideal α_ξ is a maximal prime cone of $\operatorname{Spec}_r R[X]$. The points $\xi \in R^n$ are thus naturally embedded into the real spectrum $\operatorname{Spec}_r R[X]$ which can be considered as an enrichment of the Euclidean space R^n with further "non-standard" points. To a constructible subset $\mathscr{C} \subseteq \operatorname{Spec}_r R[X]$ we can assign its "standard" part $C = \mathscr{C} \cap R^n$ which is a *semi-algebraic* subset of R^n; if $\mathscr{C}$ is a Boolean combination of certain basis open sets $\tilde{\mathcal{U}}(f_1, \ldots, f_k)$, where $f_i \in R[X]$, then C is the *same* combination of the open sets with respect to the Euclidean topology

$$\mathcal{U}(f_1, \ldots, f_k) = \{\xi \in R^n : f_1(\xi) > 0, \ldots, f_k(\xi) > 0\}.$$

It is a crucial fact that this process is reversible. If $C \subseteq R^n$ is semi-algebraic then there is one and only one constructible $\tilde{C} \subseteq \mathrm{Spec}_r R[X]$ with $C = \tilde{C} \cap R^n$. This assignment, called *operation tilde*, establishes an isomorphism of Boolean algebras

$$\{\text{semi-algebraic sets}\} \to \{\text{constructible sets}\}, \quad C \mapsto \tilde{C}.$$

This correspondence is an equivalent form of the transfer principle. From a description of C one obtains a description of $\tilde{C}$ as above but in the reverse direction; the place where model theory (e.g. [36, 37]) enters is the independence of the description. $\tilde{C}$ encompasses the full information of solutions in arbitrary real closed extension fields rather than the solution set $C \subset R^n$, a first-order formula with parameters in R – a description of C – being given.

In the case of the polynomial ring $R[X_1, \ldots, X_n]$ there is a third way of coding prime cones $\alpha \in \mathrm{Spec}_r R[X]$ as "vectors" in various ordered residue fields which allows to view them as inputs for decision trees. Let $X = (X_1, \ldots, X_n) \in R[X]^n$. If $\mathfrak{p} \subset R[X]$ is a prime ideal then X assigns to $\mathfrak{p}$ the image vector $X(\mathfrak{p}) = (X_1(\mathfrak{p}), \ldots, X_n(\mathfrak{p}))$ in $k(\mathfrak{p})^n$; vice versa, $r_{\mathfrak{p}} : R[X] \to k(\mathfrak{p})$ and hence its kernel can be "reconstructed" from $X(\mathfrak{p})$ since $k(\mathfrak{p})$ is generated over R by the elements $X_1(\mathfrak{p}), \ldots, X_n(\mathfrak{p}) \in k(\mathfrak{p})$. Hence, $\alpha = (\mathfrak{p}, \leq)$ is uniquely represented by the ordered field "point" over R given by the pair $(X(\mathfrak{p}), \leq)$.

Now we return to decision complexity. Assume $\mathscr{T}$ to be a decision tree for membership in a semi-algebraic subset $E \subset R^n$. Via the identification $\alpha = (X(\mathrm{supp}\,\alpha), \leq_\alpha)$ every prime cone $\alpha \in \mathrm{Spec}_r R[X]$ can be fed into $\mathscr{T}$, and by the tilde, $\mathscr{T}$ decides also membership in $\tilde{E} \subset \mathrm{Spec}_r R[X]$. For simplicity, let us first assume that E is an irreducible algebraic set with vanishing ideal $\mathfrak{p}$ (for semi-algebraic E see below). If $\mathrm{supp}\,\alpha = \mathfrak{p}$ then α belongs to $\tilde{E}$, and every proper generization $\beta \subset \alpha$ belongs to $\tilde{R^n} \setminus \tilde{E}$ since the prime ideal $\mathrm{supp}\,\beta$ is a proper generization of $\mathfrak{p} = \mathrm{supp}\,\alpha$. Therefore, its path $\mathscr{T}_\beta$ will be different from $\mathscr{T}_\alpha$. Consequently, the path $\mathscr{T}_\alpha$ followed by α provides a "verifying control calculation" for the question

$$\text{“}\alpha \stackrel{?}{=} \beta\text{”}$$

in the halo $\mathrm{hal}\,\alpha = \{\beta : \beta \subseteq \alpha\}$ of generizations of α ($\mathrm{hal}\,\alpha$ is the closure $\underline{\alpha}$ of α in the inverse spectral space [22]). That means, for every $\beta \subset \alpha$ there will be comparisons in $\mathscr{T}_\alpha$ witnessing the fact $\beta \neq \alpha$. The operational-relational complexity of verifying α (that is, arithmetic and comparison steps are needed and charged) is closely related to the operational complexity of computing a cheapest set of functions in the localization $R[X]_{\mathfrak{p}}$ whose zero-set in the halo of α is α; we call the latter the isolation complexity of α. In this way we get lower bounds on the arithmetical cost along $\mathscr{T}_\alpha$ alone. A further feature of this local approach is the fact that it bounds the cost along *concrete* paths unlike the above-mentioned topological bounds which have global character in the sense of an overall balance on all paths. Therefore, information on the dimensionality of the set of points in R^n producing a long path is automatic; again by the tilde, for all $\alpha \in \mathrm{Spec}_r R[X]$ the set of points in R^n following the path $\mathscr{T}_\alpha$ contains a semi-algebraic

subset of dimension $\dim(\operatorname{supp}\alpha)$. The tilde provides even more precise information. The set of points in E producing a shorter path than a common lower bound on the isolation complexities of all $\alpha \in \tilde{E}$ with support $\mathfrak{p}$ is a subset of dimension strictly less than $\dim E = \dim \mathfrak{p}$. As a consequence of focusing on the cost of "equations for α" as a source of complexity, problems can be treated that are topologically simple. The most evident example is the hypersurface of the Newton sum equation $\sum X_i^q = 1$, q even, which is topologically nothing but a sphere; here the lower bound is of order $n \log_2 q$.

If $\operatorname{ht}\mathfrak{p} = 1$ (E a hypersurface) then the isolation complexity is independently of α given by the minimum cost of computing a parameter of the real discrete valuation ring $R[X]_{\mathfrak{p}}$. For this case we give a degree-derivation bound on the isolation complexity. As mentioned above, the complexity theoretic ingredients for this bound are the Linnainmaa–Baur–Strassen Theorem and Strassen's step by step bounding of degrees along a computation which must however be complemented with further "non-computational" degree bounding arguments. If $\operatorname{ht}\mathfrak{p} > 1$ then one can choose a real prime ideal $\mathfrak{q} \subset \mathfrak{p}$ such that $(R[X]/\mathfrak{q})_{\mathfrak{p}}$ is a real discrete valuation ring and shrink the halo of α by passing to the halo in $\operatorname{Spec}_r(R[X]/\mathfrak{q})_{\mathfrak{p}}$; then a similar degree-derivation bound applies. (For an other method see [11]). Although the *discrete* valuation ring property is at present a *conditio sine qua non* for these bounds it can be expected that generalizations are possible (for instance, with valuation ring methods). On the other hand, there are several reduction techniques extending the range of applications of these bounds (see also [25]). (It remains unknown whether Strassen's $\log_2 \deg E$ bound does also hold true for isolation complexity of prime cones α with $\operatorname{supp}\alpha = \mathfrak{p}$. A further open question is whether the isolation complexity of α does only depend on $\operatorname{supp}\alpha$.)

In the case of a decision tree $\mathscr{T}$ for a semi-algebraic $E \subset R^n$ the focus is on the paths $\mathscr{T}_\alpha$ of minimal prime cones $\alpha \in \tilde{E}$; by the minimality, $\mathscr{T}_\alpha$ must verify α in its halo of generizations. This property is intrinsic and a common behavior of all decision trees for E while their behavior on non-minimal prime cones $\alpha \in \tilde{E}$, in particular on points of E, may be individual. In short, the behavior of the tree $\mathscr{T}$ on the set of minimal prime cones $\tilde{E}^{\min}$ is decisive which is not visible on the level of semi-algebraic sets. This underlines once more the fundamental significance of the concept of the real spectrum. As has been pointed out by E. Becker, the complexity theme gives the space $\tilde{E}^{\min}$ (cf. [22]) an important role. These are the reverse ends of the maximal chains of specializations ([8]) in $\tilde{E}$, called spears in [22], while the space of their tips $\tilde{E}^{\max}$ plays already the role of a natural compactification of E. If $\alpha \in \tilde{E}$ has support 0 (appearing if and only if $\dim E = n$) then α has no proper generizations, and verification of α provides no information. Generally, the symmetric view of a decision problem as a partition $\{E, E'\}$, $E' = R^n \setminus E$, is more adequate. Then the boundary of E yields the complexity creating set $((\bar{E} \cap \bar{E}')^{\sim})^{\min}$ which of course coincides with $\tilde{E}^{\min}$ iff $\dim E < n$. This is also the critical set for partions which are not "full," that is $E \cup E' \neq R^n$; $\bar{E} \cap \bar{E}'$ is then the common boundary of E and E'.

Such partions (decision problems) naturally arise when the inputs from R^n are actually outputs of computational preprocesses. Although not directly related with our theme, we would like to mention that a main step in Artin's classical solution of Hilbert's 17th problem can be considered as the passage to minimal prime cones (orderings of the rational function field), it appears also recently as a step in the Bröcker–Scheiderer theory.

Let us now summarize the organization of this paper.

As explained above, straight line programs for computations in commutative algebras will be primary objects of consideration. In Section 2 we start with some precisions on this basic computational notion. According to the very old song in computer science education of separating syntax and semantics we make a strict distinction between these syntactical objects which can be executed in any R-algebra and their result sequences. Inputs and result sequences are arbitrary *points over* R (vectors in various R-algebras); as indicated at the beginning (tentative) execution of a straight line program Γ on input vectors in different R-algebras, executability–non-executability (units–non-units) will be the source for getting information about Γ. We also discuss the heterogeneous view of Birkhoff and Lipson [5] and the variable point of view with respect to coefficients. The latter, that is to say the category **flac** of arrows of commutative rings rather than the category of commutative R-algebras (R fixed), provides more freedom and a comfortable ground with a suitable definition of morphisms. This is important for separating canonical arguments on the basis of an application of a morphism from the various "reduction techniques," notably those of transfer type, to be subsumed under the key word *partial morphism* in **flac**. (In fact, many ad hoc considerations in complexity theory become "natural" only in **flac**; see [24, 25].)

To make the paper self-contained we recall in Section 3 Strassen's degree method together with an arsenal of classical techniques for bounding degrees. Degree is a classical notion for algebraic sets, algebraically based on dimension and multiplicity theory. However, departing from the execution of a straight line program we find ourselves completely on the algebraic side. Thus, defining degree directly for points over fields rather than the more traditional style of associating algebraic sets is somewhat more flexible since it is closer to the objects under discussion. We describe Strassen's degree method entirely within the framework of such points. Executability conditions directly translate into non-zero divisor conditions, and classical degree bounding techniques (including coefficient reduction) simply appear as degree inequalities between points over different fields.

In Section 4 we equip straight line programs with additional comparison instructions and discuss what they verify in a general fashion. These "verifiers" essentially constitute the paths in decision trees. We start the discussion with verification of "abstract" points which directly gives the connection to certain operational complexities by focusing on "equational consequences." Later on the tilde will be used to establish the bridge to semi-algebraic decision complexity. The language introduced will be also used in [25].

Section 5 contains the above-mentioned degree-derivation bounds which are exemplified in Section 6 for several decision problems. Whether testing important polynomials such as resultants, discriminants, subresultants, Hankel determinants, or Hurwitz determinants have non-linear lower complexity bounds remains an open problem. Concrete bounds on computing specific polynomials given in [2] and [44] remain essentially true for testing them. (For applications to randomized decision trees see [10].)

Besides the general study of and search for concepts providing an understanding of the various causes for algorithmic difficulty a main aim of a theory of lower bounds manifests in the idea and vision of finally supplying a rather complete knowledge of the complexities of natural and omnipresent computational and decisional problems in computational practice. In the spirit of such a program section 7 is entirely devoted to test questions around various interpolation problems and Chinese remaindering. The lower bounds shown remain correct for the related decision problems for $\mathbb{Q}$-rational points. (For decision complexity and rational points, see also [4, 19, 50].)

Finally, we mention that lower bounds on decision trees entail in bounds for the uniform model of real Turing machines due to Blum et al. [9]. This theory takes the finitary view with respect to programs versus sequences of trees; the result by Meyer auf der Heide [28] shows strong evidence that the real knapsack problem may be a candidate to distinguish the uniform and the non-uniform notions of complexity. The author completely agrees with the *credemus* of [9] that a reasonable amalgamation of theoretical computer science and mathematics will eventually bring solutions to the innumerable complexity questions.

2. Straight line programs and computations in commutative algebras

Let **ac** denote the category of commutative rings and $\mathbf{ac}_R$ the category of commutative R-algebras. ($R \in \mathbf{ac}$ will usually be a field.)

Points. Let $R \to A$ be a commutative R-algebra written in form of its structural morphism in **ac**. An "(n-)vector"

$$x = (R \to A; x_1, \ldots, x_n)$$

with $x_i \in A$ is called a $(R \to A)$-valued (n-)point; x is said to be *zero* if $A = 0$, a *field point* if A is a field. The set of these points is denoted $\mathbb{A}^n_{R\to A}$; points in any $\mathbb{A}^n_{R\to A}$ are called *points over* R.

Arithmetic. Following [45] commutative R-algebras will be considered computationally as *partial* algebras in the sense of universal algebra (e.g., [13, 15]) of signature

$$\Omega^R = R \sqcup \{0, 1, +, -, *, /\}.$$

In every R-algebra $R \to A$ every operational symbol $\omega \in \Omega^R$ acts as a partial operator $\omega_A : A^{\mathrm{ar}(\omega)} \supset \mathrm{def}\,\omega_A \to A$ of arity $\mathrm{ar}(\omega)$ where $\lambda \in R$ acts as the unary multiplication with the scalar λ, the only partial "/" as division by units, and 0, 1 as constants

(nullary). Hereby the phylum (= carrier set) of $R \to A$ is considered to be (the phylum of) the ring A. So Ω^R is a possible signature for $\mathbf{ac}_R$. (One may also write A instead of $R \to A$ if the conception of A as an R-algebra is clear from the context.)

Remark 1. Let $x \in \mathbb{A}^n_{R\to A}$ be a point over R as above.

(1) Its "head" $R \to A$ is thought to carry the information about the arithmetic in the above sense; for notational ease this head will usually be suppressed, and one simply writes $x = (x_1, \ldots, x_n)$.

(2) Let $R[x] \subseteq A$ denote the finitely generated R-subalgebra generated by the coordinates $x_1, \ldots, x_n \in A$ in the usual sense without division (i.e., signature $R \sqcup \{0, 1, +, -, *\}$). Then the full Ω^R-subalgebra generated by the coordinates, denoted $R(x]$, is the localization of $R[x]$ with respect to the multiplicative system of all elements becoming units in A. So $R(x]$ lies between $R[x]$ and the total ring of fractions $R(x)$ of $R[x]$. The point x defines points $\mathrm{t}(x) \in \mathbb{A}^n_{R\to R[x]}$ and $\mathrm{ft}(x) \in \mathbb{A}^n_{R\to R(x]}$ with the same coordinates which may be called the (R-algebra) *torso* resp. the Ω^R-*torso* (or full torso) of x.

(3) The point x can also be viewed as the R-algebra morphism of evaluation

$$e_x : R[X_1, \ldots, X_n] \longrightarrow A, \quad X_i \mapsto x_i$$

having image $R[x]$; its kernel (ideal of relations) is denoted $\operatorname{ann} x$. So for fixed n points over R are in one-to-one correspondence with $R[X_1, \ldots, X_n]$-algebras.

Straight line programs. An Ω^R-*straight line program* (Ω^R-SLP) $\Gamma = (\Gamma_1, \ldots, \Gamma_t)$ *over* $n \in \mathbb{N}$ is a sequence of computational instructions Γ_i of the form

$$s_i := \omega_i(s_{j_{i1}}, \ldots, s_{j_{i\,\mathrm{ar}(\omega_i)}}),$$

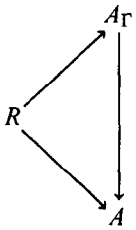
where $s_{-n+1}, \ldots, s_t$ are program variables, $\omega_i \in \Omega^R$, and $-n < j_{ia} < i$ for all i, a. An *input* for Γ is any point $x = (x_1, \ldots, x_n)$ in any $\mathbb{A}^n_{R\to A}$. Assigning the (input) variables s_i ($i \le 0$) the values x_{n+i} one can execute for $i = 1, \ldots, t$ the instructions Γ_i in $R \to A$. If no division by a non-unit occurs then Γ is said to be *executable* on x, and yields a result sequence

$$\mathrm{Res}(\Gamma, x) = (r_{-n+1} = x_1, \ldots, r_0 = x_n, r_1, \ldots, r_t) \in \mathbb{A}^{n+t}_{R\to A}.$$

The pair (Γ, x) may be called an Ω^R-*computation in* $R \to A$. (Γ, x) (resp. Γ) is said to *compute* $f \in \mathbb{A}^m_{R\to A}$ (on input x) if Γ is executable on x and all f_i appear in the result sequence $\mathrm{Res}(\Gamma, x)$. If $\iota : m \to n+t$ is an assignment ($\ell \in \mathbb{N}$ viewed as the ℓ-elements set) and Γ' is an Ω^R-SLP over m then the "interface" ι defines the composition $\Gamma \circ_\iota \Gamma'$ in the obvious way. (Usually ι will be clear from the context.)

Every Ω^R-SLP Γ over n has an (essentially) unique *universal input* u_Γ of the form $u_\Gamma = (U_1, \ldots, U_n) \in \mathbb{A}^n_{R\to A_\Gamma}$, where $A_\Gamma = R[U]_d$ for some denominator $d \in R[U]$, with the property that Γ is executable on some $x \in \mathbb{A}^n_{R\to A}$ if and only if there is a unique

R-algebra morphism



with $(u_\Gamma)_i \mapsto x_i$ [11]. Γ is said to be *nilly* if it is unexecutable on any non-zero point. This means that u_Γ is zero (so in any case the U_i above have to be interpreted in A_Γ). Clearly $R(u_\Gamma] = A_\Gamma$, and if R is a field and Γ is not nilly then e_{u_Γ} is injective, $R[u_\Gamma] = R[U]$, and $R(u_\Gamma) = R(U)$.

Complexity. Let $c : \Omega^R \to \mathbb{N}$ be a cost function, $x \in \mathbb{A}^n_{R\to A}$, $f \in \mathbb{A}^m_{R\to A}$. The *complexity* $L(c,x,f)$ of computing f from x with respect to c is defined as the minimum *c-length* $L(c,\Gamma) = \sum_{i=1}^{t} c(\omega_i)$ of an Ω^R-SLP Γ over n computing f on input x (with the convention $\min \emptyset = \infty$ throughout this paper). Pairs (c,x) are called *complexity data* on the algebra $R \to A$.

It is clear that complexity cannot increase if one applies an R-algebra morphism, and a skillful choice of an R-algebra morphism reducing complexity may be a step in proving lower bounds. However, certain indispensible processes such as scalar extension, restriction, coefficient conjugation, etc., should be included too.

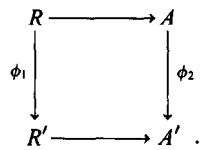
The heterogeneous view, and the variable standpoint with respect to coefficients. In contrast to viewing a commutative algebra $R \to A$ as a *homogeneous* partial Ω^R-algebra (*one* phylum), one can also view it as a *heterogeneous* partial algebra (see [5]) with the *two* phyla R and A of signature

$$\{0,1,+,-,*,/\} \sqcup \{\sigma\} \sqcup \{0,1,+,-,*,/\},$$

the first portion acting on R, the last one on A, and the scalar multiplication $\sigma : R \times A \to A$ in the "mixed" way. (It is clear that one can generally define heterogeneous SLPs with heterogeneous inputs and outputs.) Thinking for simplicity of coefficients to be free at disposal one may omit the first portion, and

$$\Omega = \{\sigma\} \sqcup \{0,1,+,-,*,/\}$$

establishes a heterogeneous signature on the wider category (of diagrams) **flac** of *all* algebras $R \to A$ of commutative rings whose morphisms are commutative squares



If the algebras (the horizontal arrows) are given a morphism ϕ in **flac** is given by the pair (ϕ_1, ϕ_2), and ϕ induces functorially a mapping

$$\mathbb{A}^n_\phi : \mathbb{A}^n_{R\to A} \longrightarrow \mathbb{A}^n_{R'\to A'}, \quad x \mapsto x' = (\phi_2(x_1), \ldots, \phi_2(x_n)).$$

(For the *functorial view* in general see e.g. [14]). For simplicity, we write $\phi(x)$ instead of $\mathbb{A}^n_\phi(x)$, and if ϕ is clear from the context we will simply speak of the *image* x' of x in $\mathbb{A}^n_{R'\to A'}$. For fixed R one obtains back the homogeneous signature Ω^R from Ω by individualizing scalar multiplication. For simplicity, we will keep the homogeneous view in what follows. In this hybrid sense of varying signatures a morphism ϕ in **flac** carries over an Ω^R-computation (Γ, x) in $R \to A$ into an $\Omega^{R'}$-computation $(\Gamma', x') = \phi(\Gamma, x)$ in $R' \to A'$ where ϕ_1 induces a mapping $\Omega^R \to \Omega^{R'}$ (also denoted by ϕ_1) giving rise to a program transformation $\Gamma \mapsto \Gamma' = \phi_1(\Gamma)$ in the obvious way. If ϕ_1 is surjective then every $\Omega^{R'}$-SLP can be lifted to an Ω^R-SLP; if $\phi_2^{-1}(A'^\times) = A^\times$ then every Ω^R-computation (Γ, x) in $R \to A$ is executable if and only if $\phi(\Gamma, x)$ in $R' \to A'$ is. The second condition is, for instance, satisfied in each of the following cases: ϕ_2 is surjective and $\ker \phi_2 \subseteq \operatorname{rad} A$ (Jacobson radical), ϕ_2 is a local morphism of local rings, and ϕ_2 is faithfully flat. If both conditions are satisfied then we call ϕ *surst* (ϕ_1 *sur*jective and ϕ_2 *st*rong (cf. [15]) with respect to signature $\{0, 1, +, -, *, /\}$ on **ac**).

If (c, x) and (c', x') are complexity data upstairs and downstairs then it is clear that for any $f \in \mathbb{A}^m_{R\to A}$

$$L(c', x', \phi(f)) \le L(c, x, f) + L(c', x', \phi(x))$$

if $c \ge c' \circ \phi_1$. Reversely, if $\tau : \mathbb{N} \to \mathbb{N}$ is any function then ϕ is said to be τ-*autarkical* (*autarkical* if $\tau = id$) for f with respect to (c, x) and (c', x') ([45], [24]) if one has an inverse inequality

$$L(c, x, f) \le \tau(L(c', x', \phi(f))).$$

Autarky results, which are helpful for proving lower bounds, can be proved if one has lower bounds on the following complexities. The *relation complexity* of a proper ideal $\mathfrak{a} \subset A$ is defined as

$$R(c, x, \mathfrak{a}) = \min\{L(c, x, f) : f \in \mathfrak{a} \setminus \{0\}\};$$

the *non-unit complexity* is defined as

$$N(c, x) = \min_{\mathfrak{a} \subset A} R(c, x, \mathfrak{a}).$$

Lower bounds on these complexities in certain cases will be a by-product of the investigations of this paper.

Lemma 2. *Let* $x' \in \mathbb{A}^n_{R'\to A'}$ *be the image of* $x \in \mathbb{A}^n_{R\to A}$ *with respect to a morphism* $\phi = (\phi_1, \phi_2)$ *in* **flac**, $\mathfrak{a}' \subset A'$ *an ideal with contraction* $\mathfrak{a} \subset A$ *with respect to* ϕ_2.

(1) *If* $c \ge c' \circ \phi_1$ *and* $R(c, x, \mathfrak{a}) < R(c, x, \ker \phi_2)$, *then* $R(c, x, \mathfrak{a}) \ge R(c', x', \mathfrak{a}')$.

(2) *If* ϕ *is surst and* $c = c' \circ \phi_1$, *then* $R(c,x,\mathfrak{a}) \leq R(c',x',\mathfrak{a}')$.

Proof. (1) If (Γ,x) is a computation in $R \to A$ for some $f \in \mathfrak{a} \setminus \ker \phi_2$ with $L(c,\Gamma) = R(c,x,\mathfrak{a})$ then $\phi(\Gamma,x)$ is one in $R' \to A'$ for some $f' \in \mathfrak{a}' \setminus \{0\}$.

(2) Any computation (Γ',x') in $R' \to A'$ for some $f' \in \mathfrak{a}' \setminus \{0\}$ can be lifted to a computation (Γ,x) in $R \to A$ for some $f \in \mathfrak{a} \setminus \{0\}$. □

Proposition 3. *Let* $x' \in \mathbb{A}^n_{R' \to A'}$ *be the image of* $x \in \mathbb{A}^n_{R \to A}$ *with respect to a morphism* $\phi = (\phi_1, \phi_2)$ *in* **flac**, ϕ_1 *surjective, and* $c = c' \circ \phi_1$. *Then the following hold.*

(1) *If* $f' \in A'$ *is non-zero and* $\phi_2^{-1}(f') \cap A^\times = \emptyset$, *then* $L(c',x',f') \geq N(c,x)$. *In particular,* $N(c',x') \geq N(c,x)$ *with equality if* ϕ *is surst and* $N(c,x) < R(c,x,\ker \phi_2)$.

(2) *If* $A' \neq 0, f \in \mathbb{A}^m_{R \to A}$, $L(c,x,f) \leq \min\{N(c,x_{\mathrm{red}}), \frac{1}{2}(R(c,x,\ker \phi_2) - c(-))\}$, *where* x_{red} *denotes the image of* x *in* $\mathbb{A}^n_{R \to A_{\mathrm{red}}}$, *then* ϕ *is autarkical for* f *with respect to* (c,x) *and* (c',x').

(3) *If* $f \in \mathbb{A}^m_{R \to A}$, $L(c,x,f) \leq \frac{1}{2}(R(c,x,\ker \phi_2) - c(-))$ *and* ϕ *is surst, then* ϕ *is autarkical for* f *with respect to* (c,x) *and* (c',x').

Proof. (1) If (Γ',x') computes f' and (Γ,x) is lying above it (that is, $\phi(\Gamma,x) = (\Gamma',x')$) then either (Γ,x) is executable, and then it computes a non-zero non-unit in A, or (Γ,x) is unexecutable, and then the maximal initial segment of Γ which is executable on x must produce even a non-nilpotent non-unit in A. By Lemma 2 equality of non-unit complexities holds under the assumptions made.

(2) Assume $L(c,x,f) > L(c',x',\phi(f))$, and let (Γ',x') compute $\phi(f)$ with $L(c',\Gamma') < L(c,x,f)$. If (Γ,x) lies above (Γ',x') then it must be executable since by assumption $L(c,x,f) \leq N(c,x_{\mathrm{red}})$, and it computes some $g \neq f$ with $\phi(g) = \phi(f)$. Composing (Γ,x) with an optimal computation for f and using one further subtraction yields a non-zero element $h \in \ker \phi_2$ with $L(c,x,h) < R(c,x,\ker \phi_2)$, a contradiction.

(3) Analogously as (2) above. □

Rational operations. For technical reasons we will also use a wider set $\hat{\Omega}^R \supseteq \Omega^R$ of rational operations in some places. A *rational operation* ω of *arity* a is a pair of polynomials $\omega = (\theta,\eta) \in R[T_1,\ldots,T_a]^2$ (written as $\omega = \theta/\eta$); if $x \in \mathbb{A}^a_{R \to A}$ then ω is defined on x if $\theta(x) \in A$ is a unit, and in the affirmative case its value is defined as $\omega(x) = \theta(x)/\eta(x)$. Let $\hat{\Omega}^R$ denote the disjoint union of rational operations of any arity. Clearly, $\hat{\Omega}^R$ is also a possible signature for $\mathbf{ac}_R$ having in every R-algebra the same clone of action (cf. [13]) as Ω^R, and everything said about Ω^R-SLPs applies to $\hat{\Omega}^R$-SLPs. (Only the above *calculus interruptus* argument in Proposition 3 needs some proviso; one should assume the cost function c on $\hat{\Omega}^R$ to be "denominator compatible," that is, $c(\theta/\eta) \geq c(\eta/1)$ for all operations θ/η.)

Finally, a *vector operation* $\omega = (\omega_1,\ldots,\omega_t) \in (\hat{\Omega}^R)^t$ of *arity* a is a list of rational operations of common arity a; it is clear that ω can be viewed as an $\hat{\Omega}^R$-SLP over a.

3. The degree method

In this section we briefly recall the notion of degree, Strassen's degree bound, and several facts about degree to be applied later on.

We assume R to be a field throughout this section. If $x \in \mathbb{A}^n_{R\to A}$ is a non-zero point over R then its *dimension* $\dim x$ is defined as the Krull-dimension of $R[x] = R[X_1,\ldots,X_n]/\operatorname{ann} x$. Its *Hilbert function* $H(x,t)$ is defined as the Hilbert function of $\operatorname{ann} x$ (cf. [27]); if $R[X]^{(\le t)} \subset R[X]$ denotes the R-vector subspace of all polynomials of degree $\le t$, then $H(x,t)$ is the R-vector space dimension of the finite-dimensional subspace $R[X]^{(\le t)}/\operatorname{ann} x \cap R[X]^{(\le t)}$ of $R[x]$. It is well known that for large t the values of the Hilbert function are given by the values of an univariate polynomial of degree $\dim x$, called the *Hilbert polynomial*,

$$H(x,t) = \sum_{i=0}^{\dim x} h_i(x)\binom{t}{\dim x - i} \quad \text{for } t \gg 0.$$

The coefficient $h_0(x) > 0$ of the leading term is called the *degree* of x and is denoted $\deg x$.

Example 4. (1) Let $X = (X_1,\ldots,X_n) \in \mathbb{A}^n_{R\to R[X]}$. Then $\operatorname{ann} X = 0$, $\dim X = n$, and $\deg X = 1$. X is the universal input of any division free Ω^R-SLP over n. Generally, if Γ is not nilly then $\dim u_\Gamma = n$, $\deg u_\Gamma = 1$.

(2) Let $s = (X_1Y_1,\ldots,X_nY_m) \in \mathbb{A}^{n\cdot m}_{R\to R[X,Y]}$ (Segre). Then $\operatorname{ann} s \subset R[S_{1\,1},\ldots,S_{n\,m}]$ is the determinantal ideal generated by all 2×2-minors, $\dim s = n+m-1$, and $\deg s = \binom{n+m-2}{n-1}$ (cf. [17, p. 54]). (This will be used in Section 5.)

We call a polynomial $f \in R[X]$ a non-zero divisor of the point x, or *x-regular*, if f is A-regular (cf. [27]) via the substitution e_x (see Remark 1(3)), and the element $e_x(f)$ is said to be presented by f. Analogously, we speak of an x-regular sequence $f_1,\ldots,f_r \in R[X]$.

If $x \in \mathbb{A}^n_{R\to A}$, $y \in \mathbb{A}^m_{R\to A}$ then their *concatenation*

$$(x_1,\ldots,x_n,y_1,\ldots,y_m) \in \mathbb{A}^{n+m}_{R\to A}$$

is denoted by xy. If $x \in \mathbb{A}^n_{R\to A}$, $y \in \mathbb{A}^m_{R\to B}$ then their *join* is defined as

$$x \bowtie y = (x_1\otimes 1,\ldots,x_n\otimes 1, 1\otimes y_1,\ldots,1\otimes y_m) \in \mathbb{A}^{n+m}_{R\to A\otimes_R B}.$$

For completeness we summarize some facts about dimension and degree that will be used freely in the sequel, in particular inequalities of Bézout type. (A more general inequality of great significance for complexity theory has been given by Heintz [18]; for a very thorough treatment of Bézout equalities and inequalities the reader is referred to the book by Vogel [49].)

Proposition 5. *Let $x \in \mathbb{A}^n_{R\to A}$ be non-zero, R a field.*

(1) *If $R[x]$ is integral with quotient field $R(x)$, then* $\dim x = \operatorname{tr.deg}_R R(x)$.

(2) *If* $y \in \mathbb{A}^m_{R\to A}$ *satisfies* $\sum Ry_j + R = \sum Rx_i + R$, *then* $\dim y = \dim x$, $\deg y = \deg x$.

(3) *Let* $A \to A'$ *be a morphism of rings,* x' *the image of* x *in* $\mathbb{A}^n_{R\to A'}$. *If* x' *is non-zero, then* $\dim x' \le \dim x$, *and if equality of dimensions holds then also* $\deg x' \le \deg x$. *If* $R[x] \to R[x']$ *is injective, then dimension and degree equalities hold.*

(4) (*Join*) *If* $y \in \mathbb{A}^m_{R\to B}$ *is a further non-zero point over* R, *then* $\dim x \bowtie y = \dim x + \dim y$, $\deg x \bowtie y = \deg x \cdot \deg y$.

(5) (*Projection*) *If* $xy \in \mathbb{A}^{n+m}_{R\to A}$ *is the concatenation of* x *and some* $y \in \mathbb{A}^m_{R\to A}$, *then* $\dim x \le \dim xy$. *If equality of dimensions holds or if* A *is an integral domain* (*or if* $R[xy]$ *is unmixed and reduced*), *then* $\deg x \le \deg xy$.

Let x' *be the image of* x *in* $\mathbb{A}^n_{R\to A/fA}$ *where* $f \in R[X]$, x' *being non-zero.*

(6) (*Bézout*) *If* f *is an* x*-regular polynomial then* $\dim x' \le \dim x - 1$; *if this is an equality then* $\deg x' \le \deg x \cdot \deg f$.

(7) (*Bézout reduced*) *If* f *is an* x*-intersecting polynomial* (*that is,* f *is* x_{red}*-regular where* x_{red} *denotes the image of* x *in* $\mathbb{A}^n_{R\to A_{\mathrm{red}}}$), *then* $\dim(x')_{\mathrm{red}} = \dim x' \le \dim x - 1$; *if this is an equality then* $\deg(x')_{\mathrm{red}} \le \deg x \cdot \deg f$.

Proof. (1) See [27, Theorem 5.6].

(2) This is clear since x and y have the same Hilbert functions.

(3) Since $\operatorname{ann} x \subseteq \operatorname{ann} x'$ we have $H(x',t) \le H(x,t)$. Comparing leading terms of Hilbert polynomials the statement is evident.

(4) One has $H(x \bowtie y, t) = \sum_{i\le t} H(x,i)\cdot H(y,t-i) - \sum_{i<t} H(x,i)\cdot H(y,t-1-i)$ (see [49, p. 61]). Replacing for large arguments Hilbert functions by Hilbert polynomials on the right-hand side one finds $H(x \bowtie y, t) = \deg x \cdot \deg y \cdot \binom{t}{\dim x + \dim y} + \cdots$ for $t \gg 0$ (see [49, p. 61]).

(5) Without loss of generality, we may assume $m = 1$. Since e_x is the composition $R[X] \hookrightarrow R[X,Y] \xrightarrow{e_{xy}} A$ we get $H(x,t) \le H(xy,t)$. So $\dim x \le \dim xy$, and also $\deg x \le \deg xy$ in case of equal dimensions. Viewing xy as the image of $x \bowtie y$ in $\mathbb{A}^{n+1}_{R\to A}$ and using (3) above we have $\dim x \le \dim xy \le \dim x \bowtie y \le \dim x + 1$. If now A is integral and $\dim x = \dim xy - 1$ then $\dim y = 1$, $R[x \bowtie y] = R[x] \otimes_R R[y]$ is integral and $R[x \bowtie y] \to R[xy]$ is injective. By (3) above $\deg xy = \deg x \bowtie y = \deg x$, since $\deg y = 1$.

(6) By definition, if f is x-regular it is A-regular. A forteriori f is $R[x]$-regular. $R[x] \to R[x']$ factors as $R[x] \to R[x]/fR[x] \to R[x']$, so by Krull's Principal Ideal Theorem and the assumption on Krull dimensions, $\dim R[x'] = \dim R[x] - 1$, we have $\dim R[x]/fR[x] = \dim R[x] - 1$. Let $\mathcal{S}$ denote the graded $R[X_0,\ldots,X_n]$, ${}^h\operatorname{ann} x \subset \mathcal{S}$ and ${}^h f \in \mathcal{S}$ denote the homogenizations of $\operatorname{ann} x$ and f. By assumption ${}^h f$ is a non-zero divisor of the graded $\mathcal{S}/{}^h\operatorname{ann} x$. A classical version of Bézout's Theorem (e.g. [49]) now says that $\deg({}^h\operatorname{ann} x + {}^h f\mathcal{S}) = \deg({}^h\operatorname{ann} x)\cdot\deg({}^h f)$. So by dehomogenization, the assumption on dimension, and from (3) above we conclude $\deg x \cdot \deg f \ge \deg x'' \ge \deg x'$ where $x'' \in \mathbb{A}^n_{R\to R[x]/fR[x]}$ is the point associated with the evaluation $R[X] \to R[x]/fR[x]$.

(7) This follows from (6) using (3). □

Remark 6. By Proposition 5(3) a point over R has the same degree (and Hilbert polynomial) as its torso, the latter allowing apparently application of more morphisms. Such partial morphisms (in $\mathbf{ac}_R$) will be used (implicitly) in many places. Others in connection with degree appear in the proof of Theorem 32 and in Lemma 51 (in **flac**); in connection with complexity see Lemma 42 and also [24], [25] where deformations of algebras and *approximative complexities* are used as an instrument to prove lower bounds on decision complexity. A partial morphism in **flac** is simply a diagram

$$\begin{array}{ccc} R'' & \longrightarrow & A'' \\ \uparrow & & \uparrow \\ R & \longrightarrow & A \\ \downarrow & & \downarrow \\ R' & \longrightarrow & A' \end{array}$$

where the top one is a monomorphism in **flac**.

Let $\omega = (\omega_1, \ldots, \omega_t)$ be a vector operation of arity a with universal input u_ω. If ω is not nilly then we define its degree $\deg \omega$ as the degree of the concatenated point $u_\omega \omega(u_\omega) \in \mathbb{A}^{a+t}_{R \to A_\omega}$ which has dimension a by Proposition 5(1) (note that viewing ω of arity $a' > a$ does not change the degree by Proposition 5(4)).

Example 7. Let $\omega = \theta/\eta \in \hat{\Omega}^R$, θ and η being relatively prime. Then $\deg \omega = \max\{\deg \theta, 1 + \deg \eta\}$. So for the operations in Ω^R, $\deg(*) = \deg(/) = 2$, the others having degree one.

The following lemma is the key step in the proof of Strassen's degree bound. For later use we formulate it for vector operations.

Lemma 8. *Let $\omega = (\omega_1, \ldots, \omega_t) \in (\hat{\Omega}^R)^t$ be a vector operation of arity a, R being a field. If $x \in \mathbb{A}^a_{R \to A}$ is non-zero and ω is executable on x, then for the concatenated point $x\omega(x) \in \mathbb{A}^{a+t}_{R \to A}$,*

$$\dim x\omega(x) = \dim x, \quad \deg x\omega(x) \leq \deg x \cdot \deg \omega.$$

Proof. Consider the non-zero join $j = x \bowtie u_\omega \omega(u_\omega) \in \mathbb{A}^{a+a+t}_{R \to A \otimes_R A_\omega}$ having dimension $\dim x + a$ and degree $\deg x \cdot \deg \omega$ by Proposition 5(4). Write $A_\omega = R[U_1, \ldots, U_a]_d$ for some $d \in R[U]$; then $A \otimes_R A_\omega = A[U]_d$. Since ω is executable on x the value of the polynomial $d \in R[U]$ at x is a unit in A, so d is a non-zero divisor of $A[U]$. Considering the substitution $e_j : R[X, U, W] \to A[U]_d$ associated with j we see that the linear polynomials $U_1 - X_1, \ldots, U_a - X_a \in R[X, U, W]$ form a j-regular sequence since for $i = 1, \ldots, a$ the image $U_i - x_i$ in $A[U]$ has leading coefficient one with respect to U_i. Since $\deg xx\omega(x) = \deg x\omega(x)$, and $\dim xx\omega(x) = \dim x\omega(x) \geq \dim x$

(by Proposition 5(2) and (5)) we can use Proposition 5(6) successively to conclude $\dim xx\omega(x) = \dim j - a = \dim x$, and $\deg xx\omega(x) \leq \deg j = \deg x \cdot \deg \omega$, hence the assertion. □

Theorem 9 (Strassen [46]). *Let R be a field, and $x \in \mathbb{A}^n_{R\to A}$, $f \in \mathbb{A}^m_{R\to A}$ be non-zero points over R. Then for the multiplicative cost function $c_* = 1_{\{*,/\}} : \Omega^R \to \mathbb{N}$,*

$$L(c_*, x, f) \geq \log_2 \deg xf - \log_2 \deg x.$$

Proof. Let Γ be an Ω^R-SLP over n computing f on x having c_*-length l. Then by Lemma 8 (repeatedly) $\dim x = \dim \mathrm{Res}(\Gamma, x)$ and $\deg \mathrm{Res}(\Gamma, x) \leq \deg x \cdot 2^l$. From Proposition 5(5) we get $\dim x \leq \dim xf \leq \dim \mathrm{Res}(\Gamma, x) = \dim x$, and therefore (again by Proposition 5(5)) $\deg xf \leq \deg \mathrm{Res}(\Gamma, x) \leq \deg x \cdot 2^l$, whence the assertion. □

In order to prove lower bounds on complexity we need some further facts about dimension and degree collected in the following proposition.

Proposition 10. *Let $x \in \mathbb{A}^n_{R\to A}$ be non-zero, R a field.*

(1) (*Scalar extension*) *Let $K \supseteq R$ be an extension field, and let x^K be the image of x in $\mathbb{A}^n_{K\to K\otimes_R A}$. Then $\dim x^K = \dim x$, $\deg x^K = \deg x$.*

(2) (*Scalar restriction*) *Let $k \subseteq R$ be a subfield, and let x be the image of the (uniquely determined) point ${}^k x \in \mathbb{A}^n_{k\to A}$. Then $\dim x \leq \dim {}^k x$, and in case of equal dimensions (which holds true if $k \subseteq R$ is algebraic) $\deg x \leq \deg {}^k x$.*

(3) (*Absorption of coordinates into the coefficient field*) *Let $y \in \mathbb{A}^m_{R\to A}$ be a further point over R, and let $y_{R[x]}$ be its image in $\mathbb{A}^m_{R[x]\to A}$. Assume $R[x]$ to be an integral domain with quotient field $R(x)$, and set $y_{R(x)} = (y_{R[x]})^{R(x)} \in \mathbb{A}^m_{R(x)\to R(x)\otimes_{R[x]} A}$. Then $\dim x + \dim y_{R(x)} \leq \dim xy$. If this is an equality (which holds true for integral A), then $\deg y_{R(x)} \leq \deg xy$.*

(4) (*Zero-dimensional points*) *If $\dim x = 0$, then $\deg x = \dim_R R[x]$ and vice versa.*

Proof. (1) One has $H(x,t) = H(x^K, t)$ since the scalar extension does not change vector space dimensions.

(2) x is the image of $({}^k x)^R$, so the statement follows from 10(1) above and Proposition 5(3). If $k \subseteq R$ is algebraic then $k[X] \to R[X]$ is flat and integral; so $\dim {}^k x = \dim x$.

(3) Without loss of generality we may assume $n = 1$. If $R(x)$ is algebraic over R then by Propositions 5(1) and (2), and 10(2) above we have $\dim x = 0$, $\dim y = \dim y_{R(x)} = \dim(xy)_{R(x)} = \dim xy$, and $\deg y_{R(x)} = \deg(xy)_{R(x)} \leq \deg xy$.

Assume $\mathrm{tr.deg}_R R(x) = 1$. By (1) above $\dim(xy)^{R(x)} = \dim xy$ and $\deg(xy)^{R(x)} = \deg xy$. The kernel of $R(x) \otimes_R A \to R(x) \otimes_{R[x]} A$ contains the non-zero-divisor $1 \otimes x_1 - x_1 \otimes 1$ which obviously can be presented by a linear $(xy)^{R(x)}$-regular polynomial. Therefore, $\dim y_{R(x)} = \dim(xy)_{R(x)} \leq \dim(xy)^{R(x)} - 1$ by Proposition 5(2), (6) and (3), and in case of equality also $\deg y_{R(x)} = \deg(xy)_{R(x)} \leq \deg(xy)^{R(x)}$.

(4) If $\dim x = 0$ then $\deg x = H(x,t) = \dim_R R[x]$ for large t. □

4. Verifiers and decision trees

In this section we equip SLPs with additional test instructions; these will later be assigned to paths in decision trees.

Verifiers. Let $n \in \mathbb{N}$, and $\mathrm{P} = \{=, \leq\}$ (resp. $\mathrm{P} = \{=\}$). An (Ω^R, P)-*SLP* $\Upsilon = (\Theta_0, \Gamma_1, \Theta_1, \ldots, \Gamma_t, \Theta_t)$ *over* n is an alternating sequence of computational instructions Γ_i (as before) and sequences of test instructions Θ_i of the form

$$s_{h_{i1}} \rho_{i1} s_{h'_{i1}}, \ldots, s_{h_{i\ell_i}} \rho_{i\ell_i} s_{h'_{i\ell_i}},$$

where $\rho_{ij} \in \mathrm{P}$, and $h_{ij}, h'_{ij} \leq i$. An input for Υ is an *ordered field* point $\mathfrak{x}$ (resp. a field point in the order free situation when $\mathrm{P} = \{=\}$) over R, that is a pair $\mathfrak{x} = (x, \leq)$ where $x \in \mathbb{A}^n_{R \to K}$, and $(K, \leq)$ is an ordered field. If Υ is executable on $\mathfrak{x}$, that is, $\Gamma(\Upsilon) = (\Gamma_1, \ldots, \Gamma_t)$ is executable on x, then it produces an *truth value* $\mathrm{tr}(\Upsilon, \mathfrak{x}) \in \prod_{i=0}^{t} \{\mathrm{yes}, \mathrm{no}\}^{\ell_i}$ according to the outcome of the tests. For arbitrary $\mathfrak{x}$ we denote by $\Upsilon_{\mathfrak{x}}$ the maximal initial segment of Υ executable on $\mathfrak{x}$. Let F be a set of ordered field n-points over R (resp. field points), $E \subseteq F$ a subset. Υ is said to *verify* E *in* F if it is executable on all $\mathfrak{x} \in E$, $\mathrm{tr}(\Upsilon, \mathfrak{x}) = \mathrm{tr}(\Upsilon, \mathfrak{y})$ for all $(\mathfrak{x}, \mathfrak{y}) \in E \times E$, and $\mathrm{tr}(\Upsilon_{\mathfrak{y}}, \mathfrak{x}) \neq \mathrm{tr}(\Upsilon_{\mathfrak{y}}, \mathfrak{y})$ for all $(\mathfrak{x}, \mathfrak{y}) \in E \times (F \setminus E)$. (Note that verification is one-sided, that is, Υ is not necessarily a verifier for the complement $F \setminus E$.)

Complexity. The *verification complexity* $V(c, E, F)$ with respect to a cost function $c : \Omega^R \sqcup \mathrm{P} \to \mathbb{N}$ is defined as the minimum *c-length* $L(c, \Upsilon) = \sum_{i \geq 1} c(\omega_i) + \sum_{i \geq 0} \sum_{j \leq \ell_i} c(\rho_{ij})$ of a verifier Υ for E in F.

Passing to a subpair does not increase verification complexity.

Remark 11. (1) $V(c, G, H) \leq V(c, E, F)$ if $(G, H) \subseteq (E, F)$.

(2) $V(c, E, G) \leq V(c, F, G) + V(c, E, F)$ if $E \subseteq F \subseteq G$.

Proof. (1) Every verifier for E in F is also a verifier for G in H.

(2) One can manufacture a verifier for E in G by composing one for F in G and one for E in F. □

Next we parametrize verification complexity with *reference points* $x \in \mathbb{A}^n_{R \to A}$ and subsets in the *real spectrum* (cf. [8]) of A (resp. Zariski spectrum of A). Let $\alpha \in \mathrm{Spec}_r A$ be a prime cone with support $\mathfrak{p}$ (resp. $\mathfrak{p} \in \mathrm{Spec}\, A$); x assigns canonically to α the ordered field point $x(\alpha) = (x(\mathfrak{p}), \leq_\alpha)$ (resp. the field point $x(\mathfrak{p})$) over R, where $x(\mathfrak{p})$ is the image of x in $\mathbb{A}^n_{R \to k(\mathfrak{p})}$, $k(\mathfrak{p})$ denoting the residue class field of $\mathfrak{p}$. If $E \subseteq F$ are subsets in $\mathrm{Spec}_r A$ (resp. in $\mathrm{Spec}\, A$) then the verification complexity $V(c, x, E, F)$ with respect to x is defined as $V(c, x(E), x(F))$.

Proving lower bounds sometimes requires to change the reference point; the following remark is evident.

Remark 12. $V(c, x, E, F) \geq V(c, y, E, F) - L(\check{c}, y, x)$ for $y \in \mathbb{A}^m_{R \to A}$ and the restriction $\check{c}$ of c on Ω^R.

If $n \in \mathbb{N}$ is fixed, and $X = (X_1, \ldots, X_n) \in \mathbb{A}^n_{R \to R[X]}$ then the assignment $\alpha \mapsto X(\alpha)$ (resp. $\mathfrak{p} \mapsto X(\mathfrak{p})$) is one-to-one; these points $X(\alpha)$ (resp. $X(\mathfrak{p})$) are precisely the Ω^R-torsos (plus induced ordering) of ordered field n-points (resp. field n-points) over R. Since passing to Ω^R-torsos does not change verification complexities one may assume for fixed n without loss of generality inputs to be points in $\mathrm{Spec}_r R[X]$ (in $\mathrm{Spec}\, R[X]$), thereby identifying α and $X(\alpha)$ (resp. $\mathfrak{p}$ and $X(\mathfrak{p})$).

Remark 13. Note that the notation $X(\alpha)$ differs from the respective one in [8] where the ordered field $(k(\mathrm{supp}\,\alpha), \leq_\alpha)$ is replaced by the real closure $k(\alpha)$. By the remark on Ω^R-torsos above this clearly does not harm. The situation is however different when operations of Nash type like $\sqrt{\ }$ are allowed. Then the image of x in $\mathbb{A}^n_{R \to k(\alpha)}$ becomes relevant.

The second part in the next statement strengthens the above remark on subpairs.

Proposition 14. *Let $E \subseteq F \subseteq \mathrm{Spec}_r R[X]$ and $G \subseteq H \subseteq \mathrm{Spec}_r R[X]$ be subsets.*

(1) *There is a verifier for E in F if and only if E is the trace in F of a elementary locally closed subset of* $\mathrm{Spec}_r R[X]$ *(that is a subset which is a finite intersection of subsets of the form $\{\alpha : a(\alpha) \geq 0\}$ or $\{\alpha : a(\alpha) \neq 0\}$, $a \in R[X]$).*

(2) *Assume for all $\alpha \in F$ the zero-sets $\mathscr{Z}(\mathrm{supp}\,\alpha) \subseteq \mathrm{Spec}_r R[X]$ to satisfy $\alpha \in \overline{\mathscr{Z}(\mathrm{supp}\,\alpha) \cap G}$ if $\alpha \in E$ and $\alpha \in \overline{\mathscr{Z}(\mathrm{supp}\,\alpha) \cap H \setminus G}$ if $\alpha \in F \setminus E$. Then every verifier for G in H is a verifier for E in F; as a consequence, $V(c, G, H) \geq V(c, E, F)$.*
(Analogously, for subsets in $\mathrm{Spec}\, R[X]$*).*

Proof. (1) This is clear.

(2) Let Υ be a verifier for G in H. For every $\alpha \in \mathrm{Spec}_r R[X]$ the subset $\{\beta : \Upsilon_\beta = \Upsilon_\alpha, \mathrm{tr}(\Upsilon_\alpha, \beta) = \mathrm{tr}(\Upsilon_\alpha, \alpha)\} \subseteq \mathrm{Spec}_r R[X]$ is an elementary local closed subset containing α. Therefore, its trace in $\mathscr{Z}(\mathrm{supp}\,\alpha)$ is a neighborhood in $\mathscr{Z}(\mathrm{supp}\,\alpha)$ of α. So we see that Υ indeed verifies also E in F under the assumptions made. □

For verification complexity with respect to a reference point $x \in \mathbb{A}^n_{R \to A}$ morphisms in **flac** provide relative lower bound in a general manner by passing to fibers. (This will especially be used in [25].)

Proposition 15. *Let $x' \in \mathbb{A}^n_{R' \to A'}$ be the image of $x \in \mathbb{A}^n_{R \to A}$ with respect to a morphism $\phi = (\phi_1, \phi_2)$ in* **flac**.

(1) *If $c \geq c' \circ \phi_1$, then for $E \subseteq F \subseteq \mathrm{Spec}_r A$,*

$$V(c, x, E, F) \geq V(c', x', (\mathrm{Spec}_r \phi_2)^{-1}(E), (\mathrm{Spec}_r \phi_2)^{-1}(F)).$$

(2) *If $c = c' \circ \phi_1$ and ϕ_1 is surjective, then for $E' \subseteq F' \subseteq \mathrm{Spec}_r A'$,*

$$V(c', x', E', F') = V(c, x, (\mathrm{Spec}_r \phi_2)(E'), (\mathrm{Spec}_r \phi_2)(F')).$$

(Analogously, for subsets in $\mathrm{Spec}\, A$.*)*

Proof. (1) This is evident since the image $\phi_1(\Upsilon)$ of a verifier Υ for $x(E)$ in $x(F)$ is one for $x'((\mathrm{Spec}_r\,\phi_2)^{-1}(E))$ in $x'((\mathrm{Spec}_r\,\phi_2)^{-1}(F))$.

(2) Let Υ' be a verifier for $x'(E')$ in $x'(F')$ and choose Υ lying above it, that is, $\phi_1(\Upsilon)=\Upsilon'$. Then obviously Υ is a verifier for $x(E)$ in $x(F)$ where $E=(\mathrm{Spec}_r\,\phi_2)(E')$, $F=(\mathrm{Spec}_r\,\phi_2)(F')$. So $V(c,x,E,F)\le V(c',x',E',F')$. On the other hand,

$$V(c,x,E,F)\ge V(c',x',(\mathrm{Spec}_r\,\phi_2)^{-1}(E),(\mathrm{Spec}_r\,\phi_2)^{-1}(F))\ge V(c',x',E',F')$$

by (1) above and the remark on subpairs above. □

For $x\in\mathbb{A}^n_{R\to A}$ and $\alpha\in\mathrm{Spec}_r A$ the verification complexity $V(c,x,\alpha)$ of α itself is defined as the verification complexity of $\{\alpha\}$ in its halo of generizations $\mathrm{hal}\,\alpha=\{\beta:\beta\subseteq\alpha\}$ in $\mathrm{Spec}_r A$. Analogously, $V(c,x,\mathfrak{p})$ is defined for $\mathfrak{p}\in\mathrm{Spec}\,A$.

Related operational complexities. Let $c:\Omega^R\to\mathbb{N}$ be a cost function and $x\in\mathbb{A}^n_{R\to A}$. For $\alpha\in\mathrm{Spec}_r A$ its *isolation complexity* is defined as

$$I(c,x,\alpha)=\min\{L(c,x,f):f\in\mathbb{A}^m_{R\to A},m\in\mathbb{N},\{\alpha\}=\mathscr{Z}(f)\cap\mathrm{hal}\,\alpha\}.$$

Analogously, the isolation complexity $I(c,x,\mathfrak{p})$ of a prime ideal $\mathfrak{p}\in\mathrm{Spec}\,A$ is defined. The *exclusion complexity* of $\mathfrak{p}\in\mathrm{Spec}\,A$ is defined as

$$E(c,x,\mathfrak{p})=\min\{L(c,x,f):f\in\mathfrak{p}\setminus\mathrm{nil}\,A\}=R(c,x_{\mathrm{red}},\mathfrak{p}).$$

Finally, if A is a field and $B\subset A$ is a real discrete valuation ring with uniformization parameter u then its *sign complexity* is defined as

$$S(c,x,B)=\min\{L(c,x,eu^r):e\in B^\times,\ r\ \text{odd}\}.$$

In the sequel when $x\in\mathbb{A}^n_{R\to A}$ and $\mathfrak{a}\subset A$ is an ideal then $x/\mathfrak{a}$ denotes the image of x in $\mathbb{A}^n_{R\to A/\mathfrak{a}}$; similarly if $\mathfrak{p}\subset A$ is a prime ideal we write $x_{\mathfrak{p}}$ for the image of x in $\mathbb{A}^n_{R\to A_{\mathfrak{p}}}$.

Lemma 16. *Let* $x\in\mathbb{A}^n_{R\to A}$.

(1) *If* $\mathfrak{p}\supseteq\mathfrak{p}'\supseteq\mathfrak{p}''$ *are prime ideals in* A, *then*

$$E(c,(x/\mathfrak{p}')_{\mathfrak{p}},\mathfrak{p})\ge E(c,(x/\mathfrak{p}'')_{\mathfrak{p}},\mathfrak{p})\le E(c,(x/\mathfrak{p}'')_{\mathfrak{p}'},\mathfrak{p}'),$$

and one of these is an equality.

(2) *Let* A *be a field,* $(B,\mathfrak{m})\subset A$ *a real discrete valuation ring. If* x *is the image of* $\hat{x}\in\mathbb{A}^n_{R\to B}$, *then* $S(c,x,B)\ge E(c,\hat{x},\mathfrak{m})$.

(3) *If* $\mathrm{hal}\,\alpha\ne\{\alpha\}$ *for* $\alpha\in\mathrm{Spec}_r A$ (*resp.* $\mathrm{hal}\,\mathfrak{p}\ne\{\mathfrak{p}\}$ *for* $\mathfrak{p}\in\mathrm{Spec}\,A$), *then*

$$I(c,x,\mathrm{supp}\,\alpha)\ge I(c,x,\alpha)\ge E(c,x,\mathrm{supp}\,\alpha)$$

(*resp.* $I(c,x,\mathfrak{p})\ge E(c,x,\mathfrak{p})$) *with equality if* A *is integral and* 0 *is the only proper generization of* $\mathrm{supp}\,\alpha$ (*resp.* $\mathfrak{p}$).

Proof. (1) Consider the canonical R-algebra morphisms

$$(A/\mathfrak{p}')_{\mathfrak{p}}\longleftarrow(A/\mathfrak{p}'')_{\mathfrak{p}}\longrightarrow(A/\mathfrak{p}'')_{\mathfrak{p}'},$$

where the first one is local, so surst. By Proposition 3(1) we have

$$N(c,(x/\mathfrak{p}')_{\mathfrak{p}}) \geq N(c,(x/\mathfrak{p}'')_{\mathfrak{p}}) \leq N(c,(x/\mathfrak{p}'')_{\mathfrak{p}'}).$$

If the first inequality is strict then, by Proposition 3(1) again and Lemma 2(1),

$$N(c,(x/\mathfrak{p}'')_{\mathfrak{p}}) \geq R(c,(x/\mathfrak{p}'')_{\mathfrak{p}},\mathfrak{p}') \geq R(c,(x/\mathfrak{p}'')_{\mathfrak{p}'},\mathfrak{p}'),$$

so the second one is then an equality.

(2) Consider $B \hookrightarrow A$. If $f \in A^{\times} \setminus B^{\times}$ then $L(c,x,f) \geq N(c,\hat{x})$, by Proposition 3(1).

(3) This is clear. □

Remark 17. The difference between sign and exclusion complexity in Lemma 16(2) may be arbitrarily large (cf. [25]; see also Example A.2(3)). The same holds true for isolation and exclusion complexity in Lemma 16(3) (e.g. [11], Corollary 20 provides an example).

Remark 18. We mention the following "complexity theoretic identity theorem": Let $x \in \mathbb{A}^n_{R\to A}$, $f \in \mathbb{A}^m_{R\to A}$ where $(A,\mathfrak{m})$ is a local integral domain with quotient field $k(0)$ and residue class field $k(\mathfrak{m})$. If $L(c,x,f) \leq \frac{1}{2}(E(c,x,\mathfrak{m}) - c(-))$ then the both R-algebra morphisms

$$k(0) \leftarrow A \rightarrow k(\mathfrak{m})$$

are autarkical for f with respect to (c,x) and $(c,x(0))$ resp. $(c,x(\mathfrak{m}))$, by Proposition 3(2) and (3).

So lower bounds on exclusion complexity may for instance serve to reduce computational complexities in algebraic function fields to the sometimes easier to determine ones in rational function fields.

Considering suitable comparisons in verifiers one can relate these operational complexities with certain verification complexities by focusing on "equational consequences".

Proposition 19. *Let* $x \in \mathbb{A}^n_{R\to A}$, $\check{c}$ *be the restriction of* $c : \Omega^R \sqcup \mathbf{P} \to \mathbb{N}$ *on* Ω^R, $\Delta(c) = \min\{c(=), c(\leq)\} - c(-)$.

(1) *If* $\alpha' \subset \alpha$ *for* $\alpha,\alpha' \in \mathrm{Spec}_r A$ *with supports* $\mathfrak{p},\mathfrak{p}'$, *then*

$$V(c,x,\{\alpha\},\{\alpha,\alpha'\}) \geq E(\check{c},(x/\mathfrak{p}')_{\mathfrak{p}},\mathfrak{p}) + \Delta(c).$$

(2) *If* $\alpha \subset \beta \supset \alpha'$, $\alpha \neq \alpha'$ *for* $\alpha,\beta,\alpha' \in \mathrm{Spec}_r A$ *with supports* $\mathfrak{p},\mathfrak{q},\mathfrak{p}'$, *then*

$$V(c,x,\{\alpha\},\{\alpha,\alpha'\}) \geq \min_{\mathfrak{P}\in\{\mathfrak{p},\mathfrak{p}'\}} E(\check{c},(x/\mathfrak{P})_{\mathfrak{q}},\mathfrak{q}) + \Delta(c).$$

(3) *If* $\Delta(c) \geq 0$, *then*

$$V(c,x,\alpha) \geq I(\check{c},x_{\mathfrak{p}},\alpha)$$

for $\alpha \in \mathrm{Spec}_r A$ *with support* $\mathfrak{p}$, *and equality holds if* $c(-) = c(=) = c(\leq) = 0$.

(4) *If A is a field, $(B,\mathfrak{m}) \subset A$ a real discrete valuation ring then if $\alpha,\alpha' \in \mathrm{Spec}_r A$ are different and specialize in $\mathrm{Spec}_r B$ both into some β with support $\mathfrak{m}$, then*

$$V(c,x,\{\alpha\},\{\alpha,\alpha'\}) \geq S(\check{c},x,B) + \Delta(c).$$

((1)–(3) *hold analogously for prime ideals and* $\mathrm{P} = \{=\}$.)

Remark 20. We refer to the appendix for illustation and visualization in the geometric situation of the cases considered. Example A.2 shows various pictures of two prime cones with a common specialization.

Proof of Proposition 19. Let Υ be a respective verifier.

(1) Here $\Gamma(\Upsilon)$ is executable on $(x/\mathfrak{p}')_{\mathfrak{p}}$ since $(A/\mathfrak{p}')_{\mathfrak{p}} \to k(\mathfrak{p})$ is surst. Considering the first comparison in Υ which distinguishes $x(\alpha)$ and $x(\alpha')$ we get $f,g \in (A/\mathfrak{p}')_{\mathfrak{p}}$ appearing in $\mathrm{Res}(\Gamma(\Upsilon),(x/\mathfrak{p}')_{\mathfrak{p}})$ such that either $f(\alpha) \leq g(\alpha)$ and $f(\alpha') > g(\alpha')$ or $f(\alpha) = g(\alpha)$ and $f(\alpha') \neq g(\alpha')$; since α' is a generization of α other cases are impossible, and in both these cases we get $(f-g)(\alpha) = 0$.

(2) Passing to the initial segment $\Upsilon_{x(\alpha')}$ we may assume Υ to be executable on both $x(\alpha)$ and $x(\alpha')$. Consider the R-algebra morphisms

$$k(\mathfrak{p}) \leftarrow (A/\mathfrak{p})_{\mathfrak{q}} \to k(\mathfrak{q}) \leftarrow (A/\mathfrak{p}')_{\mathfrak{q}} \to k(\mathfrak{p}').$$

If Υ is not executable on $x(\beta)$, that is, $\Gamma(\Upsilon)$ is not on $x(\mathfrak{q})$, then $\Gamma(\Upsilon)$ is neither executable on $(x/\mathfrak{p})_{\mathfrak{q}}$ nor on $(x/\mathfrak{p}')_{\mathfrak{q}}$. Applying Proposition 3(1) to the outward morphisms we get even $L(\check{c},\Gamma(\Upsilon)) \geq \max_{\mathfrak{P} \in \{\mathfrak{p},\mathfrak{p}'\}} N(\check{c},(x/\mathfrak{P})_{\mathfrak{q}})$, hence the assertion in this case. So we may assume Υ to be executable on $x(\beta)$. Considering the first comparison in Υ distinguishing $x(\alpha)$ and $x(\alpha')$ we get $f,g \in A_{\mathfrak{q}}$ appearing in $\mathrm{Res}(\Gamma(\Upsilon),x_{\mathfrak{q}})$ such that one of the four alternatives must hold:

$$\begin{aligned}
&f(\alpha) \leq g(\alpha) \quad \text{and} \quad f(\alpha') > g(\alpha'),\\
&f(\alpha) > g(\alpha) \quad \text{and} \quad f(\alpha') \leq g(\alpha'),\\
&f(\alpha) = g(\alpha) \quad \text{and} \quad f(\alpha') \neq g(\alpha'),\\
&f(\alpha) \neq g(\alpha) \quad \text{and} \quad f(\alpha') = g(\alpha').
\end{aligned}$$

So in any case $(f-g)(\alpha) \neq 0$ or $(f-g)(\alpha') \neq 0$, and each of the four alternatives implies $(f-g)(\beta) = 0$ since β is a common specialization of α and α'.

(3) $\Gamma(\Upsilon)$ is executable on $x_{\mathfrak{p}}$, therefore Υ is executable on all $x(\beta)$, $\beta \in \mathrm{hal}\,\alpha$. Considering all comparisons in Υ distinguishing $x(\alpha)$ and at least one $x(\beta)$, $\beta \in \mathrm{hal}\,\alpha$, we get elements $f_1,g_1,\ldots f_m,g_m \in A_{\mathfrak{p}}$ appearing in $\mathrm{Res}(\Gamma(\Upsilon),x_{\mathfrak{p}})$ such that the system $f_1 = g_1,\ldots,f_m = g_m$ is satisfied for $\beta \in \mathrm{hal}\,\alpha$ if and only if $\beta = \alpha$.

(4) Here Υ is executable on both $x(\alpha)$ and $x(\alpha')$. Considering the first comparison in Υ distinguishing $x(\alpha)$ and $x(\alpha')$ we get $f,g \in A$ appearing in $\mathrm{Res}(\Gamma(\Upsilon),x)$ with $f(\alpha) \leq g(\alpha)$ and $f(\alpha') > g(\alpha')$ or $f(\alpha) > g(\alpha)$ and $f(\alpha') \leq g(\alpha')$. By the discrete valuation ring property of B, $f-g$ or its inverse lies in B. In the one case we get $(f-g)(\beta) = 0$, in the other case we get $(f-g)^{-1}(\beta) = 0$. Since for a unit $e \in B^{\times}$ the signs of $e(\alpha)$, $e(\alpha')$, and $e(\beta)$ are the same, the order of $f-g$ must be odd. □

Remark 21. (1) The lower bound in Proposition 19(2) may be not very tight since for instance sign and exclusion complexity in Lemma 16(2) may differ. In the other cases of 19 the lower bounds match quite well the verification complexities under reasonable assumptions on c.

(2) For the analogue of Proposition 19(3) for a prime ideal $\mathfrak{p}$ and $\mathrm{P} = \{=\}$ we have $V(c,x,\mathfrak{p}) \geq I(\check{c},x_{\mathfrak{p}},\mathfrak{p})$, and by Proposition 15. 2, $V(c,x,\mathfrak{p}) = V(c,x_{\mathfrak{p}},\mathfrak{p})$. Since $\mathrm{hal}\,\mathfrak{p}$ is homeomorphic to $\mathrm{Spec}\,A_{\mathfrak{p}}$ we have $I(\check{c},x_{\mathfrak{p}},\mathfrak{p}) = \min\{L(c,x,f) : \mathscr{Z}(f) = \{\mathfrak{p}\}\}$. For $\alpha \in \mathrm{Spec}_{\mathrm{r}}\,A$ one gets an analogous statement by passing to the image x_α in $\mathbb{A}^n_{R\to A_\alpha}$ of x where A_α denotes the *strict real localization* of A in α (cf. [38]) since $\mathrm{hal}\,\alpha$ is homeomorphic to $\mathrm{Spec}_{\mathrm{r}}\,A_\alpha$: $V(c,x,\alpha) = V(c,x_{\mathfrak{p}},\alpha) = V(c,x_\alpha,\alpha) \geq I(\check{c},x_{\mathfrak{p}},\alpha) = I(\check{c},x_\alpha,\alpha)$ (by Propositions 15(2) and 3(3)). For rational operations however, it is sufficient to pass to $x_{\mathfrak{p}}$.

Decision trees. Let $(N,\preceq)$ be a finite binary tree with predecessor relation $\preceq$, $N = N_{\mathrm{l}} \sqcup N_{\mathrm{b}} \sqcup N_{\mathrm{s}}$ the partition of the set of nodes into leaves, branching, and simple nodes. For $n \in \mathbb{N}$ we think $\preceq$ to be extended to $\{-n+1,\ldots,0\} \sqcup N$ by viewing $-n+1,\ldots,0$ as linearly ordered predecessors of the root of the tree. Let s_i denote program variables for $i \in \{-n+1,\ldots,0\} \sqcup N_{\mathrm{s}}$. An (Ω^R,P)-*decision tree* $\mathscr{T}$ *over* n is a *finite* binary tree $(N,\preceq)$ together with an instruction function that assigns

- to every simple node $i \in N_{\mathrm{s}}$ an operational instruction $s_i := \omega_i(s_{j_{i1}},\ldots,s_{j_{i\,\mathrm{ar}(\omega_i)}})$ where $\omega_i \in \Omega^R$, $-n+1 \preceq j_{ia} \prec i$, and $j_{ia} \notin N_b$ (that is, $j_{ia} \in \{-n+1,\ldots,0\} \sqcup N_{\mathrm{s}}$),
- to every branching node $i \in N_{\mathrm{b}}$ a test instruction $s_{h_i}\rho_i s_{h_i'}$ where $\rho_i \in \mathrm{P}$, $-n+1 \preceq h_i, h_i' \prec i$, and $h_i, h_i' \notin N_{\mathrm{b}}$,
- to every leaf $i \in N_{\mathrm{l}}$ a label for cases, $\mathrm{case}_i \in \{1,\ldots,r\}$.

A path in the underlying binary tree from the root to a node together with the restriction of the instruction function is called a *path in* $\mathscr{T}$. An *input* for $\mathscr{T}$ is a point $\alpha \in \mathrm{Spec}_{\mathrm{r}}\,R[X]$ (resp. $\mathfrak{p} \in \mathrm{Spec}\,R[X]$) identifying as above α and $X(\alpha)$. (For $\mathrm{P} = \{=\}$ the following definitions apply analogously to $\mathfrak{p} \in \mathrm{Spec}\,R[X]$). If α is fed into $\mathscr{T}$ it defines its path in $\mathscr{T}$, denoted $\mathscr{T}_\alpha$, by executing the instructions of $\mathscr{T}$ successively in the ordered field $(k(\mathrm{supp}\,\alpha),\leq_\alpha)$ over R, continuing in a branching node with the right successor if the truth value of the outcome of its test is "yes", and with the left one if it is "no". Should an unexecutable division instruction occur $\mathscr{T}_\alpha$ ends right before it. $\mathscr{T}$ is said to be executable on α if $\mathscr{T}_\alpha$ ends up with a leaf. To $\mathscr{T}_\alpha$ is assigned an (Ω^R,P)-SLP $\Upsilon(\mathscr{T}_\alpha)$ in the obvious way, and $\mathscr{T}_\alpha$ is uniquely represented by the pair $(\Upsilon(\mathscr{T}_\alpha),\mathrm{tr}(\Upsilon(\mathscr{T}_\alpha),\alpha))$, that is, the outcome of the tests is the additional information coded in the path $\mathscr{T}_\alpha$. Notationally, we will however not distinguish between $\mathscr{T}_\alpha$ and $\Upsilon(\mathscr{T}_\alpha)$. By the above convention $\mathscr{T}_\alpha$ is not nilly.

If $\alpha,\beta,\ldots \in \mathrm{Spec}_{\mathrm{r}}\,R[X]$ then $\mathscr{T}_{\alpha,\beta,\ldots}$ denotes the common piece of the paths $\mathscr{T}_\alpha, \mathscr{T}_\beta, \ldots$. Let $\mathrm{Ex}\,\mathscr{T} \subseteq \mathrm{Spec}_{\mathrm{r}}\,R[X]$ denote the subset of all α such that $\mathscr{T}$ is executable on α, and for $\alpha \in \mathrm{Spec}_{\mathrm{r}}\,R[X]$ let $\mathrm{Cell}(\mathscr{T},\alpha) = \{\beta : \mathscr{T}_\beta = \mathscr{T}_\alpha\} \subseteq \mathrm{Spec}_{\mathrm{r}}\,R[X]$. Clearly, $\mathrm{Ex}\,\mathscr{T} = \bigcup\{\mathrm{Cell}(\mathscr{T},\alpha) : \alpha \in \mathrm{Ex}\,\mathscr{T}\}$, and by the finiteness of $\mathscr{T}$ this union can be written as a finite one by selecting finitely many $\alpha \in \mathrm{Ex}\,\mathscr{T}$.

The following statements are all evident.

Lemma 22. (1) $\mathrm{Cell}(\mathscr{T},\alpha)$ *is an elementary locally closed subset of* $\mathrm{Spec}_r R[X]$.

(2) $\mathrm{Ex}\,\mathscr{T}$ *is a constructible subset of* $\mathrm{Spec}_r R[X]$.

(3) *If* $\alpha \in \mathrm{Ex}\,\mathscr{T}$, *then* $\mathscr{T}_\alpha$ *verifies* $\mathrm{Cell}(\mathscr{T},\alpha)$ *in* $\mathrm{Ex}\,\mathscr{T}$.

(4) *If* $\alpha \in \overline{\mathscr{Z}(\mathrm{supp}\,\alpha)\cap E}$ *for a subset* $E \subseteq \mathrm{Spec}_r R[X]$, *then* $\mathrm{Cell}(\mathscr{T},\alpha)\cap E \neq \emptyset$.
(*Analogously for prime ideals and* $\mathrm{P} = \{=\}$.)

Let $E_1,\ldots,E_r$ be pairwise disjoint and non-empty subsets of $\mathrm{Spec}_r R[X]$. The decision tree $\mathscr{T}$ is said to *decide* the partition $\mathscr{E} = \{E_1,\ldots,E_r\}$ of their union if for every $j = 1,\ldots,r$ and for every $\alpha \in E_j$ the path $\mathscr{T}_\alpha$ leads to a case j leaf. (Throughout this paper $r = 2$.)

Complexity. The *decision complexity* $C(c,\mathscr{E})$ with respect to $c : \Omega^R \sqcup \mathrm{P} \to \mathbb{N}$ is defined as the minimum *c-cost* $C(c,\mathscr{T}) = \max_{\alpha\in\bigcup\mathscr{E}} L(c,\mathscr{T}_\alpha)$ of a decision tree over n for $\mathscr{E}$.

The following two propositions, 23 and 26 below, combine the information about what paths in decision trees verify with the bounds in Proposition 19; some statements are specific for the real spectrum, some for the Zariski spectrum.

Proposition 23. *Let* $\mathrm{P} = \{=,\leq\}$, *and* $\check{c}$ *be the restriction of* $c : \Omega^R \sqcup \mathrm{P} \to \mathbb{N}$ *on* Ω^R, $\Delta(c) = \min\{c(=),c(\leq)\} - c(-)$. *Let* $\mathscr{T}$ *be an* (Ω^R,P)*-decision tree over* n *for* $\{E,E'\}$ *where* $E,E' \subseteq \mathrm{Spec}_r R[X]$ *are disjoint.*

(1) *If* $\alpha' \subset \alpha$ *with supports* $\mathfrak{p}' \subset \mathfrak{p}$ *satisfy* $\alpha \in \overline{\mathscr{Z}(\mathfrak{p})\cap E}$ *and* $\alpha' \in \overline{\mathscr{Z}(\mathfrak{p}')\cap E'}$, *then*

$$L(c,\mathscr{T}_{\alpha,\alpha'}) \geq E(\check{c},(X/\mathfrak{p}')_{\mathfrak{p}},\mathfrak{p}) + \Delta(c).$$

(2) *If* $\alpha \subset \beta \supset \alpha'$ *with supports* $\mathfrak{p} \subset \mathfrak{q} \supset \mathfrak{p}'$ *satisfy* $\alpha \in \overline{\mathscr{Z}(\mathfrak{p})\cap E}$ *and* $\alpha' \in \overline{\mathscr{Z}(\mathfrak{p}')\cap E'}$, *then*

$$L(c,\mathscr{T}_{\alpha,\beta,\alpha'}) \geq \min_{\mathfrak{P}\in\{\mathfrak{p},\mathfrak{p}'\}} E(\check{c},(X/\mathfrak{P})_{\mathfrak{q}},\mathfrak{q}) - |\Delta(c)|.$$

(3) *Let* $\mathfrak{a} \subset R[X]$ *be an ideal, and assume* α *with support* $\mathfrak{p} \supseteq \mathfrak{a}$ *to satisfy* $\alpha \in \overline{\mathscr{Z}(\mathfrak{p})\cap E}$, *and all its proper generizations* $\alpha' \in \mathrm{hal}\,\alpha \cap \mathscr{Z}(\mathfrak{a})$ *to satisfy* $\alpha' \in \overline{\mathscr{Z}(\mathrm{supp}\,\alpha')\cap E'}$. *Then if* $\Delta(c) \geq 0$,

$$L(c,\mathscr{T}_\alpha) \geq I(\check{c},(X/\mathfrak{a})_{\mathfrak{p}},\alpha).$$

(4) *Assume* α,α' *to have both support* $\mathfrak{p}$, $\alpha \in \overline{\mathscr{Z}(\mathfrak{p})\cap E}$ *and* $\alpha' \in \overline{\mathscr{Z}(\mathfrak{p})\cap E'}$. *If* $(B,\mathfrak{m}) \subset k(\mathfrak{p})$ *is a real discrete valuation ring, and* α,α' *both specialize in* $\mathrm{Spec}_r B$ *into some* β *with support* $\mathfrak{m}$, *then*

$$L(c,\mathscr{T}_{\alpha,\alpha'}) \geq S(\check{c},X(\mathfrak{p}),B) + \Delta(c).$$

Proof. (1) By Lemma 22(4) one has $\alpha,\alpha' \in \mathrm{Ex}\,\mathscr{T}$, and $\mathscr{T}_\alpha \neq \mathscr{T}_{\alpha'}$. By Lemma 22. (3) and Proposition 14(2) $\mathscr{T}_\alpha$ verifies $\{\alpha\}$ in $\{\alpha,\alpha'\}$, so $\mathscr{T}_{\alpha,\alpha'}$ too, and one can use Proposition 19(1).

(2) Here, $\mathscr{T}_{\alpha,\alpha'}$ verifies $\{\alpha\}$ in $\{\alpha,\alpha'\}$, and one can use Proposition 19(2) if $\mathscr{T}_{\alpha,\alpha'} = \mathscr{T}_{\alpha,\beta,\alpha'}$. Otherwise, either $\mathscr{T}_{\alpha,\beta,\alpha'}$ verifies $\{\beta\}$ in $\{\beta,\alpha\}$ or $\{\beta\}$ in $\{\beta,\alpha'\}$ and then one

can use Proposition 19(1), or $\mathscr{T}_{\alpha,\alpha'}$ is not executable on β and then $L(c,\mathscr{T}_{\alpha,\beta,\alpha'}) \geq \max_{\mathfrak{P}\in\{\mathfrak{p},\mathfrak{p}'\}} E(\check{c},(X/\mathfrak{P})_{\mathfrak{q}},\mathfrak{q})$.

(3) and (4) follow using Proposition 19(3) and (4). □

For a real closed field R and a *semi-algebraic* subset $E\subseteq R^n$ the crucial condition $\alpha \in \overline{\mathscr{Z}(\operatorname{supp}\alpha)\cap E}$ is equivalent to $\alpha\in\tilde{E}$, $\tilde{E}\subseteq \operatorname{Spec}_r R[X]$ denoting the associated constructible set (cf. [8, 7.2]). In applications however often $R=\mathbb{Q}$ and subsets $E\subseteq\mathbb{Q}^n$ appear. Practical examples (linear algebra, linear programming, etc.) often lead to vanishing ideals that are extensions of rational or at least unirational prime ideals in $\mathbb{Q}[X]$. This makes clear the more general formulations which nevertheless may lead to at least some fragmentary information. We leave it to the reader to check the lower bounds in Section 7 below to hold true for rational inputs as well.

For real closed fields R the operation tilde provides the perfect correspondence between semi-algebraic partitions $\mathscr{F}$ in R^n and constructible partitions $\tilde{\mathscr{F}}$ in $\operatorname{Spec}_r R[X]$. If $U\subseteq R^n$ is a semi-algebraic open subset then a semi-algebraic partition $\{F,F'\}$ in R^n is said to be *U-full* if $F\cup F'\supseteq U$. The minimal prime cones in the tilde of the common boundary $\bar{F}\cap\bar{F}'$ will be complexity creating prime cones.

We summarize these consequences for semi-algebraic decision trees explicitly.

Theorem 24. *Let R be a real closed field, and $\mathscr{T}$ be an (Ω^R,P)-decision tree over n, $\mathrm{P}=\{=,\leq\}$, $\mathscr{F}$ a semi-algebraic partition in R^n.*

(1) *$\mathscr{T}$ decides the semi-algebraic partition $\mathscr{F}$ iff $\mathscr{T}$ decides the constructible partition $\tilde{\mathscr{F}}$.*

(2) *Assume $\mathscr{F}=\{F,F'\}$. Then $\beta\in\operatorname{Spec}_r R[X]$ possesses generizations $\alpha\in\tilde{F}$, $\alpha'\in\tilde{F}'$ iff $\beta\in(\bar{F}\cap\bar{F}')^{\sim}$. Furthermore,*

$$\dim\bar{F}\cap\bar{F}'\leq\min\{\dim F,\dim F'\},\quad \dim\bar{F}\cap\bar{F}'<\max\{\dim F,\dim F'\}.$$

(3) *Let $\mathscr{F}=\{F,F'\}$ be U-full for some semi-algebraic open $U\subseteq R^n$, and assume $\mathscr{T}$ to decide $\mathscr{F}$. Then for every minimal prime cone β of $(U\cap\bar{F}\cap\bar{F}')^{\sim}$ precisely one of the following three statements holds true:*

(a) *$\beta\in\tilde{F}^{\min}$, $\operatorname{hal}\beta\setminus\{\beta\}\subseteq\tilde{F}'$, and $\mathscr{T}_\beta$ verifies $\{\beta\}$ in $\operatorname{hal}\beta$.*

(b) *$\beta\in\tilde{F}'^{\min}$, $\operatorname{hal}\beta\setminus\{\beta\}\subseteq\tilde{F}$, and $\mathscr{T}_\beta$ verifies $\{\beta\}$ in $\operatorname{hal}\beta$.*

(c) *$\beta\notin\tilde{F}^{\min}\cup\tilde{F}'^{\min}$, $\dim\beta=n-1$, then β has exactly two proper generizations $\alpha\in\tilde{F}$, $\alpha'\in\tilde{F}'$ (both of support 0), $\operatorname{hal}\beta=\{\alpha,\beta,\alpha'\}$, and $\mathscr{T}_\beta$ verifies $\{\alpha\}$, $\{\beta\}$, or $\{\alpha'\}$ in $\operatorname{hal}\beta$.*

Proof. (1) This is an immediate consequence of [8, 7.2.3]. In fact, if $\mathscr{F}=\{F_1,\ldots,F_r\}$, $\tilde{\mathscr{F}}=\{\tilde{F}_1,\ldots,\tilde{F}_r\}$, then we have $\tilde{F}_i\cap\tilde{F}_j=(F_i\cap F_j)^{\sim}=\emptyset=\emptyset$, so $\tilde{\mathscr{F}}$ is indeed a partition in $\operatorname{Spec}_r R[X]$. If $\mathscr{T}$ decides $\mathscr{F}$ then for each i

$$F_i=\bigcup\{\operatorname{Cell}(\mathscr{T},\xi_i)\cap R^n:\xi_i\in F_i\}\cap\bigcup\mathscr{F}.$$

Since $\mathscr{T}$ is a *finite* tree, these unions of cells can be written as finite unions by selecting for every i finitely many $\xi_i \in F_i$. So by the tilde,

$$\tilde{F}_i = \bigcup\{\mathrm{Cell}(\mathscr{T}, \xi_i) : \xi_i \in F_i\} \cap \bigcup \tilde{\mathscr{F}}$$

and $\mathscr{T}$ decides $\tilde{\mathscr{F}}$. The reverse is clear.

(2) Again by [8, 7.2.3],

$$(\bar{F} \cap \bar{F}')^{\sim} = \bar{\tilde{F}} \cap \bar{\tilde{F}'},$$

and by [8, 7.1.20], $\beta \in \mathrm{Spec}_r R[X]$ possesses generizations in $\tilde{F}$ and in $\tilde{F}'$ iff β appears in $\bar{\tilde{F}}$ and in $\bar{\tilde{F}'}$.

Since the dimension of a semi-algebraic set is the maximum dimension of a prime cone in its tilde ([8, 7.5.6]) we have $\dim \bar{F} \cap \bar{F}' \leq \min\{\dim F, \dim F'\}$ and $\dim \bar{F} \cap \bar{F}' < \max\{\dim F, \dim F'\}$; every minimal $\beta \in (\bar{F} \cap \bar{F}')^{\sim}$ possesses generizations $\alpha \in \tilde{F}$ and $\alpha' \in \tilde{F}'$, and one of them is a proper generization of β by $\tilde{F} \cap \tilde{F}' = \emptyset$.

(3) We may assume $F \cup F' = U$. Let $\beta \in ((U \cap \bar{F} \cap \bar{F}')^{\sim})^{\min}$. Since U is open, $\mathrm{hal}\,\beta \subset \tilde{U}$ [8, 7.1.21], and $\mathrm{hal}\,\beta \setminus \{\beta\} \neq \emptyset$ by $\dim \beta \leq n-1$. If $\beta \in \tilde{F}^{\min}$ then $\mathrm{hal}\,\beta \setminus \{\beta\} \subset \tilde{F}'$, and for every $\alpha \in \mathrm{hal}\,\beta \setminus \{\beta\}$ the paths $\mathscr{T}_\alpha$ and $\mathscr{T}_\beta$ end with different leaves; thus, $\mathscr{T}_\beta$ verifies $\{\beta\}$ in $\mathrm{hal}\,\beta$. Analogously, for $\beta \in \tilde{F'}^{\min}$.

Assume now $\beta \notin \tilde{F}^{\min} \cup \tilde{F'}^{\min}$, and let $\alpha \in \tilde{F}$, $\alpha' \in \tilde{F}'$ be proper generizations of β. Since β is minimal in $(U \cap \bar{F} \cap \bar{F}')^{\sim}$ we have $\mathrm{hal}\,\alpha \subset \tilde{F}$, $\mathrm{hal}\,\alpha' \subset \tilde{F}'$; that is, $\alpha \in \mathrm{int}_{\tilde{U}} \tilde{F}$, $\alpha' \in \mathrm{int}_{\tilde{U}} \tilde{F}'$. We now show that $\dim \beta = n-1$; then α and α' both have support 0 and are the solely possible generizations of β [8, 10.2.6]. By way of contradiction assume $\dim \beta \leq n-2$. We have the disjoint decomposition

$$\tilde{U} = \mathrm{int}_{\tilde{U}} \tilde{F} \cup (U \cap \bar{F} \cap \bar{F}')^{\sim} \dot{\cup}\, \mathrm{int}_{\tilde{U}} \tilde{F}'. \tag{4.1}$$

Since $\dim \beta \leq n-2$ there is an open semi-algebraically connected subset $W \subset U$ such that

$$\dim W \cap \bar{F} \cap \bar{F}' \leq n-2 \text{ and } \beta \in \tilde{W}. \tag{4.2}$$

(Otherwise, one could choose an algebraic set B of dimension $n-2$ such that $\beta \in \tilde{B}$, and

$$\dim W \cap ((\bar{F} \cap \bar{F}') \setminus B) = n-1$$

for every open W with $\beta \in \tilde{W}$. Since the $\tilde{W}$ and $(\bar{F} \cap \bar{F}')^{\sim} \setminus \tilde{B}$ are compact for the constructible topology [8, 7.1.12], $(\bar{F} \cap \bar{F}')^{\sim} \setminus \tilde{B}$ would contain a proper generization γ of β, contradicting $\beta \in ((\bar{F} \cap \bar{F}')^{\sim})^{\min}$.) But (4.2) implies that $W \setminus (\bar{F} \cap \bar{F}')$ is semi-algebraically connected. So the connected components of $\mathrm{int}_{\tilde{U}} \tilde{F}$ and $\mathrm{int}_{\tilde{U}} \tilde{F}'$ in which α and α' lie are the same, contradicting the disjointness of the decomposition (4.1).

Therefore $\dim \beta = n-1$. The common path $\mathscr{T}_{\alpha,\beta,\alpha'}$ of all three (and hence $\mathscr{T}_\beta$) now verifies $\{\alpha\}$, $\{\beta\}$, or $\{\alpha'\}$ in $\mathrm{hal}\,\beta$ since either $\mathscr{T}_\alpha \neq \mathscr{T}_{\beta,\alpha'}$ or $\mathscr{T}_\beta \neq \mathscr{T}_{\alpha,\alpha'}$ or $\mathscr{T}_{\alpha'} \neq \mathscr{T}_{\alpha,\beta}$. □

The tilde furthermore provides information about the set of points in R^n producing a long path in a decision tree and its dimensionality.

Proposition 25. *Let R be a real closed field, and $\mathscr{T}$ be an (Ω^R, P)-decision tree over n, $\mathrm{P} = \{=, \leq\}$.*

(1) *For any irreducible algebraic subset $E \subset R^n$ and any minimal prime cone $\alpha \in (\mathrm{Reg}\, E)^\sim$ the trace $\mathrm{Cell}(\mathscr{T}, \alpha) \cap E$ of $\mathrm{Cell}(\mathscr{T}, \alpha)$ in E is an elementary locally closed semi-algebraic subset of E of maximal dimension $\dim E$.*
Assume $\mathscr{T}$ to decide a semi-algebraic partition $\{F, F'\}$, and let $\check{c}$ be the restriction of $c : \Omega^R \sqcup \mathrm{P} \to \mathbb{N}$ on Ω^R, $\Delta(c) = \min\{c(=), c(\leq)\} - c(-)$.

(2) *If*

$$e = e(\check{c}, \bar{F} \cap \bar{F}') = \min\{E(\check{c}, X_{\mathrm{supp}\,\alpha}, \mathrm{supp}\,\alpha) : \alpha \in ((\bar{F} \cap \bar{F}')^\sim)^{\min}\},$$

then the subset

$$\{\xi \in \bar{F} \cap \bar{F}' : L(c, \mathscr{T}_\xi) < e - |\Delta(c)|\}$$

of all points in the common boundary of F and F' producing a path in $\mathscr{T}$ of shorter length than $e + \Delta(c)$ is a semi-algebraic subset of $\bar{F} \cap \bar{F}'$ of dimension strictly less than $\dim \bar{F} \cap \bar{F}'$.

(3) *If $\{F, F'\}$ is U-full for some semi-algebraic open $U \subseteq R^n$, $\Delta(c) \geq 0$, and*

$$i = i(\check{c}, U \cap \bar{F} \cap \bar{F}') = \min\{I(\check{c}, X_{\mathrm{supp}\,\alpha}, \alpha) : \alpha \in ((U \cap \bar{F} \cap \bar{F}')^\sim)^{\min}\},$$

then the subset

$$\{\xi \in U \cap \bar{F} \cap \bar{F}' : L(c, \mathscr{T}_\xi) < i\}$$

of all points in the boundary of $U \cap F$ in U producing a path in $\mathscr{T}$ of shorter length than i is a semi-algebraic subset of $U \cap \bar{F} \cap \bar{F}'$ of dimension strictly less than $\dim U \cap \bar{F} \cap \bar{F}'$.

As a consequence, if $\mathscr{T}$ decides membership in an irreducible algebraic subset $F \subset R^n$, then there is a non-void Zariski open subset $G \subseteq F$ such that for all $\xi \in G$ the path length is bounded below as

$$L(c, \mathscr{T}_\xi) \geq i(\check{c}, F).$$

Proof. (1) For $\alpha \in \tilde{E}$ we have $\dim \alpha = \dim E$ iff

$$\alpha \in ((\mathrm{Reg}\, E)^\sim)^{\min} = \mathrm{Spec}_r\, k(E)$$

([8, 7.6.1 and 2]). So by [8, 7.5.8] $\dim \mathrm{Cell}(\mathscr{T}, \alpha) \cap E \geq \dim \alpha = \dim E$ if $\alpha \in ((\mathrm{Reg}\, E)^\sim)^{\min}$.

(2) If $\dim \beta = \dim \bar{F} \cap \bar{F}'$ and

$$\beta \in \{\xi \in \bar{F} \cap \bar{F}' : L(c, \mathscr{T}_\xi) < e - |\Delta(c)|\}^\sim, \tag{4.3}$$

then $\beta \in ((\tilde{F} \cap \tilde{F'})^{\sim})^{\min}$ and possesses generizations $\alpha \in \tilde{F}$, $\alpha' \in \tilde{F'}$ by Theorem 24(2) one of them proper. Relation (4.3), Proposition 23(1) or (2) and Lemma 16(1) imply the contradiction

$$e - |\Delta(c)| > L(c, \mathscr{T}_\beta) \geq L(c, \mathscr{T}_{\alpha,\beta,\alpha'}) \geq e - |\Delta(c)|.$$

(3). Analogously, using Theorem 24(3) and Proposition 23(3) for the cases (a) and (b) in Theorem 24(3) and Proposition 23(1) together with Lemma 16(3) for the case (c) in Theorem 24(3). □

For comparison we now turn to similar statements as in Proposition 23 for the order-free case. Statements (4) and (5) in the next proposition have no real counterpart since the specializations of a prime cone form a totally ordered chain [8, 7.1.22]; the first three statements are completely analogous to the above ones in Proposition 23.

Proposition 26. *Let* $\mathrm{P} = \{=\}$, *and* $\check{c}$ *be the restriction of* $c : \Omega^R \sqcup \mathrm{P} \to \mathbb{N}$ *on* Ω^R, $\Delta(c) = c(=) - c(-)$. *Let* $\mathscr{T}$ *be an* (Ω^R, P)*-decision tree over* n *for* $\{E, E'\}$ *where* $E, E' \subseteq \operatorname{Spec} R[X]$ *are disjoint.*

(1) *If* $\mathfrak{p}' \subset \mathfrak{p}$ *satisfy* $\mathfrak{p} \in \overline{\mathscr{Z}(\mathfrak{p}) \cap E}$ *and* $\mathfrak{p}' \in \overline{\mathscr{Z}(\mathfrak{p}') \cap E'}$, *then*

$$L(c, \mathscr{T}_{\mathfrak{p},\mathfrak{p}'}) \geq E(\check{c}, (X/\mathfrak{p}')_{\mathfrak{p}}, \mathfrak{p}) + \Delta(c).$$

(2) *If* $\mathfrak{p} \subset \mathfrak{q} \supset \mathfrak{p}'$ *satisfy* $\mathfrak{p} \in \overline{\mathscr{Z}(\mathfrak{p}) \cap E}$ *and* $\mathfrak{p}' \in \overline{\mathscr{Z}(\mathfrak{p}') \cap E'}$, *then*

$$L(c, \mathscr{T}_{\mathfrak{p},\mathfrak{q},\mathfrak{p}'}) \geq \min_{\mathfrak{P} \in \{\mathfrak{p},\mathfrak{p}'\}} E(\check{c}, (X/\mathfrak{P})_{\mathfrak{q}}, \mathfrak{q}) - |\Delta(c)|.$$

(3) *Let* $\mathfrak{a} \subset R[X]$ *be an ideal,* $\mathfrak{a} \subseteq \mathfrak{p} \in \overline{\mathscr{Z}(\mathfrak{p}) \cap E}$, *and assume all proper generizations* $\mathfrak{p}' \in \operatorname{hal} \mathfrak{p} \cap \mathscr{Z}(\mathfrak{a})$ *to satisfy* $\mathfrak{p}' \in \overline{\mathscr{Z}(\mathfrak{p}') \cap E'}$. *Then if* $\Delta(c) \geq 0$,

$$L(c, \mathscr{T}_{\mathfrak{p}}) \geq I(\check{c}, (X/\mathfrak{a})_{\mathfrak{p}}, \mathfrak{p}).$$

(4) *If* $\mathfrak{p} \supset \mathfrak{Q} \subset \mathfrak{p}'$ *satisfy* $\mathfrak{p} \in \overline{\mathscr{Z}(\mathfrak{p}) \cap E}$ *and* $\mathfrak{p}' \in \overline{\mathscr{Z}(\mathfrak{p}') \cap E'}$, *then*

$$L(c, \mathscr{T}_{\mathfrak{p},\mathfrak{Q},\mathfrak{p}'}) \geq \min_{\mathfrak{P} \in \{\mathfrak{p},\mathfrak{p}'\}} E(\check{c}, (X/\mathfrak{Q})_{\mathfrak{P}}, \mathfrak{P}) + \Delta(c).$$

(5) *If* $\mathfrak{p} \subset \mathfrak{q} \supset \mathfrak{p}'$, $\mathfrak{p} \supset \mathfrak{Q} \subset \mathfrak{p}'$, $\mathfrak{p} \in \overline{\mathscr{Z}(\mathfrak{p}) \cap E}$ *and* $\mathfrak{p}' \in \overline{\mathscr{Z}(\mathfrak{p}') \cap E'}$, *then*

$$L(c, \mathscr{T}_{\mathfrak{p},\mathfrak{p}',\mathfrak{q},\mathfrak{Q}}) \geq E(\check{c}, (X/\mathfrak{Q})_{\mathfrak{q}}, \mathfrak{q}) - |\Delta(c)|.$$

Proof. (4) Since $\mathscr{T}_{\mathfrak{p},\mathfrak{p}'}$ verifies $\{\mathfrak{p}\}$ in $\{\mathfrak{p}, \mathfrak{p}'\}$ and $\mathscr{T}_{\mathfrak{p},\mathfrak{p}'}$ is executable on the common generization $\mathfrak{Q}$, $\mathscr{T}_{\mathfrak{p},\mathfrak{Q},\mathfrak{p}'}$ must verify $\{\mathfrak{p}\}$ in $\{\mathfrak{p}, \mathfrak{Q}\}$ or $\{\mathfrak{p}'\}$ in $\{\mathfrak{p}', \mathfrak{Q}\}$. So the statement follows from the analogue of Proposition 19(1) for prime ideals.

(5) The initial segment $\mathscr{T}_{\mathfrak{p},\mathfrak{p}',\mathfrak{q},\mathfrak{Q}}$ of $\mathscr{T}_{\mathfrak{p},\mathfrak{p}',\mathfrak{q}}$ and $\mathscr{T}_{\mathfrak{p},\mathfrak{p}',\mathfrak{Q}}$ coincides with one of them. So the statement follows from (2) and (3) together with Lemma 16(1).

We skip the (straightforward) discussion of similar consequences as in Theorem 24 and Proposition 25 for the order-free case and finally we mention the two degree based

lower bounds on verification complexities due to Strassen [47] and Ben-Or [4] which we will extend in the next section.

For isolation complexity of prime ideals one has the following lower bound which is contained in [47] together with Proposition 26(3); precisely one extracts from [47]:

Theorem 27 (Strassen [47]). *Let R be a field, $\mathfrak{p} \supseteq \mathfrak{p}'$ prime ideals in $R[X]$. Then for the multiplicative cost function*

$$V(c_*, X/\mathfrak{p}', \mathfrak{p}) = I(c_*, (X/\mathfrak{p}')_{\mathfrak{p}}, \mathfrak{p}) \geq \log_2 \deg X(\mathfrak{p}) - \log_2 \deg X(\mathfrak{p}').$$

The proof of this result is based on Theorem 9 and the reduced Bézout's inequality 5(7), since $(R[X]/\mathfrak{p}')_{\mathfrak{p}}$ does not need to be Cohen–Maccaulay.

It is easy to see by examples that a respective analogue of Theorem 27 for isolation complexity of prime cones does not hold in general, at least in its relative form when $\mathfrak{p}' \neq 0$. In the real case there is however an other way to use the degree argument due to Ben-Or which is based on a result by Milnor [29] and Thom [48]. (See also the further developments mentioned in the introduction.)

Theorem 28 (Ben-Or [4]). *Let R be a real closed field, and $E \subseteq \operatorname{Spec}_r R[X]$ an elementary locally closed subset. Then for $c_{*,\leq} = 1_{\{*,/,=,\leq\}}$,*

$$V(c_{*,\leq}, E, \operatorname{Spec}_r R[X]) \geq \frac{\log_2 \sharp E}{\log_2 3} - n,$$

where $\sharp E$ denotes the number of connected components of E.

This theorem yields a global type lower bound on decision trees by considering the union of all cells of all paths of points of the decided set [4]. But it also implies lower bounds on isolation complexity.

Corollary 29. *Let R be a real closed field.*

(1) *If $f \in R[X]$ is irreducible, $\mathfrak{p} = fR[X]$, then*

$$I(c_*, X_{\mathfrak{p}}, \mathfrak{p}) \geq \frac{\log_2 \sharp \operatorname{Spec}_r R[X]_f}{\log_2 9} - \frac{n+1}{2}.$$

(2) *If $f \in \mathbb{A}^m_{R \to R(X)}$, all $f_i \notin R$, and $p \in R[X_1, \ldots, X_n]$ represents the product of all prime divisors appearing in at least one of the f_i, then*

$$L(c_*, X(0), f) \geq \frac{\log_2 \sharp \operatorname{Spec}_r R[X]_p}{\log_2 9} - \frac{n+m}{2}.$$

Proof. (2) If Γ with universal input $u_\Gamma \in \mathbb{A}^n_{R \to A_\Gamma}$ computes f on $X(0)$ then one can manufacture a verifier for $\operatorname{Spec}_r(A_\Gamma)_{\Pi f_i}$ in $\operatorname{Spec}_r R[X]$ by introducing for each division step and each f_i a zero test; hence, the assertion follows by Theorem 28 and $\sharp \operatorname{Spec}_r(A_\Gamma)_{\Pi f_i} \geq \sharp \operatorname{Spec}_r R[X]_p$.

(1) By (2), using again $\#\operatorname{Spec}_r[X]_p \geq \#\operatorname{Spec}_r R[X]_f$ for non-zero multiples $p \in R[X]$ of f. □

5. Degree-derivation bounds

In the next proposition we give a degree analysis in the derivation theorem given in [26] and [2] (see also [34]) and consider a variant of it for Euler derivations which takes additive operations into account as well. (The bound based on Euler derivations has been motivated by Morgenstern [33, Théorème 20], and has been found independently by Strassen.)

Proposition 30. *Let R be a field, $f \in R(X)$, and $\partial f = (\partial_1 f, \ldots, \partial_n f) \in \mathbb{A}^n_{R \to R(X)}$, $\partial_E f = (X_1 \partial_1 f, \ldots, X_n \partial_n f) \in \mathbb{A}^n_{R \to R(X)}$. Then*

(1) $L(c_*, X(0), f) \geq (1/\log_2 6) \log_2 \deg X(0) f \partial f$,

(2) $L(c_{+,*}, X(0), f) \geq \log_2 \deg X(0) f \partial_E f$ *for* $c_{+,*} = 1_{\{+,-,*,/\}}$.

Proof. Let $A = R[X]$, $S \subseteq A \setminus \{0\}$ be an arbitrary multiplicative system and X_S the image of X in $\mathbb{A}^n_{R \to A_S}$. Let $\Gamma = (\Gamma_1, \ldots, \Gamma_t)$ be an Ω^R-SLP over n, executable on X_S, with result sequence $\operatorname{Res}(\Gamma, X_S) = (X_1, \ldots, X_n, r_1, \ldots, r_t)$.

(1) We show by induction on t that if (Γ, X_S) computes some $f \in A_S$ then

$$\deg X_S f \partial f \leq 6^{L(c_*, \Gamma)}. \tag{5.1}$$

This is clear if $t = 0$. For $t \geq 1$, let $\Gamma' = (\Gamma'_2, \ldots, \Gamma'_t)$ denote the Ω^R-SLP over $n+1$ obtained from Γ by deleting the first instruction Γ_1 and replacing in all successor instructions calls to the result of the first one by calls to an additional new input component. Let $A' = A[X_0]$, and let $S' \subseteq A' \setminus \{0\}$ denote the preimage of $A_S^\times$ under the substitution $\sigma : A' \to A_S$, $X_0 \mapsto r_1$, extending $A \to A_S$. By construction, Γ' is executable on $X'_{S'} = (X_0, \ldots, X_n) \in \mathbb{A}^{n+1}_{R \to A'_{S'}}$ and computes some $f' \in A'_{S'}$ with $\sigma_{S'}(f') = f$. By the inductive hypothesis

$$\deg X'_{S'} f' \partial' f' \leq 6^{L(c_*, \Gamma')},$$

where $\partial' f' = (\partial_0 f', \ldots, \partial_n f')$, and the chain rule gives

$$\partial_i f = \sigma_{S'}(\partial_i f') + \sigma_{S'}(\partial_0 f') \cdot (\partial_i r_1) \quad \text{for } i \geq 1. \tag{5.2}$$

Now (5.1) follows from the inductive hypothesis by considering for every $\omega_1 \in \Omega^R$ the case that r_1 results in instruction Γ_1 from an application of ω_1. Leaving the discussion of a linear operation to the reader, we exemplarily inspect the case when $\omega_1 \in \{*, /\}$ and assume for concreteness the arguments to be X_1 and X_2, so $r_1 = X_1 \cdot X_2$ resp. $r_1 = X_1 / X_2$. Then $\partial_i r_1 = 0$ for $2 < i \leq n$, and $\partial_1 r_1 = X_2$, $\partial_2 r_1 = X_1$ resp. $\partial_1 r_1 = 1/X_2$, $\partial_2 r_1 = (-1/X_1) \cdot (X_1/X_2)$. Using a vector operation of degree 3 and one of degree 2

according to Lemma 31(1) below to produce $y = (X_1 \cdot X_2, \partial_0 f' \cdot X_2, \partial_0 f' \cdot X_1)$ resp. $y = (X_1/X_2, \partial_0 f'/X_2, \partial_0 f' \cdot X_0/X_2)$ Lemma 8 yields

$$\deg X'_{S'} f'(\partial' f') y \leq 6^{L(c_*,\Gamma')+1} = 6^{L(c_*,\Gamma)}.$$

Now applying the substitution $\sigma_{S'}$ to this point one obtains from Proposition 5(6)

$$\deg r_1 X_S f \sigma_{S'}(\partial' f') \sigma_{S'}(y) \leq 6^{L(c_*,\Gamma)}$$

since the generator $X_0 - r_1 \in A'_{S'}$ of its kernel can be presented by a linear polynomial which is regular with respect to $X'_{S'} f'(\partial' f') y$. Using linear operations and a projection (Proposition 5(5)) Eqs. (5.2) imply

$$\deg X_S f \partial f \leq \deg r_1 X_S f \sigma_{S'}(\partial' f') \sigma_{S'}(y),$$

hence the asserted (5.1).

(2) Parallel to the above proof arrangement we show by induction on t that if (Γ, X_S) computes $f \in A_S$ then $\deg X_S f \partial_E f \leq 2^{L(c_+,*,\Gamma)}$, however now under the additional assumption that $\mathrm{Res}(\Gamma, X_S) \in (A_S^{\times})^{n+t}$ since logarithmic derivatives will come in. Keeping the above notations the chain rule gives in the inductive step

$$X_i \partial_i f = \sigma_{S'}(X_i \partial_i f') + \sigma_{S'}(X_0 \partial_0 f') \cdot \frac{X_i \cdot \partial_i r_1}{r_1} \qquad \text{for } i \geq 1.$$

If $r_1 = X_1 \cdot X_2$ or $r_1 = X_1/X_2$ then $(X_i \cdot \partial_i r_1)/r_1 \in \{-1, 0, 1\}$, and then linear operations and only one quadratic operation to produce r_1 are required to complete the inductive argument. If $r_1 = X_1 \pm X_2$ then

$$\frac{X_1 \cdot \partial_1 r_1}{r_1} = 1 - \frac{X_2 \cdot \partial_2 r_1}{r_1},$$

so only one quadratic operation as in Lemma 31(1) and linear ones are required to complete the induction. Constant and scalar multiplication operations do not require non-linear operations. □

When part of a computation is known explicitly one can use degrees of certain vector operations rather than a step by step analysis to obtain better degree bounds. The following lemma exemplifies this in some concrete cases.

Lemma 31. *Let R be a field.*

(1) (*Segre*) *The vector operation* $(T_1, T_1T_3/T_2, \ldots, T_1T_a/T_2) \in (\hat{\Omega}^R)^{a-1}$ *of arity* $a \geq 2$ *has degree* $a - 1$.

(2) (*Veronese*) *The vector operation* $(T_1^{i_1} \cdots T_a^{i_a} : 0 \leq \sum i_j \leq r) \in (\hat{\Omega}^R)^{\binom{a+r}{a}}$ *of arity* a *has degree* $r^a (r \geq 1)$.

(3) *The matrix vector multiplication operation* $(T_{ij})(T'_j) \in (\hat{\Omega}^R)^a$ *of arity* $a \cdot b + b$ *has degree* 2^a.

(4) *The operation of solving a quadratic linear system* $(T_{ij})^{-1}(T'_j) \in (\hat{\Omega}^R)^a$ (*Cramer's formula*) *of arity* $a^2 + a$ *has degree* 2^a.

Proof. The first statement follows from Example 4(2) (using $n = 2$, $m = a - 1$); for the second one see [17, p. 54, Ex. 7.1]. For the remaining ones one can use Proposition 5(7); the details are left to the reader. □

Theorem 32. *Let R be a field of characteristic zero, $\mathfrak{p} \subset R[X]$ a prime principal ideal and $u \in R[X]_{\mathfrak{p}}$ an uniformizing parameter. Then*

(1) $I(c_*, X_{\mathfrak{p}}, \mathfrak{p}) \geq (1/\log_2 6)(\log_2 \deg(X_{\mathfrak{p}} \partial u)(\mathfrak{p}) - \log_2 \deg X_{\mathfrak{p}} u - \log_2(n+1))$,

(2) $I(c_{+,*}, X_{\mathfrak{p}}, \mathfrak{p}) \geq \log_2 \deg(X_{\mathfrak{p}} \partial_E u)(\mathfrak{p}) - \log_2 \deg X_{\mathfrak{p}} u - \log_2(n+1)$.

Proof. (1) Let $h = e \cdot u^{\mu}$ be any parameter of the discrete valuation ring $R[X]_{\mathfrak{p}}$, $e \in R[X]_{\mathfrak{p}}^{\times}$ and $\mu \geq 1$, such that $L(c_*, X_{\mathfrak{p}}, h) = I(c_*, X_{\mathfrak{p}}, \mathfrak{p})$. Denote this number by l. Lemma 8 and Proposition 30(1) imply $\deg(X_{\mathfrak{p}} u h \partial h)(0) \leq \deg(X_{\mathfrak{p}} u)(0) \cdot 6^l$, thereby viewing $h\partial h$ as a vector operation of arity n and degree at most 6^l. Observe that the elements of $k(0) = R(X)$

$$u \cdot \frac{\partial_i h}{h} = \mu \cdot \partial_i u + u \cdot \frac{\partial_i e}{e}$$

lie in $R[X]_{\mathfrak{p}}$, and their residues in $k(\mathfrak{p})$ coincide with those of $\partial_i u$ up to the constant factor μ. By Lemma 31(1) one obtains for $f = (u\partial_1 h/h, \ldots, u\partial_n h/h) \in \mathbb{A}^n_{R \to R[X]_{\mathfrak{p}}}$ after a projection

$$\deg X_{\mathfrak{p}} u f = \deg(X_{\mathfrak{p}} u f)(0) \leq \deg(X_{\mathfrak{p}} u)(0) \cdot 6^l \cdot (n+1).$$

Obviously, the generator u of the maximal ideal of $R[X]_{\mathfrak{p}}$ can be presented by a linear polynomial which is regular with respect to $X_{\mathfrak{p}} u f$; so by Proposition 5(6)

$$\deg(X_{\mathfrak{p}} \partial u)(\mathfrak{p}) = \deg(X_{\mathfrak{p}} u f)(\mathfrak{p}) \leq \deg X_{\mathfrak{p}} u f \leq \deg(X_{\mathfrak{p}} u)(0) \cdot 6^l \cdot (n+1).$$

(2) Analogously, using 30(2). □

Remark 33. 1. If $u \in R[X]$ is an irreducible polynomial generating $\mathfrak{p}$ then the bounds in Theorem 32 remain valid for positive field characteristic $> (\deg u)^n$. This follows easily by applying in the above proof Strassen's degree bound Theorem 9 directly to $h = eu^{\mu}$ if the field characteristic divides μ.

(2) It remains an open question whether a similar Jacobian lower-bound criterion holds true for $I(c, X_{\mathfrak{p}}, \mathfrak{p})$ (or for $I(c, X_{\mathfrak{p}}, \alpha)$) if $\operatorname{ht} \mathfrak{p} > 1$.

Examining the proof of Theorem 32 one sees that the tools used are degree, derivations, and the discrete valuation ring property of $R[X]_{\mathfrak{p}}$. By Lemma 16(3) the bounds in Theorem 32 apply in the same way to isolation complexity of prime cones $\alpha \in \operatorname{Spec}_r R[X]$ with support $\mathfrak{p}$ of dimension $n - 1$. If $\dim \alpha < n - 1$ then one can shrink its halo of generizations by choosing a real prime ideal $\mathfrak{q} \subset \mathfrak{p}$ such that $(R[X]/\mathfrak{q})_{\mathfrak{p}}$ is a real discrete valuation ring. Then $I(c_*, X_{\mathfrak{p}}, \alpha) \geq I(c_*, (X/\mathfrak{q})_{\mathfrak{p}}, \mathfrak{p})$, by Propositions 19(3), 15(1) and Lemma 16(3). The next result translates the approach of Theorem 32 to the situation when $\mathfrak{q} \neq 0$.

In the sequel when $y \in \mathbb{A}^m_{R\to A}$ and $d = (d_1,\dots,d_s) \in \mathrm{Der}_R(A, A^s)$ then $d(y)$ denotes the point $(d_i y_j) \in \mathbb{A}^{sm}_{R\to A}$.

Theorem 34. *Let R be a field of characteristic zero, $\mathfrak{q} \subset \mathfrak{p} \subset R[X]$ prime ideals, such that $A = (R[X]/\mathfrak{q})_{\mathfrak{p}}$ is a discrete valuation ring. Let $x = (X/\mathfrak{q})_{\mathfrak{p}}$, u an uniformizing parameter of A, and let $d_1,\dots,d_s \in \mathrm{Der}_R A$. Then the following hold.*

(1) $I(c_*, x, \mathfrak{p}) \geq (\log_2 \deg(xd(xu))(\mathfrak{p}) - \log_2 \deg xd(x)u - 2s)/\log_2 6$.

(2) *Let $x_1,\dots,x_s$ be a transcendence basis of $k(\mathfrak{q})$ over R, and assume $d_i x_j = \delta_{ij}$ for $1 \leq i,j \leq s$. If u is the image of a polynomial $U \in R[X]$ and if $F_1,\dots,F_{n-s} \in R[X]$ are polynomials of degree $\leq r$ generating the maximal ideal in $R[X]_{\mathfrak{q}}$, then*

$$I(c_*, x, \mathfrak{p}) \geq (\log_2 \deg(xd(u))(\mathfrak{p}) - \log_2 \deg U - (1 + 2\log_2 r)n)/\log_2 6.$$

Proof. Let $h = e \cdot u^\mu \in A$ be any parameter, $e \in A^\times$ and $\mu \geq 1$, such that $L(c_*, x, h) = I(c_*, x, \mathfrak{p})$. Denote this number by l. Let $\phi : R[X]_{\mathfrak{p}} \to A$ denote the canonical morphism, and choose $H \in R[X]_{\mathfrak{p}}$ with $L(c_*, X_{\mathfrak{p}}, H) = l$ lying above h. Again $H\partial H$ can be viewed as a vector operation of degree at most 6^l, and one has

$$d_i h = \sum_{j=1}^{n} \phi(\partial_j H) \cdot d_i x_j \quad \text{for } i = 1,\dots,s. \tag{5.3}$$

(1) By Lemmas 8, 31(3) and a projection these equations imply

$$\deg xd(x)uhd(h) \leq \deg xd(x)u \cdot 6^l \cdot 2^s.$$

Since the elements of $k(\mathfrak{q})$

$$u \cdot \frac{d_i h}{h} = \mu \cdot d_i u + u \cdot \frac{d_i e}{e}$$

lie in A one can argue as in the proof of Theorem 32 to conclude

$$\deg(xd(x)d(u))(\mathfrak{p}) \leq \deg xd(x)u \cdot 6^l \cdot 2^s \cdot (s+1);$$

hence the first assertion.

(2) In addition to Eqs. (5.3)

$$0 = \sum_{k=1}^{n} \phi(\partial_k F_j) \cdot d_i x_j \quad \text{for } i = 1,\dots,s,\ j = 1,\dots,n-s.$$

By 32(1) we may assume that $r \geq 2$ (since linear operations are not counted). Let $a = (\partial_1 H,\dots,\partial_s H)(\mathfrak{q})$, $b = (\partial_{s+1} H,\dots,\partial_n H)(\mathfrak{q})$, and partition the Jacobian $(\partial F)(\mathfrak{q})$ accordingly as

$$(\partial F)(\mathfrak{q}) = (J_1, J_2) \in k(\mathfrak{q})^{(n-s)\times s} \times k(\mathfrak{q})^{(n-s)\times(n-s)}$$

By the assumptions J_2 is non-singular, and using Eqs. (5.3) one can write in $k(\mathfrak{q})$

$$d(h)(\mathfrak{q}) = a - b(J_2^{-1})J_1.$$

Lemmas 8 and 31(2)–(4) linear operations and projections now give

$$\deg xhd(h)u = \deg(xhd(h)u)(\mathfrak{q}) \leq \deg x(\mathfrak{q}) \cdot 6^l(r-1)^n \cdot 2^{n-s} \cdot 2^s \cdot \deg U.$$

Since $\deg x(\mathfrak{q}) \leq r^{n-s}$, by Proposition 5(6), it follows as above

$$\deg(xd(u))(\mathfrak{p}) \leq 6^l \cdot r^{2n-s} \cdot 2^n \cdot \deg U \cdot (s+1);$$

whence the second assertion. □

6. Applications

This and the next section are devoted to applications of the previous results thereby getting meaningful lower bounds on test complexity in concrete cases. These complement the results on decision complexity based on topological arguments mentioned in the introduction and extend also lower bounds on *computing* a power sum, an elementary symmetric polynomial by Baur and Strassen [2] and a Lagrange interpolation polynomial given by Stoß [44] (see next section).

The subsequent lemma serves for bounding below the degrees of the main terms in Theorem 32 in concrete applications. We recall the classical fact that if $f_1,\ldots,f_n \in R[X_1,\ldots,X_n]$ are homogeneous polynomials (weight $(1,\ldots,1)$) that form a regular sequence then the extensions

$$R[f_1,\ldots,f_i] \hookrightarrow R[X]/(f_{i+1},\ldots,f_n)$$

are free of the same rank $\prod_{j=1}^{n} \deg f_j$ for all $i = 0,\ldots,n$. A sequence of arbitrary polynomials $f_1,\ldots,f_r$ is said to be a *top-regular sequence* if their highest homogeneous parts form a regular sequence.

Lemma 35. *Let R be a field, $\mathfrak{p} \subset R[X]$ be a prime principal ideal generated by the irreducible polynomial $u \in R[X]$ of degree $q \geq 2$. If the top homogeneous parts of the $\partial_i u$ generate an ideal of height m in $R[X]$, then* $\deg(X\partial u)(\mathfrak{p}) \geq q(q-1)^{m-1}$.

Proof. Without loss of generality, R may be assumed to be infinite (using a purely transcendental extension of the base field R; see Proposition 10(1)). By Kronecker's trick u and further $m-1$ R-linear combinations of the $\partial_i u$ form a top-regular sequence which may be assumed to be $u, \partial_1 u,\ldots,\partial_{m-1}u$ by a respective linear change of coordinates. Let $\ell_1,\ldots,\ell_{n-m}$ be linear forms such that $u, \partial_1 u,\ldots,\partial_{m-1}u, \ell_1,\ldots,\ell_{n-m}$ is a maximal top-regular sequence. Homogenizing these polynomials the above-mentioned fact says that

$$R[X_0, {}^h(\partial_1 u),\ldots,{}^h(\partial_{m-1}u), \ell_1,\ldots,\ell_{n-m}] \hookrightarrow R[X_0,\ldots,X_n]/({}^h u)$$

is free of rank $q(q-1)^{m-1}$. Reduction modulo $X_0 - 1$ shows that

$$R[\partial_1 u,\ldots,\partial_{m-1}u, \ell] \hookrightarrow R[X]/(u)$$

is also free of the same rank. It follows by localizing with respect to the multiplicative system of all non-zero elements in $R[\partial_1 u, \ldots, \partial_{m-1} u, \ell]$ that the field extension $K = R(\partial_1 u, \ldots, \partial_{m-1} u, \ell) \subset k(\mathfrak{p})$ is finite of the same rank. So by Propositions 5(2) and 10(3) and (4),

$$\deg(X\partial u)(\mathfrak{p}) = \deg(X\ell\partial u)(\mathfrak{p}) \geq \deg X(\mathfrak{p})_K = q(q-1)^{m-1},$$

hence the statement. □

Remark 36. We note the following convenient irreducibility criterion. If $u \in R[X]$ is any polynomial with $m \geq 3$ (m as in the above lemma), then u is irreducible (cf. [23, p. 175]). Furthermore if R is real closed and u is homogeneous and irreducible then $(u-a)R[X]$ is a real prime ideal for all positive or for all negative $a \in R$ ([8, 4.5.1, 9.5.2]); if u is of odd degree then $(u-a)R[X]$ is real for all non-zero a.

In the sequel R denotes a real closed field.

Corollary 37. *Let* $u = \sum_{i=1}^{n} X_i^q - 1 \in R[X]$, *and* $n, q \geq 2$. *If* $\mathscr{E} = \{E, E'\}$ *denotes the partition of* R^n *into the zeroes and non-zeroes of* u, *then*

$$C(c_*, \mathscr{E}) \geq ((n-1)\log_2(q-1) - \log_2(n+1))/\log_2 6,$$

$$C(c_{+,*}, \mathscr{E}) \geq (n-1)\log_2 q - \log_2 2(n+1).$$

The same bounds hold as well for $\mathscr{E}_1 = \{\{u \leq 0\}, \{u > 0\}\}$ *and for* $\mathscr{E}_2 = \{\{u < 0\}, \{u > 0\}\}$.

Proof. A decision tree $\mathscr{T}$ for $\mathscr{E}$ also decides the partition $\tilde{\mathscr{E}}$ by Theorem 24. If $\alpha \in \tilde{E}$ is any prime cone with support $uR[X]$ then the both proper generizations β, β' with support 0 (cf. [8, 10.2.6]) lie in $\tilde{E}'$. So by Proposition 23(1), Lemma 16(3) and Theorem 32(1),

$$L(c_*, \mathscr{T}_\alpha) \geq L(c_*, \mathscr{T}_{\alpha,\beta}) \geq (\log_2 \deg(X\partial u)(\mathfrak{p}) - \log_2 q - \log_2(n+1))/\log_2 6$$

as $\deg Xu = q$ (Remark 7). Since the $\partial_i u = qX_i^{q-1}$ form a maximal regular sequence of homogeneous polynomials, Lemma 35 yields

$$\deg(X\partial u)(\mathfrak{p}) \geq q(q-1)^{n-1},$$

whence the first assertion. The second one, which matches almost perfectly the obvious upper bound and is still meaningful for $q = 2$, follows analogously using Theorem 32(2).

$\mathscr{E}_1$ and $\mathscr{E}_2$ are left to the reader. □

Remark 38. For all three partitions $\mathscr{E}$, $\mathscr{E}_1$, and $\mathscr{E}_2$ the zero-set of u contains a non-void Zariski open subset of points producing a long path by Proposition 25; for $\mathscr{E}_2$ this set is outside of $\bigcup \mathscr{E}_2$.

Remark 39. Let $q \gg 0$ be even, and consider the decision problem $\mathscr{E} = \{\{\sum X_i^q - a = 0\}, \{\sum X_i^q - b = 0\}\}$ where $0 < a < b \in R$. If $b-a$ is sufficiently large then for some $c > 0$ the hypersurface $\{\sum X_i^2 - c = 0\}$ lies between the two ones, and $C(c_*, \mathscr{E}) \leq n$ by testing the sign of $\sum X_i^2 - c$. If $\leq$-branching is *not* allowed then by Proposition 26(4) and Corollary 37 the decision complexity is still of order $n \log_2 q$. This exemplifies in concrete terms the dependency of decision complexity on the relations allowed.

Corollary 40. *Let $\sigma_q \in R[X]$ denote the qth elementary symmetric polynomial, $2 \leq q \leq n/2$, and let $\mathscr{E}$ be the partition of R^n into the zeroes and non-zeroes of $\sigma_q - 1$. Then*

$$C(c_*, \mathscr{E}) \geq ((n-q)\log_2(q-1) - \log_2(n+1))/\log_2 6.$$

Proof. From the partial derivatives with respect to X_j of

$$\prod_{i=1}^{n}(T + X_i) = \sum_{q=0}^{n} \sigma_q T^{n-q} \in R[X][T]$$

($\sigma_0 = 1$) one gets the identity

$$\prod_{i=1}^{n}(T + X_i) = (T + X_j)\partial_j \prod_{i=1}^{n}(T + X_i) = \sum_{q=0}^{n}(\partial_j \sigma_q)T^{n-q+1} + \sum_{q=0}^{n} X_j(\partial_j \sigma_q)T^{n-q};$$

hence by comparing coefficients,

$$\partial_j \sigma_{q+1} + X_j \partial_j \sigma_q = \sigma_q \quad \text{for } j = 1, \ldots, n.$$

By the Euler identity, σ_q lies in the ideal $(\partial_1 \sigma_q, \ldots, \partial_n \sigma_q)R[X]$, and by induction this ideal contains the regular sequence $\sigma_q, \ldots, \sigma_n$. Hence its height is at least $n-q$. Using Lemma 35 the stated lower bound follows analogously as above. □

Remark 41. For testing the resultant, discriminant, a subresultant, etc., for zero Theorem 32 does imply good bounds since the degrees are small.

Next we want to exemplify the bound in Proposition 23(2). We will use the following.

Lemma 42. *Let $\mathfrak{p} \subset R[X]$, $\mathfrak{q} \subset R[Y]$ be real prime ideals. Then their join $J(\mathfrak{p}, \mathfrak{q}) \subset R[X] \otimes_R R[Y]$ is real and prime. If $\mathfrak{p}' \subseteq \mathfrak{p}$, $\mathfrak{q}' \subseteq \mathfrak{q}$ are also real and prime, then*

$$E(c_*, (X/\mathfrak{p}' \bowtie Y/\mathfrak{q}')_{J(\mathfrak{p},\mathfrak{q})}, J(\mathfrak{p}, \mathfrak{q})) = \min\{E(c_*, (X/\mathfrak{p}')_{\mathfrak{p}}, \mathfrak{p}), E(c_*, (Y/\mathfrak{q}')_{\mathfrak{q}}, \mathfrak{q})\}.$$

Proof. The fact that $J(\mathfrak{p}, \mathfrak{q}) = \mathfrak{p} \otimes_R R[Y] + R[X] \otimes_R \mathfrak{q}$ is real and prime follows from a standard application of the Artin–Lang Theorem [8, 4.1.2].

Applying Lemma 16(1) to the triplet $J(\mathfrak{p}, \mathfrak{q}) \supseteq J(\mathfrak{p}', \mathfrak{q}) \supseteq J(\mathfrak{p}', \mathfrak{q}')$ yields either

$$E(c_*, (X/\mathfrak{p}' \bowtie Y/\mathfrak{q}')_{J(\mathfrak{p},\mathfrak{q})}, J(\mathfrak{p}, \mathfrak{q})) = E(c_*, (X/\mathfrak{p}' \bowtie Y/\mathfrak{q})_{J(\mathfrak{p},\mathfrak{q})}, J(\mathfrak{p}, \mathfrak{q}))$$

or

$$E(c_*,(X/\mathfrak{p}' \bowtie Y/\mathfrak{q}')_{J(\mathfrak{p},\mathfrak{q})},J(\mathfrak{p},\mathfrak{q})) = E(c_*,(X/\mathfrak{p}' \bowtie Y/\mathfrak{q}')_{J(\mathfrak{p}',\mathfrak{q})},J(\mathfrak{p}',\mathfrak{q})).$$

Assuming by symmetry the first equality (say) the local monomorphism of R-algebras $(R[X]/\mathfrak{p}')_{\mathfrak{p}} \hookrightarrow (R[X]/\mathfrak{p}' \otimes_R R[Y]/\mathfrak{q})_{J(\mathfrak{p},\mathfrak{q})}$ yields

$$E(c_*,(X/\mathfrak{p}' \bowtie Y/\mathfrak{q})_{J(\mathfrak{p},\mathfrak{q})},J(\mathfrak{p},\mathfrak{q})) \leq E(c_*,(X/\mathfrak{p}')_{\mathfrak{p}},\mathfrak{p})$$

which is easily seen to be an equality by using a suitable Artin–Lang substitution

$$((R[X]/\mathfrak{p}')_{\mathfrak{p}} \otimes_R R[Y]/\mathfrak{q})_d \to (R[X]/\mathfrak{p}')_{\mathfrak{p}} \otimes_R R;$$

here, starting out from the universal input of a respective SLP, the denominator $d \in R[X] \otimes_R R[Y]$ has to be chosen to establish the transfer of a certain non-zero relation into a non-zero relation. □

Using, for instance, Corollary 37 the statement of the following can be made concrete.

Corollary 43. *Assume $u \in R[X]$ to generate a real prime ideal $\mathfrak{p} \subset R[X]$, and let $\mathfrak{q} \subset R[Y]$ be generated by $u' = u(Y)$. Then for the partition $\mathscr{E} = \{\{u > 0, u' = 0\}, \{u' > 0, u = 0\}\}$ in R^{2n}*

$$C(c_*,\mathscr{E}) \geq I(c_*,X_{\mathfrak{p}},\mathfrak{p}).$$

Proof. Let $E = \{\{u > 0, u' = 0\}, E' = \{u' > 0, u = 0\}\}$. Choose $\beta \in \mathrm{Spec}_{\mathrm{r}} R[X] \otimes_R R[Y]$ with support $J(\mathfrak{p},\mathfrak{q})$ and generizations $\alpha \in \tilde{E}$, $\alpha' \in \tilde{E}'$ with supports $J(0,\mathfrak{q})$ and $J(\mathfrak{p},0)$. By Proposition 23(2) the minimum of the two numbers $E(c_*,(X \bowtie Y/\mathfrak{q})_{J(\mathfrak{p},\mathfrak{q})}, J(\mathfrak{p},\mathfrak{q}))$ and $E(c_*,(X/\mathfrak{p} \bowtie Y)_{J(\mathfrak{p},\mathfrak{q})},J(\mathfrak{p},\mathfrak{q}))$ provides a lower bound on the decision complexity $C(c_*,\mathscr{E})$. By Lemma 42 both coincide with $E(c_*,X_{\mathfrak{p}},\mathfrak{p}) = I(c_*,X_{\mathfrak{p}},\mathfrak{p})$, whence the assertion. □

Remark 44. By Proposition 25(1) the zero-set of u and u' contains a Zariski open subset of points producing a long path. This set is outside $\bigcup \mathscr{E}$.

Finally, we exemplify the bound in Proposition 23(3) in a case of an algebraic set of codimension > 1.

Corollary 45. *Let $E \subset R^{n\times n} \times R^{n\times n}$ be the set of pairs of invertible matrices (a,b) such that $b = a^{-1}$ and $\sum a_{ij}^q = 1$, $q \gg 1$. Denote by $\mathscr{E} = \{E,E'\}$ the partition of $R^{n\times n} \times R^{n\times n}$ into E and its complement E'. Then*

$$C(c_*,\mathscr{E}) \geq \textit{const.}\ n^2 \log_2 q.$$

Proof. Let $A = R[X_{1\,1},\ldots,X_{n\,2n}]$, $\mathfrak{q} \subset A$ be the vanishing ideal of the graph of matrix inversion, $\mathfrak{p} \supset \mathfrak{q}$ the vanishing ideal of E. Then $(A/\mathfrak{q})_{\mathfrak{p}}$ is a real discrete valuation ring.

If $\alpha \in \tilde{E}$ has support $\mathfrak{p}$ then its two generizations in $\mathscr{Z}(\mathfrak{q})$ belong to $\tilde{E}'$. By Proposition 23(3) (or (1)) and Lemma 16(3), $I(c_*, (X/\mathfrak{q})_{\mathfrak{p}}, \mathfrak{p})$ is a lower bound on the decision complexity. Obviously, the images of $X_{11}, \ldots, X_{nn}$ in $k(\mathfrak{q})$ form a transcendence basis of $k(\mathfrak{q}) \simeq R(X_{11}, \ldots, X_{nn})$ over R, and also obviously $A_{\mathfrak{q}}$ has a regular system of parameters given by quadratic polynomials. Using Theorem 34(2) it follows in an analogous manner as above that

$$I(c_*, (X/\mathfrak{q})_{\mathfrak{p}}, \mathfrak{p}) \geq ((n^2 - 1)\log_2(q-1) - 3n^2)/\log_2 6,$$

whence the statement. □

Remark 46. (1) In this example we have shrunk the halo of α since the vanishing ideal $\mathfrak{q} \subset A$ is obviously generated by "cheap" (quadratic) polynomials, and therefore $E(c_*, X_{\mathfrak{p}}, \mathfrak{p}) \leq n$ is small.

(2) The proof shows that having also the inverse of an invertible matrix a is essentially of no help for testing whether $\sum a_{ij}^q = 1$.

Next we consider zeroes and non-zeroes of an "easier" and a more "difficult" polynomial.

Corollary 47. *Let* $e = X_{n-1} - \sum_{i=1}^{n-2} X_i^n, d = X_n - \sum_{i=1}^{n-2} X_i^{n^2} \in R[X]$, *and consider the partitions in* R^n,

$$\mathscr{E}_0 = \{\{e = d = 0\}, \{e^2 + d^2 \neq 0\}\},$$

$$\mathscr{E}_1 = \{\{e = d = 0\}, \{e = 0, d \neq 0\}\},$$

$$\mathscr{E}_2 = \{\{e = d = 0\}, \{e \neq 0, d = 0\}\},$$

$$\mathscr{E}_3 = \{\{e = 0, d \neq 0\}, \{e \neq 0, d = 0\}\}.$$

Then each of these test problems has a complexity

$$C(c_*, \mathscr{E}_i) \geq \textit{const.}\ n\log_2 n.$$

Proof. Consider the prime ideals $0 \subset \mathfrak{p} \subset \mathfrak{q} \supset \mathfrak{p}' \supset 0$ in $R[X]$ where $\mathfrak{p} = eR[X]$, $\mathfrak{q} = (e,d)R[X]$, $\mathfrak{p}' = dR[X]$. From Lemma 16(1) we get two lines of inequalities which arrange themselves in a "cross"

$$\begin{array}{ccccc} E(c_*, (X/\mathfrak{p})_{\mathfrak{q}}, \mathfrak{q}) & \geq & E(c_*, X_{\mathfrak{q}}, \mathfrak{q}) & \leq & E(c_*, X_{\mathfrak{p}}, \mathfrak{p}) \\ & & \| & & \\ E(c_*, (X/\mathfrak{p}')_{\mathfrak{q}}, \mathfrak{q}) & \geq & E(c_*, X_{\mathfrak{q}}, \mathfrak{q}) & \leq & E(c_*, X_{\mathfrak{p}'}, \mathfrak{p}'). \end{array}$$

The aim is now to show a lower bound of order $n\log_2 n$ for the middle number. First of all, the right-hand numbers in each line have such a lower bound by Theorem 32(1), and if one of the right-hand inequalities is an equality the statement is clear. So

assume both right ones to be strict inequalities. Then by Lemma 16(1) *both* left-hand inequalities must in fact be equalities, and one can apply Theorem 34(1) to bound the top left number as

$$E(c_*, (X/\mathfrak{p})_\mathfrak{q}, \mathfrak{q}) \geq ((n-2)\log_2(n^2-1) - (n-2)\log_2(n-1) - 3\log_2 n \\ -2(n-2))/\log_2 6$$

using $R[X]/\mathfrak{p} \simeq R[X_1,\ldots,X_{n-2},X_n]$, the partials $\partial_1,\ldots,\partial_{n-2} \in \mathrm{Der}_R(R[X]/\mathfrak{p})_\mathfrak{q}$, and a degree analysis in an analogous fashion as above. (Note that direct application of Theorem 34(1) to the bottom left number does *not* lead to such a bound.) Now the bounds on the complexities of the $\mathscr{E}_i$ follow in the habitual way from Proposition 23(1) and (2). □

Remark 48. The problem $\mathscr{E}_3$ can be interpreted as the sign determination of the function $(d+e)/(d-e)$ under the knowledge that it is defined and its absolute value is one.

The subsequent lemma prepares for the applications in the next section. Testing whether a "rational expression" (whenever defined) takes a certain given value leads to prime principal ideals $\mathfrak{p}$ with rational residue class field, and the degrees in Theorem 32 can conveniently be bounded as follows.

Lemma 49. *Let R be a field and $\mathfrak{p} \in R[X_1,\ldots,X_n]$ be a prime principal ideal generated by the irreducible polynomial $aX_1 - b$ where $a,b \in R[X_2,\ldots,X_n]$ are both non-zero. Then, for $c = b/a \in R(X_2,\ldots,X_n)$, $u = X_1 - c \in R[X]_\mathfrak{p}$ is an uniformizing parameter, and*

$$\deg(X_\mathfrak{p}\partial u)(\mathfrak{p}) = \deg X'(0)c\partial' c \geq \deg X'(0)\partial' c,$$

where $X' = (X_2,\ldots,X_n) \in \mathbb{A}^{n-1}_{R\to R[X_2,\ldots,X_n]}$ and $\partial' c = (\partial_2 c,\ldots,\partial_n c) \in \mathbb{A}^{n-1}_{R\to R(X_2,\ldots,X_n)}$.

Proof. This follows immediately from the canonical isomorphism $k(\mathfrak{p}) \simeq R(X_2,\ldots,X_n)$ using a projection 5(5). □

7. Solvability test of overdetermined interpolation tasks

Let R be a real closed field, $[a,b] \subset R$ an interval, $a < b$. If $a \leq x_0 < \ldots < x_n \leq b$ are "nodes" between a and b and $y_0,\ldots,y_n \in R$ are given "values" then a standard computational task asks for computing an interpolating function I with $I(x_j) = y_j$ for $j = 0,\ldots,n$. In this section we will show for several common interpolation functions I that even the test whether the value $I(t)$ in a further point of $[a,b]$ coincides with a further given value $z \in R$ has already a considerable complexity. We first introduce these interpolation tasks:

Set $S = \{a \leq x_0 < \cdots < x_n \leq b\} \times [a,b] \subset R^{n+2}$.

Lagrange interpolation. The Lagrange interpolation polynomial

$$L = \sum_{k=0}^{n} Y_k l_k \in R[X_0, \ldots, X_n]_v[Y_0, \ldots, Y_n][T]$$

with the Lagrange polynomials

$$l_k = \prod_{j=0,\, j\neq k}^{n} \frac{T - X_j}{X_k - X_j} \in R[X]_v[T]$$

and the Vandermonde determinant $v = \prod_{i>k}(X_i - X_k)$ defines a partition $\mathscr{L}$ of $S \times R^{n+2}$ into the zeroes and non-zeroes of $Z - L \in R[X]_v[Y, T, Z]$.

Hermite interpolation. More generally, prescribing in the nodes values for the derivatives (with respect to the indeterminate T) up to certain orders $\nu_0 - 1, \ldots, \nu_n - 1 \geq 0$ leads to the Hermite interpolation polynomial (e.g. [40])

$$H = \sum_{k=0}^{n} \sum_{j=0}^{\nu_k - 1} Y_{k,j} h_{k,j} \in R[X]_v[Y][T],$$

where among the Hermite polynomials $h_{k,j} \in R[X]_v[T]$ the top ones have the following explicit form:

$$h_{k,\nu_k - 1} = \frac{(T - X_k)^{\nu_k - 1}}{(\nu_k - 1)!} \prod_{j=0,\, j\neq k}^{n} \left(\frac{T - X_j}{X_k - X_j}\right)^{\nu_j}$$

(cf. [40, p. 116]). Let $\mathscr{H}$ denote the partition of $S \times R^{m+1}$, $m = \sum_{k=0}^{n} \nu_k$, into the zeroes and non-zeroes of $Z - H \in R[X]_v[Y, T, Z]$.

Fractional interpolation. For $m \leq n$ the equations

$$X_j^{n-m} + \sum_{i=0}^{n-m-1} c_i X_j^i = Y_j \sum_{k=0}^{m} d_k X_j^k \quad \text{for } j = 0, \ldots, n \tag{7.1}$$

define uniquely $c_i, d_k \in R[X_0, \ldots, X_n, Y_0, \ldots, Y_n]_w$ where w is the determinant of the respective linear system. Consider the interpolation function (e.g. [35])

$$F = \frac{T^{n-m} + \sum_{i=0}^{n-m-1} c_i T^i}{\sum_{k=0}^{m} d_k T^k} \in (R[X, Y]_w[T])_d,$$

where $d = \sum_{k=0}^{m} d_k T^k$, and the open semi-algebraic subset $S' \subset S \times R^{n+1}$ where w does not vanish and moreover $d(t) \neq 0$ for all $t \in [a, b]$. Let $\mathscr{F}$ denote the partition of $S' \times R$ into the zeroes and non-zeroes of $Z - F \in (R[X, Y]_w[T])_d[Z]$.

Lagrange interpolation of higher degree polynomials. Substituting the elements $\sum_{j=0}^{2n+2} C_j X_k^j \in R[X_0, \ldots, X_n, C_0, \ldots, C_{2n+2}]$ for the Y_k in the Lagrange interpolation polynomial one obtains a Lagrange interpolation polynomial

$$L' \in R[X_0, \ldots, X_n, C_0, \ldots, C_{2n+2}][T]$$

which results as the remainder of the Euclidean division (with respect to the indeterminate T)

$$\sum_{j=0}^{2n+2} C_j T^j = q \cdot p + L', \tag{7.2}$$

where $p = \prod_{i=0}^{n}(T - X_i) = T^{n+1} + \sum_{j=1}^{n+1}(-1)^j \sigma_j T^{n+1-j}$, and q denotes the respective quotient. Let $\mathscr{L}'$ denote the partition of $S \times R^{2n+4}$ into the zeroes and non-zeroes of $Z - L' \in R[X, C, T, Z]$.

Theorem 50. *Each of the interpolation tests* $\mathscr{I} \in \{\mathscr{L}, \mathscr{H}, \mathscr{F}, \mathscr{L}'\}$ *has a complexity*

$$C(c_*, \mathscr{I}) \geq \text{const. } n \log_2 n.$$

To prove this theorem we will apply deformation processes transforming a given point into one whose degree is not bigger and easier to bound using the following lemma.

Lemma 51. *Let* $(A, \mathfrak{m})$ *be a discrete valuation ring with residue class field* $k(\mathfrak{m})$ *and quotient field* $k(0)$, $d \in \mathbb{A}^n_{A \to B}$ *be a non-zero point over* A. *If* $\mathfrak{m} = \varepsilon A$, *and the generator* ε *of* $\mathfrak{m}$ *is* B*-regular, then* $\dim d^{k(0)} \geq \dim d^{k(\mathfrak{m})}$, *if* $d^{k(\mathfrak{m})}$ *is non-zero. If equality of dimensions holds, then also* $\deg d^{k(0)} \geq \deg d^{k(\mathfrak{m})}$.

Proof. The relations in $\operatorname{ann} d \subset A[D_1, \ldots, D_n]$ of degree at most t form a finite and free module over the principal ideal domain A and march via coefficient reduction into the $k(\mathfrak{m})$-vector space of relations in $\operatorname{ann} d^{k(\mathfrak{m})} \subset k(\mathfrak{m})[D_1, \ldots, D_n]$ of degree at most t. Since ε is B-regular $A[D]^{(\leq t)} / \operatorname{ann} d \cap A[D]^{(\leq t)}$ is also free. It results therefore for the Hilbert functions

$$H(d^{k(0)}, t) \geq H(d^{k(\mathfrak{m})}, t)$$

implying the dimension inequality. If equality holds then a comparison of leading terms of Hilbert polynomials yields the inequality of degrees. □

In the applications below we will have $A = R[\varepsilon]_{(\varepsilon)}$ and $B = K[\varepsilon]_{(\varepsilon)}$ where K is an extension field of R and ε is an indeterminate over K. If $R(d^{k(\mathfrak{m})}) = K$ and $R(\varepsilon)(d^{k(0)}) = K(\varepsilon)$ then the equality of dimensions clearly holds by Proposition 5(1).

Proof of Theorem 50. We first treat the partition $\mathscr{H}$ of Hermite interpolation (including $\mathscr{L}$). By differentiation with respect to Y_{k,v_k-1} only and Lemma 49 it suffices to bound the degree of $(XT)(0)h \in \mathbb{A}^{n+2+n+1}_{R \to R(X,T)}$ where

$$h_k = (T - X_k)^{v_k - 1} \prod_{j=0,\, j \neq k}^{n} \left(\frac{T - X_j}{X_k - X_j} \right)^{v_j}.$$

The plan is to verify for the following points, having all the same dimension $n+2$, the inequalities

$$\deg(XT)(0)h \geq \deg(XT)(0)h' \geq \deg(XT)(0)h'' \geq \prod_{k=0}^{n-1}\left(\sum_{i=k+1}^{n} v_i\right) \geq n!, \tag{7.3}$$

where

$$h'_k = T^{m-1}\prod_{j=0,\, j\neq k}^{n}(X_k - X_j)^{-v_j},$$

$$h''_k = T^{m-1}\prod_{j=0}^{k-1}(-X_j)^{-v_j}\cdot X_k^{-\sum_{i=k+1}^{n} v_i}$$

Let $d, d' \in \mathbb{A}^{n+2+n+1}_{R[\varepsilon]_{(\varepsilon)}\to R(X,T)[\varepsilon]_{(\varepsilon)}}$ be the points

$$d = (X_0,\ldots,X_n,T,d_0,\ldots,d_n), \quad d' = (X_0,\ldots,X_n,T,d'_0,\ldots,d'_n),$$

where

$$d_k = (\varepsilon^{-1}T - X_k)^{v_k-1}\prod_{j=0,\, j\neq k}^{n}\left(\frac{\varepsilon^{-1}T - X_j}{X_k - X_j}\right)^{v_j}\cdot \varepsilon^{m-1},$$

$$d'_k = T^{m-1}\prod_{j=0,\, j\neq k}^{n}(\varepsilon^k X_k - \varepsilon^j X_j)^{-v_j}\cdot\prod_{i=0}^{k-1}\varepsilon^{iv_i}\cdot\prod_{i=k+1}^{n}\varepsilon^{kv_i}.$$

By Proposition 5(2) the image of d in $\mathbb{A}^{n+2+n+1}_{R(\varepsilon)\to R(\varepsilon,X,T)}$ and $(((XT)(0)h)^{R(\varepsilon)})(0)$ has the same dimension and the same degree which coincide with the dimensions and degrees of $((XT)(0)h)^{R(\varepsilon)})$ and of $(XT)(0)h$ by Propositions 5(3) and 10(1). This shows the first inequality in (7.3) by Lemma 51. The same argument applied to d' yields the second inequality. Finally, absorbing the coordinates $T, h''_0,\ldots,h''_{n-1},X_n$ of $(XT)(0)h''$ into the coefficient field implies also the third one by Lemma 52 below.

Lemma 52. *Let R be a field, $q_i \in R(X_1,\ldots,X_{i-1})\setminus\{0\}$, $v_i \in \mathbb{Z}\setminus\{0\}$ for $i = 1,\ldots,m$. Then the field extension*

$$R(q_1X_1^{v_1},\ldots,q_mX_m^{v_m}) \subseteq R(X_1,\ldots,X_m)$$

is finite of degree $|\prod_i v_i|$.

Proof. Without loss of generality all $v_i > 0$. Using induction on m the statement follows immediately considering the tower of finite extensions

$$R(q_1X_1^{v_1},\ldots,q_mX_m^{v_m}) \subseteq R(X_1,\ldots,X_{m-1},q_mX_m^{v_m}) \subseteq R(X_1,\ldots,X_m). \quad \square$$

We continue with proof of Theorem 50 for $\mathscr{F}$ and observe first that one may assume that $n > m \geq n-m$ by the following argument. If $F = b/a$ is a relatively prime quotient

representation of F with polynomials $a, b \in R[X, Y, T]$ and $\mathfrak{p} \subset R[X, Y, T, Z]$ is generated by $Za - b$ then $Z - F$ is an uniformizing parameter of $R[X, Y, T, Z]_{\mathfrak{p}}$ (e.g. Lemma 49) as well as $Z^{-1} - F^{-1}$. Changing the reference point $(XYTZ)_{\mathfrak{p}}$ according to replacing the Y_i and Z by their inverses if $m < n - m$ one may assume that $m \geq n - m$, by Remark 12. By the same argument and the already treated Lagrange interpolation one may furthermore assume that $m < n$.

We are now going to bound the degree of the point

$$(XYT)(0)\partial'_Y F \in \mathbb{A}^{2(n+1)+1+m+1}_{R \to R(X,Y,T)}$$

where $\partial'_Y = (\partial_{Y_0}, \ldots, \partial_{Y_m})$. Let $\mathfrak{q} \subset R[X, Y, T]$ denote the prime ideal generated by $Y_{m+1}, \ldots, Y_n$. Since the determinant w of the system (7.1) is not in $\mathfrak{q}$ one sees that all e_i, d_k and F as elements of $R(X, Y, T)$ lie already in $R[X, Y, T]_{\mathfrak{q}}$. If F' denotes the image of F in $k(\mathfrak{q}) \simeq R(X, Y', T)$, $Y' = (Y_0, \ldots, Y_m)$, then the degree of the point

$$(XY'T)(0)\partial'_Y F' \in \mathbb{A}^{n+1+m+1+1+m+1}_{R \to R(X,Y',T)}$$

provides a lower bound on the degree of the above point, and the partials $\partial_{Y_0} F'$ $, \ldots, \partial_{Y_m} F'$ are easy to determine. If $c'_i, d'_k \in R(X, Y', T)$ denote the images of the $c_i, d_k \in R[X, Y, T]_{\mathfrak{q}}$ then these are defined by the equations

$$Y_j^{-1}\left(X_j^{n-m} + \sum_{i=0}^{n-m-1} c'_i X_j^i\right) = \sum_{k=0}^{m} d'_k X_j^k \quad (j = 1, \ldots, m),$$

$$X_j^{n-m} + \sum_{i=0}^{n-m-1} c'_i X_j^i = 0 \quad (j = m+1, \ldots, n);$$

so $c'_i = (-1)^{n-m-i}\sigma_{n-m-i} \in R[X_{m+1}, \ldots, X_n]$,

$$T^{n-m} + \sum_{i=0}^{n-m-1} c'_i T^i = \prod_{r=m+1}^{n} (T - X_r),$$

$$\sum_{k=0}^{m} d'_k T^k = \sum_{j=0}^{m} \left(Y_j^{-1} \prod_{r=m+1}^{n} (X_j - X_r)\right) \cdot l_j,$$

where the $l_j \in R(X_0, \ldots, X_m)[T]$ are the Lagrange polynomials. It follows that

$$F' = \frac{\prod_{r=m+1}^{n}(T - X_r)}{\sum_{j=0}^{m}\left(Y_j^{-1}\prod_{r=m+1}^{n}(X_j - X_r)\right) \cdot l_j}$$

and

$$\partial_{Y_s} F' = \frac{\prod_{r=m+1}^{n}(T - X_r)}{\left(\sum_{j=0}^{m}\left(Y_j^{-1}\prod_{r=m+1}^{n}(X_j - X_r)\right) \cdot l_j\right)^2} \cdot \prod_{r=m+1}^{n} (X_s - X_r) \cdot l_s \cdot Y_s^{-2}$$

for $s = 0, \ldots, m$.

Let $\mathfrak{Q} \subset R[X_0,\ldots,X_n,Y_0,\ldots,Y_m,T]$ denote the prime ideal generated by $X_{m+1},\ldots,X_n$, $Y_0-1,\ldots,Y_m-1$. Then the elements $\partial_{Y_s}F'$ lie in the localization $R[X,Y',T]_{\mathfrak{Q}}$, and their residues in $k(\mathfrak{Q})=R(X_0,\ldots,X_m,T)$ are $l'_s=T^{m-n}X_s^{n-m}l_s$. Therefore,

$$\deg(XY'T)(0)\partial'_Y F' \geq \deg(X'T)(0)l',$$

where $X'=(X_0,\ldots,X_m)\in \mathbb{A}^{m+1}_{R\to R[X_0,\ldots,X_m,T]}$. It follows by applying an analogous deformation procedure as in the above proof that

$$\deg(X'T)(0)l' \geq \deg(X'T)(0)l'',$$

where

$$l''_s = T^{2m-n-1}\prod_{i=0}^{s-1}(-X_i)\cdot X_s^{s+n-2m} \quad \text{for } s=0,\ldots,m.$$

Absorbing now the coordinates $T,l''_0,\ldots,l''_{2m-n-1},X_{2m-n},l''_{2m-n+1},\ldots,l''_{m-1},X_m$ of the point $(X'T)\,(0)l''$ into the coefficient field, Lemma 52 implies

$$\deg(X'T)(0)l'' \geq (2m-n)!(n-m-1)!.$$

Since $(2m-n)+(n-m-1)=m-1$ the right-hand product is at least $(\lfloor (m-1)/2\rfloor !)^2$, implying the assertion by $m\geq n/2$.

The next lemma prepares for proving Theorem 50 for the partion $\mathscr{L}'$.

Lemma 53. *Let $R\subseteq K$ be a field extension, and assume $ab\in 1+T^{m+1}K[T]$ for $a=\sum_{i=0}^m a_iT^i, b=\sum_{i=0}^m b_iT^i\in K[T]$. If $q\in K[C_0,\ldots,C_m][T]$ is the remainder of the product $(\sum_{i=0}^m C_iT^i)\cdot a$ modulo $T^{m+1}K[C_0,\ldots,C_m][T]$, then*

$$\partial_{C_i}q = T^i\cdot\sum_{j=0}^{m-i}a_jT^j \quad \textit{for } i=0,\ldots,m,$$

and $R(T,\partial_{C_0}q,\ldots,\partial_{C_m}q)=R(T,a_0,\ldots,a_m)=R(T,b_0,\ldots,b_m)$. As a consequence, if $a_0\in R$ then $R(T,(\partial_{C_0}q)\cdot p,\ldots,(\partial_{C_m}q)\cdot p)=R(T,b_0,\ldots,b_m,p)$ for every non-zero $p\in K$.

Proof. Clearly $R[\underline{b}\,]\subseteq R[\underline{a}\,][a_0^{-1}]$, so $R(\underline{b})\subseteq R(\underline{a})$ with equality by symmetry. If $a_0\in R^\times$, then $p=a_0^{-1}\cdot T^{-m}\cdot(\partial_{C_m}q)\cdot p$, implying the consequence. □

Analogously as above the lower bound on the partition $\mathscr{L}'$ in Theorem 50 is obtained by showing that

$$\deg XCT\partial_C L' \geq (n+1)!.$$

Eq. (7.2) implies that

$$\partial_{C_j}L' = T^j-(\partial_{C_j}q)p$$

since $p \in R[X,T]$. As the coefficients with respect to T of p are up to sign the elementary symmetric polynomials $\sigma_j \in R[X_0,\ldots,X_n]$ and $\deg_T L' = n$, Lemma 53 shows that

$$R(T,\partial_{C_{2n+1}}L',\ldots,\partial_{C_{n+1}}L') = R(T,\sigma_1,\ldots,\sigma_{n+1})$$

(multiply Eq. (7.2) with T^{-2n-2} and consider the parameter T^{-1} to use the lemma). So by absorbing respective coordinates into the coefficient field it follows that

$$\deg XCT\partial_C L' \geq [R(X,C,T) : R(\sigma,C,T)] \geq (n+1)!$$

since the elementary symmetric polynomials form a regular sequence. This completes the proof of Theorem 50. □

Lagrange interpolation of a higher degree product of polynomials. If one interpolates a higher degree product of polynomials an analogous bound holds as well. Let $n_1,\ldots,n_t \in \mathbb{N}$ be numbers of sum $2n+2$, and define $c_i \in R[D_{1\,0},\ldots,D_{t\,n_t}]$ by

$$\sum_{k=0}^{2n+2} c_k T^k = \prod_{i=1}^{t}\left(\sum_{j=0}^{n_i} D_{i\,j}T^j\right).$$

Substituting the elements c_i for the C_i in L' one obtains a Lagrange interpolation polynomial

$$L'' \in R[X_0,\ldots,X_n,D_{1\,0},\ldots,D_{t\,n_t}][T].$$

Let $\mathscr{L}''$ denote the corresponding partition of $S\times R^{2n+3+t}$ into the zeroes and non-zeroes of $Z - L'' \in R[X,D,T,Z]$.

Corollary 54. *The interpolation test $\mathscr{L}''$ has a complexity*

$$C(c_*,\mathscr{L}'') \geq \textit{const.}\ n\log_2 n.$$

Proof. We show $\deg XDT\partial_D L'' \geq (n+1)!$. First observe that by the chain rule the $\partial_{D_{i\,j}}L''$ are $R[D]$-linear combinations of the $\partial_{C_k}L' \in R[X_0,\ldots,X_n,T]$; and since the $c_i \in R[D]$ are algebraically independent over R, the Jacobian $(\partial_D c)$ has maximal rank $2n+3$. Therefore,

$$\deg XDT\partial_D L'' \geq \deg(XDT\partial_D L'')_{R(D,T)} = \deg(XDT\partial_C L')_{R(D,T)} \geq (n+1)!$$

as above. □

Chinese remaindering. Finally, we mention a consequence for Chinese remaindering. Let $n_1,\ldots,n_t \in \mathbb{N}_+$ be positive numbers of sum $n+1$, $m_i = T^{n_i} + \sum_{j=0}^{n_i-1} X_{i\,j}T^j \in R[X][T]$, $r_i = \sum_{j=0}^{n_i-1} Y_{i\,j}T^j \in R[Y][T]$, and consider the polynomial $C \in R[X]_p[Y][T]$ of degree n with respect to T defined by Chinese remaindering, that is $C \equiv r_i \bmod$

$m_i R[X]_p[Y][T]$; here p is the product of the respective resultants of pairs of the m_i. Let $\mathscr{C}$ denote the partition of R_p^{2n+4} into the zeroes and non-zeroes of $Z-C \in R[X]_p[Y,T,Z]$.

If the entropy of the probability vector $(n_1/n,\ldots,n_t/n)$ is large the following bound is meaningful.

Corollary 55. *The Chinese remaindering test $\mathscr{C}$ has a complexity*

$$C(c_*,\mathscr{C}) \geq \frac{1}{11} n \log_2 n - 11 \sum_{i=1}^{t} n_i \log_2 n_i.$$

Proof. A decision tree for $\mathscr{C}$ can be used to manufacture one for $\mathscr{L}$ by computing first elementary symmetric polynomials and interpolation coefficients in respective packages $x_0,\ldots,x_{n_1-1}, y_0,\ldots,y_{n_1-1},\ldots$ By [46] these can be computed with $11\sum_{i=1}^{t} n_i \log_2 n_i$ non-linear operations. □

Appendix A. The idea of the real spectrum, examples – a little ragôut

The subsequent additional comments are thought to ease the access to the specialized literature for the computer science reader.

Real algebra is not algebraic alone; in terms of logic, we have a richer language due to the presence of the "$\leq$" relational symbol. Consequently, rather than a "property," the non-algebraic notion of "positivity" must enjoy the full status of a "given thing" (a building stone) from the very beginning. Starting with the zeroes in $\mathbb{R}^n$ of polynomials $f_1,\ldots,f_r \in \mathbb{R}[X_1,\ldots,X_n]$, the evolution of real algebra can be considered as a series of "liberations" from various confinements in the way of contemplation such as the pure real number view, the pure field view, the pure real closed fields view, or the pure ordered fields view. We consciously do not comment on what we mean by these confinements and leave the aha-experience of checking Artin–Schreier theory and the culmination in the concept of the real spectrum to the reader.

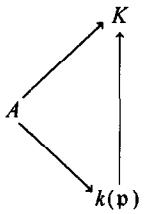
Artin–Schreier theory: Artin-Schreier theory introduces real fields, real closed fields, and ordered fields. A field K is called (formally) real if sum of squares in K are never -1. A field K is called a real closed field if it is real and does not admit proper algebraic extensions that are real. If $\leq$ is an ordering on a field K then its positive cone $P = \{x \in K : 0 \leq x\}$ satisfies the following axioms:

(i) $x \in P, y \in P \Rightarrow x+y \in P$,
(ii) $x \in P, y \in P \Rightarrow x \cdot y \in P$,
(iii) $x \in K \Rightarrow x^2 \in P$,
(iv) $-1 \notin P$,
(v) $P \cup -P = K$;

reversely, an ordering $\leq$ can be recovered from such a P by $x \leq y \Leftrightarrow y-x \in P$. Pairs $(K,\leq)$ are called ordered fields. Real fields are exactly those fields that can be equipped with an ordering. Reality is the "equational aspect" of ordered fields. If R is

a real closed field then there is one and only one ordering on R; its positive cone is the set of squares $P = \{x^2 : x \in R\}$. Every ordered field $(K, \leq)$ possesses an (essentially) unique real closure R, that is, an algebraic real closed extension field R of K the unique ordering of which induces the given one $\leq$ on K. We remark that real fields appear as the result of a *selecting* process via an *algebraic (equational) condition* and ordered fields as the result of a *supplying* process, the equipment with a *non-algebraic* notion of positivity.

The real spectrum: Prime ideals $\mathfrak{p}$ of a commutative ring A are the kernels of homomorphisms $A \to K$ into fields K which factor uniquely through the residue field,



Removing the arbitrariness of "becoming zero" in a field K one can restrict consideration to homomorphisms into residue fields $k(\mathfrak{p})$, resp. to the "quintessence" $\mathfrak{p}$ in A. This is the way to the Zariski spectrum

$$\operatorname{Spec} A = \{\mathfrak{p} : \mathfrak{p} \subset A \text{ prime ideal}\}.$$

Applying the above selection process accordingly by considering homomorphisms into real fields we arrive at the subspace of real prime ideals

$$(\operatorname{Spec} A)_{re} = \{\mathfrak{p} : \mathfrak{p} \text{ real prime ideal}\} \subseteq \operatorname{Spec} A$$

of the Zariski spectrum; $\mathfrak{p}$ is called real if $k(\mathfrak{p})$ is real. Applying the above supplying process accordingly we arrive at the one presentation of the real spectrum

$$\operatorname{Spec}_r A = \{(\mathfrak{p}, \leq) : \mathfrak{p} \text{ real}, \leq \text{ ordering on } k(\mathfrak{p})\}.$$

Alternatively, one can consider homomorphisms into ordered fields $\phi : A \to (K, \leq)$ (or into real closed fields with their unique ordering). The "quintessence in A" of "becoming ≥ 0" is a prime cone

$$\alpha = \{a \in A : \phi(a) \geq 0\};$$

every prime cone can be obtained in this way. This leads to the presentation of the real spectrum

$$\operatorname{Spec}_r A = \{\alpha : \alpha \subset A \text{ prime cone}\}$$

as the set of all prime cones of A.

We mention that the dimension $\dim \alpha$ of a prime cone α is simply defined as the dimension $\dim \operatorname{supp} \alpha$ of its support, that is, the Krull dimension of $A/\operatorname{supp} \alpha$. Unlike

for the Zariski spectrum, the specializations of a prime cone form always a totally ordered chain with a unique maximal specialization [8, 7.1.22 and 23]. Considering the associated chain of supports in $\operatorname{Spec} A$ it is clear that the length of the chain of specializations is at most $\dim \alpha = \dim \operatorname{supp} \alpha$, but it may be shorter (see the examples given below).

The formal properties of the real spectrum are analogous to those of the Zariski spectrum. Let $\phi : A \to B$ be a ring homomorphism. If β is a prime cone of B then its contraction in A

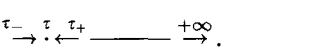
$$\alpha = \{a \in A : \phi(a) \in \beta\},$$

denoted $(\operatorname{Spec}_r \phi)(\beta)$, is a prime cone in A; indeed, if β is given by a homomorphism $B \to R$ into a real closed field R then α is given by the composition with ϕ. This means that Spec_r – like Spec – is a contravariant functor from the category of commutative rings into the category of topological spaces, and supp is a natural transformation of the functor Spec_r into the functor Spec. For every A the image of $\operatorname{supp}_A : \operatorname{Spec}_r A \to \operatorname{Spec} A$ is the subspace $(\operatorname{Spec} A)_{re}$. We remark that for the canonical processes of localization and taking residue classes $\operatorname{Spec}_r \phi$ are injective and homeomorphisms onto their images. If $B = A_S$, $S \subseteq A$ a multiplicative system, then the image is $\{\alpha \in \operatorname{Spec}_r A : S \cap \operatorname{supp} \alpha = \emptyset\}$; hereby α with $S \cap \operatorname{supp} \alpha = \emptyset$ corresponds to the prime cone $\{a/s : as \in \alpha\}$ of A_S. If $B = A/\mathfrak{a}$, $\mathfrak{a} \subseteq A$ an ideal, then the image is the zero-set $\mathscr{Z}(\mathfrak{a}) = \{\alpha \in \operatorname{Spec}_r A : \mathfrak{a} \subseteq \operatorname{supp} \alpha\}$.

The real spectrum of a polynomial ring, the tilde, examples of minimal prime cones and halos: We mention first a prototype construction of a generization which gives many examples of prime cones by using morphisms. Let $(A, \mathfrak{m})$ be a real discrete valuation (real means that $\mathfrak{m}$ is real), t a generator of $\mathfrak{m}$. If $\alpha \in \operatorname{Spec}_r A$ representing an ordering on $k(\mathfrak{m})$ is given then there is one and only one proper generization $\alpha_+ \in \operatorname{Spec}_r A$ with $t \in \alpha_+$. Assume a non-zero element $a \in A$ to be written as $a = ut^r$ with $u \in A$ a unit, then

$$a \in \alpha_+ \iff u \in \alpha.$$

Applying the same procedure to the generator $-t$ yields a generization α_- of α. It is easy to see that both generizations have support 0, and $\operatorname{hal} \alpha = \{\alpha_+, \alpha, \alpha_-\}$. The prime cones α_+ and α_- correspond to orderings of the quotient field FrA of A. (FrA is therefore real). For example, if $A = \mathbb{R}[T]_{(T-\tau)}$, and τ also denotes the prime cone α_τ corresponds to the evaluation in $\tau \in \mathbb{R}$, then τ_+ and τ_- correspond to orderings of the rational function field $\mathbb{R}(T)$ in which $T - \tau$ is a positive resp. negative infinitesimal over $\mathbb{R}$. For $f \in \mathbb{R}[T]$ we have $f \geq_{\tau_+} 0$ iff finally $f(\sigma) \geq 0$ when $\sigma \in \tau + \mathbb{R}_+$ is moved down to τ. So the idea of τ_+ is that of a "sneaker" on the real line. (Analogously for τ_-.) The contractions of 0_+ and 0_- with respect to $\mathbb{R}[1/T] \hookrightarrow \mathbb{R}(T)$ gives us further prime cones $+\infty, -\infty \in \operatorname{Spec}_r \mathbb{R}[1/T] \subset \operatorname{Spec}_r \mathbb{R}(1/T) = \operatorname{Spec}_r \mathbb{R}(T)$. These "sneakers" can be visualized on the real line as arrows



The real spectrum of $\mathbb{R}[T]$ is completely described as

$$\mathrm{Spec}_r\,\mathbb{R}[T] = \{-\infty\} \cup \bigcup_{\tau\in\mathbb{R}} \{\tau_-, \tau, \tau_+\} \cup \{+\infty\}$$

[8, 7.1.4]; $+\infty$ and $-\infty$ are minimal and maximal. The real spectrum of its quotient field $\mathbb{R}(T)$ is the "space of orderings"

$$\mathrm{Spec}_r\,\mathbb{R}(T) = \{-\infty\} \cup \bigcup_{\tau\in\mathbb{R}} \{\tau_-, \tau_+\} \cup \{+\infty\},$$

it consists of all "one-dimensional sneakers," that is, the minimal prime cones of $\mathrm{Spec}_r\,\mathbb{R}[T]$. Also the tilde can be made "visible;" for instance, the tilde of the half-line $H = \{\tau : \tau \geq 0\}$ is

$$\tilde{H} = \{0, 0_+\} \cup \bigcup_{\tau>0} \{\tau_-, \tau, \tau_+\} \cup \{+\infty\}.$$

Its minimal prime cones are given as

$$\tilde{H}^{\min} = \{0_+\} \cup \bigcup_{\tau>0} \{\tau_-, \tau_+\} \cup \{+\infty\},$$

its maximal ones compactify the right end of the half-line H,

$$\tilde{H}^{\max} = H \cup \{+\infty\}.$$

Next we exemplify prime cones in the two-variable case $\mathbb{R}[X, Y]$. The zero-dimensional prime cones correspond to the points in the plane $\mathbb{R}^2$. The one-dimensional prime cones are "sneakers" on algebraic curves, or "half branches" of algebraic curves [8, 10.3.3]. Let $f \in \mathbb{R}[X, Y]$ be an irreducible polynomial with $\mathfrak{p} = (f)$ being real. Assume the composition $\mathbb{R}[X] \hookrightarrow \mathbb{R}[X, Y] \to k(\mathfrak{p})$ to be injective, and let $\mathbb{R}(X) \hookrightarrow k(\mathfrak{p})$ be the induced extension. Every ordering on $k(\mathfrak{p})$ induces an ordering on $\mathbb{R}(X)$ – a "sneaker on the X-axis" –, and for every ordering on $\mathbb{R}(X)$ there are finitely many orderings or no ordering on $k(\mathfrak{p})$ extending the given one on $\mathbb{R}(X)$. The picture is as follows:

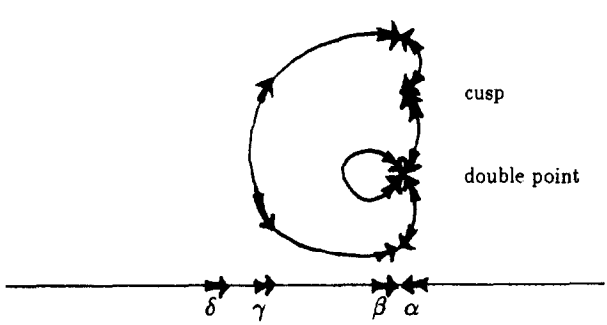


Fig. A.

In this example there are 6 orderings of $k(\mathfrak{p})$ over α, 4 over β, 2 over γ, and none over δ.

Now we give examples of two-dimensional prime cones in $\mathrm{Spec}_r\,\mathbb{R}[X,Y]$. Let again $f \in \mathbb{R}[X,Y]$ be irreducible, $\mathfrak{p} = (f)$, α be a "sneaker" on the curve $f = 0$, that is an ordering on $k(\mathfrak{p})$. $\mathbb{R}[X,Y]_{\mathfrak{p}}$ is a real discrete valuation ring, $f \in \mathbb{R}[X,Y]_{\mathfrak{p}}$ an uniformization parameter. There are two proper generizations α_- and α_+ of α – orderings on $\mathbb{R}(X,Y)$ –. They "sneak" into α, and can be considered as the two "banks" of α. The picture is as follows:

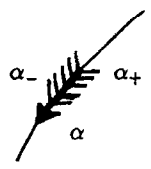


Fig. B.

The picture makes "visible" that α_- belongs to $\{f < 0\}^{\sim}$ and that α_+ belongs to $\{f > 0\}^{\sim}$. (So the indices should more precisely be $-f$ and f rather than $-$ and $+$.)

This construction can be iterated in $\mathbb{R}[X_1,\ldots,X_n]$ accordingly if a regular system of parameters in $\mathbb{R}[X_1,\ldots,X_n]_{(X_1,\ldots,X_n)}$ is given.

Remark A.1. Although the idea of "sneakers" (infinitesimals) is very basic, there are in general further orderings on $R(T)$, R being a real closed field. For example, if $R = \mathbb{R}_{\mathrm{alg}}$ is the field of real algebraic numbers, and $\tau \in \mathbb{R}$ is a transcendental number, then τ_-, τ, τ_+ contract with respect to the inclusion $\iota : \mathbb{R}_{\mathrm{alg}}[T] \hookrightarrow \mathbb{R}[T]$ to the same one-dimensional prime cone $(\mathrm{Spec}_r\,\iota)(\tau_-) = (\mathrm{Spec}_r\,\iota)(\tau) = (\mathrm{Spec}_r\,\iota)(\tau_+)$ which is minimal and maximal. Note that the transcendental extension $\mathbb{R}_{\mathrm{alg}} \hookrightarrow \mathbb{R}_{\mathrm{alg}}(T)$ is *Archimedian* with respect to the corresponding ordering on $\mathbb{R}_{\mathrm{alg}}(T)$, whereas $\mathbb{R}$ does not possess Archimedian extensions. Even if we start with the reals $\mathbb{R}$, this property is immediately lost if we pass to a simple transcendental extension of $\mathbb{R}$: We mention further that there are two-dimensional prime cones in $\mathrm{Spec}_r\,\mathbb{R}[X,Y]$ that do not possess one-dimensional specializations, but zero-dimensional ones (see [8, 10.3.5]):

Let $\mathbb{R}\langle X\rangle$ denote the ring of convergent power series. $\mathbb{R}\langle X\rangle$ is a discrete valuation ring; let $0_-, 0_+$ denote the two proper generizations of the maximal prime cone associated with the evaluation in $0 \in \mathbb{R}$. Consider the embedding $\iota : \mathbb{R}[X,Y] \hookrightarrow \mathbb{R}\langle X\rangle$ sending Y to the power series (expansion in 0) of the exponential function. Then $(\mathrm{Spec}_r\,\iota)(0_+)$ is a "sneaker" on a transcendental curve, the graph of the exponential function. It has dimension 2, and its sole specialization is the point $(0,1) \in \mathbb{R}^2$. (If we "sneak" to "infinity" on a transcendental plane curve we get two-dimensional prime cones of $\mathrm{Spec}_r\,\mathbb{R}[X,Y]$ that are minimal and maximal.)

Secondly, take the irreducible polynomial $X \in \mathbb{R}[X,Z]$, α a "sneaker" on the Z-axis specializing into the point $(0,0) \in \mathbb{R}^2$, and let $\beta \in \mathrm{Spec}_r\,\mathbb{R}[X,Z]$ one of the both two-

dimensional generizations. The contraction of β with respect to the $\mathbb{R}(X)$-isomorphism $\mathbb{R}(X,Y) \to \mathbb{R}(X,Z)$, $Y \mapsto Z/X$, is a "corkscrew" prime cone in $\mathrm{Spec}_r\, \mathbb{R}(X,Y)$ specializing in $\mathrm{Spec}_r\, \mathbb{R}[X,Y]$ only into the point $(0,0)$ of the "(X,Y)-plane."

In order to illustrate minimal prime cones of semi-algebraic set, let $E \subset \mathbb{R}^n$ be an irreducible algebraic subset of dimension d. The minimal prime cones of $\tilde{E}$ split into two parts. The "main" part consists of the d-dimensional prime cones, that is, the orderings of the function field $k(E)$,

$$\mathrm{Spec}_r\, k(E) = ((\mathrm{Reg}\, E)^{\sim})^{\min};$$

the others lie in $(\mathrm{Sing}\, E)^{\sim}$, the tilde of the singular locus of E. For instance, if $f = Y^2 + X^2 - X^3$, and $E \subset \mathbb{R}^2$ is the cubic of the equation $f = 0$,

Fig. C.

then $\tilde{E}^{\min}$ consists of all one-dimensional "sneakers" on the one-dimensional part on the right plus the isolated singular point $(0,0) \in E$. In the case of the "umbrella" $E \subset \mathbb{R}^3$ of the equation $z^2 x = y^2$, $\tilde{E}$ consists of all two-dimensional prime cones in the tilde of $E \cap \{x \geq 0\}$ plus all one-dimensional "sneakers" on the "stick" $\{z = y = 0, x < 0\}$ (cf. [8, 3.5.9]):

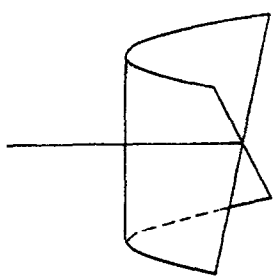


Fig. D.

If $E \subset \mathbb{R}^n$ is semi-algebraic and $\alpha \in \tilde{E}^{\min}$ then there is an open semi-algebraic set $U \subset \mathbb{R}^n$ such that $\alpha \in \tilde{U}$, and E coincides with the zero set of $\mathrm{supp}\, \alpha$ inside U. The minimal prime cones of $\tilde{E} \cap \tilde{U}$ and $\mathscr{Z}(\mathrm{supp}\, \alpha) \cap \tilde{U}$ are the same.

Next we "visualize" halos in some concrete cases: As mentioned above, the halo of a point $\tau \in \mathbb{R}$ on the real line consists of τ and its left and right "sneakers" τ_- and

τ_+; the halo in $\mathrm{Spec}_r\,\mathbb{R}[X,Y]$ of a "sneaker" α on a curve in $\mathbb{R}^2$ adds to α its two "banks." The halo of a point in the plane $\mathbb{R}^2$ adds to the point the whole "corona" of its one- and two-dimensional generizations. (The halo of a disk looks in fact like the halo of the "moon.") The halo in $\mathrm{Spec}_r\,\mathbb{R}[X,Y,Z]$ of a "sneaker" α on a curve in $\mathbb{R}^3$ looks like a "bouquet" around α, the halo in $\mathrm{Spec}_r\,\mathbb{R}[X,Y,Z]$ of a two-dimensional prime cone α adds to α the two "sides" of the "diaphragm" α.

Beside the two "banks" of a "sneaker" on a plane curve mentioned above here are some further examples of two prime cones with a common specialization.

Example A.2. We consider surfaces $E \subset \mathbb{R}^3$.

(1) Let E be the union of the two planes of the equations $x = z$ and $x = -z$ which intersect transversally in the y-axis.

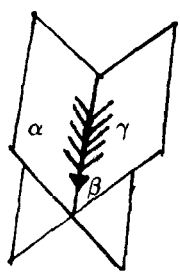


Fig. E.

Here β is a "sneaker" on the y-axis. The two-dimensional α and γ with different supports are generizations in the tildes of the two different planes.

(2) Let E be the union of the two surfaces of the equations $x = z^2$ and $x = -z^4$ which touch in the y-axis.

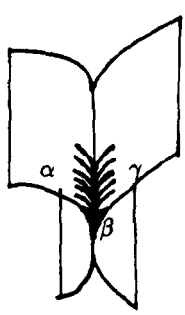


Fig. F.

Here β is a "sneaker" on the y-axis. The two-dimensional α and γ with different supports are generizations in the tildes of the two different irreducible surfaces.

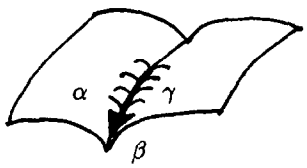


Fig. G.

(3) Let E be the irreducible surface of the equation $z^3 = (y + x^2)^2$.

Here β is a "sneaker" on the singular locus $\operatorname{Sing} E = \{z = y + x^2 = 0\}$, α and γ are the two proper generizations in $\tilde{E}$.

Let $\mathfrak{p} = (Z^3 - (Y + X^2)^2) \subset A = \mathbb{R}[X, Y, Z]$. It is easy to realize the difference between sign and exclusion complexity for the real discrete valuation ring $(B, \mathfrak{m}) = \mathbb{R}[X, f]_{(f)} \subset k(\mathfrak{p}) = k(E)$ where $f = (Y + X^2)^{1/3}$:

$$S(c_*, (X, Y, Z)(\mathfrak{p}), B) > E(c_*, (X, Y, Z)\hat{}, \mathfrak{m}) = 0;$$

here $(X, Y, Z)\hat{}$ denotes the image of $(X, Y, Z) \in \mathbb{A}^3_{\mathbb{R} \to A}$ in $\mathbb{A}^3_{\mathbb{R} \to B}$.

Acknowledgements

The author would like to thank W. Baur, S. Breitsprecher, M.-F. Roy, and A. Schönhage for discussion. Likewise thanks go to the referee for carefully reading the manuscript and constructive comments. This work has been sponsored by a DFG Heisenberg fellowship (Grant Li 405/2-1).

References

[1] W. Baur, manuscript, Universität Konstanz (1989).
[2] W. Baur and V. Strassen, The complexity of partial derivatives, Theoret. Comput. Sci. 22 (1983) 317–330.
[3] E. Becker, On the real spectrum of a ring and its applications to semi-algebraic geometry, Bull. Am. Math. Soc. (N. S.) 15 (1986) 19–60.
[4] M. Ben-Or, Lower bounds for algebraic computation trees, Proc. 15th ACM STOC, Boston (1983) 80–86.
[5] G. Birkhoff and J.D. Lipson, Heterogeneous algebras, J. Combin. Theory 8 (1970) 115–133.
[6] A. Björner and L. Lovász, Linear decision trees, subspace arrangements and Möbius function, preprint (1992).
[7] A. Björner, L. Lovász and A. Yao, Linear decision trees: volume estimates and topological bounds, Proc. STOC'92 (1992) 170–177.
[8] J. Bochnak, M. Coste and M.-F. Roy, Géométrie algébrique réelle, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band 12 (Springer, Berlin, 1987).
[9] L. Blum, M. Shub and S. Smale, On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines, Bull. Amer. Math. Soc. 21 (1989) 1–46.
[10] P. Bürgisser, M. Karpinski and T. Lickteig, On randomized semi-algebraic decision complexity, J. Complexity 9 (1993) 231–251.

[11] P. Bürgisser and T. Lickteig, Verification complexity of linear prime ideals, J. Pure Appl. Algebra 81 (1992) 247–267.
[12] P. Bürgisser, T. Lickteig and M. Shub, Test complexity of generic polynomials, J. Complexity 8 (1992) 203–215.
[13] P.M. Cohn, Universal Algebra, Mathematics and its Applications 16 (Reidel, Dordrecht, Holland, 1981).
[14] M. Demazure and P. Gabriel, Introduction to algebraic geometry and algebraic groups, Math. Stud. (North Holland, Amsterdam, 1980).
[15] G. Grätzer, Universal Algebra (Springer, Berlin, 2nd ed., 1979).
[16] D. Grigoriev, M. Karpinski and N. Vorobjov, Lower bounds on testing membership to a polyhedron by algebraic decision trees, Proc. STOC'94, to appear.
[17] R. Hartshorne, Algebraic Geometry, Graduate Texts in Mathematics 52 (Springer, Berlin, 1977).
[18] J. Heintz, Definability and fast quantifier elimination over algebraically closed fields, Theoret. Comput. Sci. 24 (1983) 239–278.
[19] M.D. Hirsch, Lower bounds for the non-linear complexity of algebraic computation trees with integer inputs, Comput. Complexity 1 (1991) 257–268.
[20] G. Hotz and J. Sellen, On algebraic computation trees and Betti numbers, Tech. Report No. 10/93, Sonderforschungsbereich 124, Saarbrücken–Kaiserslautern, Germany (1993).
[21] E. Kaltofen, B.D. Saunders and M. Singer, Size efficient parallel algebraic circuits for partial derivatives, Tech. Report, Rensselaer Polyt. Institute, Troy, NY (1988).
[22] M. Knebusch and C. Scheiderer, Einführung in die reelle Algebra, Vieweg-Studium 63 (Aufbaukurs Mathematik, Vieweg, 1989).
[23] E. Kunz, Einführung in die kommutative Algebra und algebraische Geometrie, Vieweg-Studium 46 (Aufbaukurs Mathematik, Vieweg, 1980).
[24] T. Lickteig, On semialgebraic decision complexity, Tech. Report TR-90-052 Int. Comp. Science Inst., Berkeley (1990) and Univ. Tübingen, Habilitationsschrift.
[25] T. Lickteig, Semi-algebraic decision complexity and approximative complexity, in preparation.
[26] S. Linnainmaa, Taylor expansion of the accumulated rounding error, BIT 16 (1976) 146–160.
[27] H. Matsumura, Commutative ring theory, Cambridge Studies in Advanced Mathematics 8 (Cambridge Univ. Press, Cambridge, 1986).
[28] F. Meyer auf der Heide, A polynomial linear search algorithm for the n-dimensional knapsack problem, J. ACM 31 (1984) 668–676.
[29] J. Milnor, On the Betti numbers of real varieties, Proc. Amer. Math. Soc. 15 (1964) 275–280.
[30] J.L. Montaña, J.E. Morais and L.M. Pardo, Lower bounds for arithmetic networks II: sum of Betti numbers, AAECC 7 (1995), to appear.
[31] J.L. Montaña and L.M. Pardo, Lower bounds for arithmetic networks, AAECC 4 (1993) 1–24.
[32] 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) (Birkhäuser, Base, 1991) 347–361.
[33] J. Morgenstern, Complexité linéaire de calcul, Thése, Université de Nice, (1978)
[34] J. Morgenstern, How to compute fast a function and all its derivatives, SIGACT News 16 (1985) 60–62.
[35] R. Mennicken and E. Wagenführer, Numerische Mathematik 2, rororo Vieweg, Grundkurs Mathematik (1977).
[36] A. Prestel, Lectures on formally real fields, Lecture Notes in Mathematics, Vol. 1093 (Springer, Berlin, 1984).
[37] A. Prestel, Einführung in die Mathematische Logik und Modelltheorie, Vieweg-Studium 60 (Aufbaukurs Mathematik, Vieweg, 1986).
[38] M.-F. Roy, Faisceau structural sur le spectre réel et fonctions de Nash, in: Géométrie algébrique réelle et formes quadratiques, Lecture Notes in Mathematics, Vol. 959 (Springer, Berlin, 1982) 406–432.
[39] C.P. Schnorr, An extension of Strassen's degree bound, SIAM J. Comput. 10 (1981) 371–382.
[40] A. Schönhage, Approximationstheorie (de Gruyter, Berlin, 1971).
[41] A. Schönhage, An elementary proof for Strassen's degree bound, Theoret. Comput. Sci. 3 (1976) 267–272.
[42] P. Schuster, Interpolation und Kettenbruchentwicklung, Die Komplexität einiger Berechnungsaufgaben, Dissertation, Universität Zürich (1980).
[43] J.M. Steele and A.C.C. Yao, Lower bound for algebraic decision trees, J. Algorithms 3 (1982) 1–8.

[44] H.J. Stoß, The complexity of evaluating interpolation polynomials, Theoret. Comput. Sci. 41 (1985) 319–323.
[45] V. Strassen, Berechnung und Programm I, Acta Inform. 1 (1973) 320–335.
[46] V. Strassen, Die Berechnungskomplexität von elementarsymmetrischen Funktionen und Interpolationskoeffizienten, Num. Math. 20 (1973) 238–251.
[47] V. Strassen, The computational complexity of continued fractions, SIAM J. Comput. 12 (1983) 1–27.
[48] R. Thom, Sur l'homologie des variétés algébriques réelles, in: S.S. Cairns, ed., Differential and Combinatorial Topology (Princton Univ. Press, Princeton, 1965) 255–265.
[49] W. Vogel, On Results on Bézout's Theorem, Lecture Notes, TATA Institute of Fundamental Research, Bombay, No. 74 (1984).
[50] A.C.C. Yao, Lower bounds for algebraic computation trees with integer inputs, SIAM J. Comput. 20 (1989) 655–668.
[51] A.C.C. Yao, Algebraic decision trees and Euler characteristics, Proc. FOCS'92 (1992) 268–277.
[52] A.C.C. Yao, Decision trees and Betti numbers, Proc. STOC'94 (1994), to appear.