DECISION COMPLEXITY OF GENERIC COMPLETE INTERSECTIONS

PETER BÜRGISSER

Abstract. We study the complexity of algebraic decision trees that decide membership in a semi-algebraic subset $X \subseteq R^m$, where R is a real (or algebraically) closed field. We prove a general lower bound on the verification complexity (cf. [5, 14]) of the vanishing ideal of an irreducible algebraic subset $X \subseteq R^m$ in terms of the degree of transcendency of its minimal field of definition. As an application, we determine exactly the number of additions, subtractions and comparisons that are needed to test membership in a generic complete intersection $X = Z(f_1, \ldots, f_r) \subseteq R^m$; for the number of multiplications, divisions and comparisons needed, we obtain an asymptotically optimal lower bound as $\max_i \deg f_i \to \infty$. This generalizes the main results in [6]. A further application is given to test problems related to partial or continued fractions.

Key words. Algebraic decision trees, straight line programs, transcendence degree bounds.

Subject classifications. 68C20, 68C25, 14P10.

1. Introduction

Let $f_1, \ldots, f_r \in \mathrm{R}[x_1, \ldots, x_m]$ be polynomials. We study the complexity of the algorithmic problem of deciding whether a given input vector $\xi \in \mathrm{R}^m$ is a solution of the system of equations

$$f_1(x) = 0, \ldots, f_r(x) = 0,$$

i.e. of deciding whether ξ lies in the zeroset X of these polynomials. Possible decision procedures are e.g. obtained as follows: let $f_1', \ldots, f_r'$ be a sequence of polynomials generating the same ideal as $f_1, \ldots, f_r$. The decision procedure then consists in evaluating $f_1', \ldots, f_r'$ at an input $\xi \in \mathrm{R}^m$ and testing the resulting values for zero. More generally, we allow as decision procedures any algorithms which compute with the four basic arithmetic operations , perform tests according to $=$- or $\leq$-comparisons and use preconditioned real constants.

Formally, such algorithms are described as algebraic decision trees. The R-preconditioned decision complexity $C(X)$ of a semi-algebraic subset $X \subset \mathrm{R}^m$ is defined as the minimum number of arithmetic operations and comparisons needed by an algebraic decision tree deciding membership in X.

Let us briefly summarize some known lower bound results. Ben-Or [3] shows, using a result from real algebraic geometry due to Milnor and Thom,

$$C(X) \geq (\log_2 N - m \log_2 3)/\log_2 6,$$

where N is the number of connected components of a semi-algebraic subset X of R^m. If X is an irreducible hypersurface and (f) its vanishing ideal, then by Lickteig [14]

$$\begin{aligned} C(X) \;\; \geq \;\; & \log_2 \deg \operatorname{graph}(x_1\partial_1 f, \ldots, x_m \partial_m f) \mid_X \\ & - \log_2 \deg X - \log_2(m+1). \end{aligned}$$

If the coefficients of f are algebraically independent over Q, then by Bürgisser-Lickteig-Shub [6]

$$C(X) \sim \frac{3}{2}\binom{\deg f + m}{m} \quad \text{as } \deg f \to \infty. \tag{1.1}$$

In this paper we generalize (1.1) to algebraic subsets $X \subset \mathrm{R}^m$ which are Q-generic complete intersections, i.e. X is zeroset of $r < m$ polynomials $f_1, \ldots, f_r$ whose total system of coefficients is algebraically independent over Q and $\operatorname{codim}_{\mathrm{R}^m} X = r$. Let $d_i := \deg f_i$ and write for $\ell \in \mathrm{N}$

$$\begin{aligned} S(d_1, \ldots, d_r)^{(\ell)} := \;\; \{ \;\; & g \in \mathrm{R}[x_0, x_1, \ldots, x_m] : g \text{ homogeneous of degree } \ell, \\ & \deg_{x_1} g < d_1, \ldots, \deg_{x_r} g < d_r \}. \end{aligned}$$

Then we can show

$$C(X) \sim \frac{3}{2} \sum_{i=1}^{r} \dim S(d_1, \ldots, d_r)^{(d_i)} \quad \text{as } \max d_i \to \infty. \tag{1.2}$$

We remark that $\dim S(d_1, \ldots, d_r)^{(\ell)}$ is just the value at ℓ of the Hilbert function of the homogenization of the vanishing ideal of X. If $\max_i d_i < 2 \min_i d_i$, then the right-hand side of (1.2) equals

$$\frac{3}{2} \sum_{i=1}^{r} \left[\binom{d_i + m}{m} - \sum_{j : d_j \leq d_i} \binom{d_i - d_j + m}{m} \right];$$

for $d = d_1 = \ldots = d_r$ this becomes $\frac{3}{2}r(\binom{d+m}{m} - r)$. The upper bound in (1.2) is obtained in the following way. First, we prove that there exists an ideal basis $f'_1, \ldots, f'_r$ of $(f_1, \ldots, f_r)$ satisfying $f'_i \in y_i^{d_i} + S(d_1, \ldots, d_r)^{(d_i)}$. Then we show, using a result by Eve [7], that the complexity of $f'_1, \ldots, f'_r$ is asymptotically bounded from above by the right-hand side of (1.2) as $\max_i d_i \to \infty$. The lower bound in (1.2) turns out to be a consequence of a much more general result: if $X \subset \mathrm{R}^m$ is an irreducible algebraic subset with minimal field of definition K, then

$$C(X) \geq \frac{3}{2}\mathrm{tr.deg}_{\mathrm{Q}}K. \tag{1.3}$$

The proof of (1.3) is based on the transcendence degree bounds for complexity (cf.[1, 2, 6, 16, 17]) and the following observation: let $X \subseteq Y \subseteq \mathrm{R}^m$ be algebraic subsets, X irreducible and assume that Y is defined over a subfield K of R. If $X \cap W = Y \cap W$ for some Euclidean open subset W of R^m containing a nonsingular point of X, then X is defined over K.

Let us now indicate the organization of the paper. In Section 2 we introduce notations and give definitions connected with algebraic decision trees. Following the approach initiated by Lickteig [14] we focus on the auxiliary, purely algebraic notion of real verification complexity, which provides lower bounds on decision complexity. In Section 3 we recall the notion of the minimal field of definition $\mathrm{def}_{R/k}(I)$ of an ideal I in $R \otimes_k A$, A being a k-algebra and $k \to R$ a field extension. A lower bound on the real verification complexities of localizations $(R \otimes_k A)_p$ in real prime ideals p of $R \otimes_k A$ in terms of the transcendence degree of $\mathrm{def}_{R/k}(p)$ over k is proved under general assumptions. Section 4 is devoted to our main application of this result to generic complete intersections. In Section 5 we give another application to test problems related to "general" partial or continued fractions, obtaining optimal lower bounds.

In fact, we prove separate lower bounds holding for the number of additions, subtractions and comparisons, respectively for the number of multiplications, divisions and comparisons. Also, it is shown that analogous results for algebraically closed fields and equality branching trees hold.

2. Some terminology

We recall some definitions following the terminology in Lickteig [14] and Bürgisser-Lickteig [5]. Let $k \to R$ be a field extension, R real closed (e.g. $k = \mathrm{Q}$, $R = \mathrm{R}$). We consider (Ω^k, P)-decision trees T over $m \in \mathrm{N}$; these decision trees take as inputs elements from R^m, use operations in $\Omega^k := k \sqcup \{0, 1, +, -, *, /\}$ ($\lambda \in k$ stands for the scalar multiplication with λ) and branch according to the

relations in $P := \{=, \leq\}$. To each leaf of such a tree T is assigned one of the symbols *yes* or *no*. For $\xi \in R^m$ we denote by T_ξ the path in T defined by the input ξ (leading to a leaf or ending prior to an unexecutable instruction).

Let $X \subseteq Y \subseteq R^m$ be semi-algebraic subsets. We say that T decides the partition $\{X, Y \setminus X\}$ of Y (or T decides membership in X relative to Y) if for all $\xi \in X$ the path T_ξ ends up with a *yes*-leaf and for all $\xi \in Y \setminus X$ the path T_ξ ends up with a *no*-leaf.

Let $c : \Omega^k \sqcup P \to \mathbf{N}$ be a cost function (e.g. $c_+ := 1_{\{+,-\}}$ or $c_* := 1_{\{*,/\}}$). The c-length $L(c, \pi)$ of a path π in T is defined as the sum of the costs along π; the c-cost of the tree T is the maximum of the $L(c, \pi)$ taken over all paths π in T. The *decision complexity* $C(c, \{X, Y \setminus X\})$ of the partition $\{X, Y \setminus X\}$ of Y with respect to (k and) c is defined as

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

where T varies over all (Ω^k, P)-decision trees over m deciding the partition $\{X, Y \setminus X\}$. One has $C(c, \{X, Y \setminus X\}) < \infty$ for semi-algebraic X and Y if and only if X is the trace in Y of a k-definable subset of R^m. In order to deal with arbitrary partitions $\{X, Y \setminus X\}$ one must allow preconditioning of certain $\zeta_1, \ldots, \zeta_s \in R$. This fits naturally into our model if we view these preconditioned "constants" $\zeta_1, \ldots, \zeta_s$ as additional, fixed inputs; so we consider partitions

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

of $\{\zeta\} \times Y \subseteq R^{s+m}$. We define the *R-preconditioned decision complexity* of $\{X, Y \setminus X\}$ with respect to c as

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

(The quantity $C(X)$ in the introduction is defined formally in this way considering $c = 1_\Omega Q_{\sqcup P}$ which counts all operations and comparisons at unit cost.)

For proving lower bounds on decision complexity we employ the auxiliary notion of real verification complexity introduced in [5]. Its definition involves some real algebraic geometry , in particular the notion of the real spectrum of a commutative ring. In [5] a short summary of the basic facts of this theory which are needed for our purposes can be found. For a detailed presentation of this theory the reader is referred to the books by Bochnak-Coste-Roy [4] and Knebusch-Scheiderer [10].

Let us recall the definition of real verification complexity. Let A be a commutative k-algebra. The *real verification complexity* of a real prime ideal

$p \in \operatorname{Spec} A$ in a prime cone $\alpha \in \operatorname{Spec}_r A$ of support p with respect to an input $x \in A^m$ and a cost function $c : \Omega^k \to \mathbf{N}$ is defined as

$$\begin{aligned} VC_{r,k\to A}(c,x,\alpha) \;:=\; & \min\{L_{k\to A}(c,x,F) : F \subseteq A \text{ finite}, \\ & Z(F) \cap W = Z(p) \cap W \\ & \text{for some neighbourhood } W \text{ of } \alpha \text{ in } \operatorname{Spec}_r A\}. \end{aligned}$$

Here $L_{k\to A}(c,x,F)$ denotes the *straight line program complexity* to compute F in the k-algebra A from the components of x with respect to the cost function c. So the real verification complexity is the complexity of a cheapest set of "functions" whose zeroset coincides with that of p locally at α. The relation to decision complexity is as follows: Let $X \subseteq Y \subseteq R^m$ be algebraic subsets, X irreducible, and let $\mathcal{O}_{X,Y} := (R[x_1,\ldots,x_m]/I(Y))_{I(X)}$ be the localization of the coordinate ring of Y in the vanishing ideal $I(X)$ of X. Then we have for any prime cone $\alpha \in \operatorname{Spec}_r \mathcal{O}_{X,Y}$ with $\operatorname{supp}\alpha = I(X)$ and $x' := (x_1 + I(Y), \ldots, x_m + I(Y))$

$$C(c,\{X, Y \setminus X\}) \geq VC_{r,k\to\mathcal{O}_{X,Y}}(c\mid_{\Omega^k}, x', \alpha) \tag{2.4}$$

provided that the cost function c satisfies $c(-) \leq \min\{c(=), c(\leq)\}$.

When dealing with nonordered fields R we study a counterpart of real verification complexity, the *Zariski verification complexity*, which is defined as

$$VC_{k\to A}(c,x,p) := \min\{L_{k\to A}(c,x,F) :\; F \subseteq A \text{ finite}, Z(F) = Z(p) \text{ in } \operatorname{Spec} A\}$$

for a commutative k-algebra A, $p \in \operatorname{Spec} A$, $x \in A^m$ and $c : \Omega^k \to \mathbf{N}$ a cost function (cf. [5, 14]).

3. Verification complexity and degree of transcendency

Let $k \to R$ be a field extension, A a commutative k-algebra and $F \subseteq R \otimes_k A$ be a subset. There is a smallest subfield K of R containing k such that $F \subseteq K \otimes_k A$. We call this subfield the *coefficient field of F in R over k* and denote it by $\operatorname{coeff}_{R/k}(F)$.

Let $I \subseteq R \otimes_k A$ be an ideal. We say that I *is defined over* A if $I = R \otimes_k J$ for some ideal J of A. For every ideal $I \subseteq R \otimes_k A$ there is a unique smallest subfield K of R containing k such that I is defined over $K \otimes_k A$ with respect to the isomorphism $R \otimes_k A = R \otimes_K (K \otimes_k A)$ (cf. Lang [13, p. 62, chapt. III, Thm. 7]). K is called the *minimal field of definition of I in R over k* and denoted by $\operatorname{def}_{R/k}(I)$. $\operatorname{def}_{R/k}(I)$ is the smallest subfield K of R containing k

such that there exists an ideal basis F of I satisfying $\mathrm{coeff}_{R/k}(F) \subseteq K$. We remark that for a polynomial $g \in R[x] = R \otimes_k k[x]$ we have

$$\mathrm{def}_{R/k}(gR[x]) = \mathrm{coeff}_{R/k}(g) \tag{3.5}$$

if one of the coefficients of g lies in $k^\star$.

THEOREM 3.1. *Let k be a subfield of a perfect field R , let A be a finitely generated k-algebra and assume $p \in \mathrm{Spec}\, R \otimes_k A$. Moreover, let $\zeta \in R^r$, $a \in A^s$ for some $r, s \in \mathbf{N}$. Then:*

1. *For the real verification complexities we have for any prime cone $\alpha \in \mathrm{Spec}_r\, R \otimes_k A$ with $\mathrm{supp}\, \alpha = p$*

$$VC_{r,k\to(R\otimes_k A)_p}(c_+, \zeta a, \alpha) \geq \mathrm{tr.deg}_k \mathrm{def}_{R/k}(p), \tag{3.6}$$

$$VC_{r,k\to(R\otimes_k A)_p}(c_*, \zeta a, \alpha) \geq \frac{1}{2}(\mathrm{tr.deg}_k \mathrm{def}_{R/k}(p) - \mathrm{ht}\, p). \tag{3.7}$$

2. *For the Zariski verification complexities we have*

$$VC_{k\to(R\otimes_k A)_p}(c_+, \zeta a, p') \geq \mathrm{tr.deg}_k \mathrm{def}_{R/k}(p), \tag{3.8}$$

$$VC_{k\to(R\otimes_k A)_p}(c_*, \zeta a, p') \geq \frac{1}{2}(\mathrm{tr.deg}_k \mathrm{def}_{R/k}(p) - \mathrm{ht}\, p), \tag{3.9}$$

where $p' := p(R \otimes_k A)_p$.

The proof is based on the subsequent Theorem 3.2 and Lemma 3.3.

THEOREM 3.2. *Let $k \to R$ be a field extension, A a k-algebra and $p \in \mathrm{Spec}\, R \otimes_k A$. Moreover assume that $F = \{f_1, \ldots, f_t\}$ is a finite subset of the localization $(R \otimes_k A)_p$ and let $\zeta \in R^r$, $a \in A^s$ for some $r, s \in \mathbf{N}$. Then:*

1. *there exists $\mathcal{U} = \{u_0, \ldots, u_t\} \subseteq R \otimes_k A$ with $u_0 \notin p$ such that for $i = 1, \ldots, t$*

$$Rf_i = Ru_i/u_0, \quad L_{k\to(R\otimes_k A)_p}(c_+, \zeta a, F) \geq \mathrm{tr.deg}_k \mathrm{coeff}_{R/k}(\mathcal{U});$$

2. *there exists $\mathcal{U} = \{u_0, \ldots, u_t\} \subseteq R \otimes_k A$ with $u_0 \notin p$ such that for $i = 1, \ldots, t$*

$$f_i + R = u_i/u_0 + R, \quad 2L_{k\to(R\otimes_k A)_p}(c_*, \zeta a, F) \geq \mathrm{tr.deg}_k \mathrm{coeff}_{R/k}(\mathcal{U}).$$

The proof is analogous as in [1, 2, 16, 17] or [6, Thm. 3].

LEMMA 3.3. *Let $k \to R$ be a separable field extension with the property that k is algebraically closed in R. Furthermore let A be a finitely generated k-algebra and let I be an ideal of $R \otimes_k A$ which is defined over A. Then:*

1. *All the prime divisors of I are defined over A.*

2. *Assume that a real prime ideal $p \in \operatorname{Spec} R \otimes_k A$ containing I satisfies*

$$Z(I) \cap W = Z(p) \cap W \quad \text{in } \operatorname{Spec}_r (R \otimes_k A)_p \tag{3.10}$$

for some neighbourhood W of some α in $\operatorname{Spec}_r (R \otimes_k A)_p$ with $\operatorname{supp} \alpha = p$. Then p is defined over A.

PROOF. W.l.o.g. we may assume $I = 0$.

1. The canonical morphism $A \to R \otimes_k A$ is flat, so by Matsumura [15, p. 179, Thm. 23.2]

$$\operatorname{Ass}_{R \otimes_k A}(R \otimes_k A) = \bigcup_{p' \in \operatorname{Ass}_A(A)} \operatorname{Ass}_{R \otimes_k A}((R \otimes_k A)/(R \otimes_k p')). \tag{3.11}$$

On the other hand the extension $R \otimes_k p'$ of any prime ideal $p' \in \operatorname{Spec} A$ with respect to the canonical morphism $A \to R \otimes_k A$ is again prime; namely by Jacobson [8, p. 550, Thm. 8.51] the tensor product $R \otimes_k (A/p')$ is an integral domain since the field extension $k \to R$ is assumed to be regular. Therefore by (3.11) $\operatorname{Ass}_{R \otimes_k A}(R \otimes_k A) = \{R \otimes_k p' : p' \in \operatorname{Ass}_A(A)\}$ and the assertion follows.

2. We proceed by induction on the height of p. If $\operatorname{ht} p = 0$, then the assertion follows from the first part of this lemma. So let us assume $\operatorname{ht} p > 0$. We can replace A by A/p' where $R \otimes_k p'$ is a minimal prime ideal contained in p, hence we may assume w.l.o.g. that A is an integral domain.

If the prime ideal p were regular, then α had a generization β with support zero. (This follows e.g. from the fact that the completion of the regular local ring $(R \otimes_k A)_p$ is a power series ring over the residue field $\kappa(p)$ (cf. Zariski-Samuel[19, p. 307, § 12, Cor.]).) On the other hand our assumption (3.10) reads as $W \subseteq Z(p)$ which would imply $p = 0$, contradicting our assumptions.

Therefore p is a singular prime ideal and by the Jacobian criterion (cf. Matsumura [15, p. 216, Lemma 1; p. 233, Thm. 30.3] or Kunz [12, p. 176, Satz 1.15]) there is a nonzero $f \in A$ with $1 \otimes_k f \in p$. We apply now the induction hypothesis to the k-algebra $A/(f)$ and to the prime ideal $p \bmod f(R \otimes_k A)$ of $R \otimes_k (A/(f))$. □

PROOF. (of Theorem 3.1) 1. Let $c \in \{c_+, c_*\}$. By the definition of the real verification complexity there is a finite subset $F = \{f_1, \ldots, f_t\} \subseteq (R \otimes_k A)_p$ such that

$$VC_{r,k\to(R\otimes_k A)_p}(c, \zeta a, \alpha) = L_{k\to(R\otimes_k A)_p}(c, \zeta a, F) \tag{3.12}$$

and

$$Z(F) \cap W = Z(p) \cap W \text{ in } \mathrm{Spec}_r\,(R \otimes_k A)_p$$

for some neighbourhood W of α in $\mathrm{Spec}_r\,(R \otimes_k A)_p$. Theorem 3.2 says that there is a subset $\mathcal{U} = \{u_0, \ldots, u_t\} \subseteq R \otimes_k A$ with $u_0 \notin p$ such that for $1 \le i \le t$

$$Rf_i = Ru_i/u_0,\ \mathrm{tr.deg}_k \mathrm{coeff}_{R/k}(\mathcal{U}) \le L_{k\to(R\otimes_k A)_p}(c_+, \zeta a, F), \tag{3.13}$$

respectively

$$f_i + R = u_i/u_0 + R,\ \mathrm{tr.deg}_k \mathrm{coeff}_{R/k}(\mathcal{U}) \le 2L_{k\to(R\otimes_k A)_p}(c_*, \zeta a, F). \tag{3.14}$$

We first settle the case $c = c_+$. Let K denote the algebraic closure of $\mathrm{coeff}_{R/k}(\mathcal{U})$ in R. We apply Lemma 3.3 to the field extension $K \to R$, the K-algebra $K \otimes_k A$ and to the ideal $(u_1, \ldots, u_t)R \otimes_k A$, which is defined over $K \otimes_k A$, and conclude that p is also defined over $K \otimes_k A$. Therefore

$$\mathrm{tr.deg}_k \mathrm{def}_{R/k}(p) \le \mathrm{tr.deg}_k K = \mathrm{tr.deg}_k \mathrm{coeff}_{R/k}(\mathcal{U})$$

and (3.6) follows with (3.12) and (3.13).

Assume now $c = c_*$ and let $\mu_i \in R$ such that $f_i = u_i/u_0 + \mu_i$. If $q \in \mathrm{Spec}\, R \otimes_k A$ is a minimal prime divisor of $(\mu_1 u_0 + u_1, \ldots, \mu_t u_0 + u_t)$ which is contained in p, then

$$Z(q) \cap W = Z(p) \cap W \text{ in } \mathrm{Spec}_r\,(R \otimes_k A)_p. \tag{3.15}$$

k is infinite since $\mathrm{char} k = 0$, so by Kronecker's trick (cf. Matsumura [15, p. 112, Thm. 14.14]) there is a matrix $\lambda \in k^{\mathrm{ht}\, q \times t}$ such that q is minimal prime divisor of the ideal

$$(\sum_{j=1}^{t} \lambda_{ij}(\mu_j u_0 + u_j) :\ 1 \le i \le \mathrm{ht}\, q).$$

Let K denote the algebraic closure in R of the subfield obtained from $\mathrm{coeff}_{R/k}(\mathcal{U})$ by adjoining $\{\sum_{j=1}^{t} \lambda_{ij}\mu_j : 1 \le i \le \mathrm{ht}\, q\}$. Lemma 3.3 implies that q is defined over $K \otimes_k A$, hence by (3.15) and the same lemma also the ideal p is defined over $K \otimes_k A$. Therefore

$$\begin{aligned} \mathrm{tr.deg}_k \mathrm{def}_{R/k}(p) &\le \mathrm{tr.deg}_k K \le \mathrm{tr.deg}_k \mathrm{coeff}_{R/k}(\mathcal{U}) + \mathrm{ht}\, q \\ &\le 2L_{k\to(R\otimes_k A)_p}(c_*, \zeta a, F) + \mathrm{ht}\, p \end{aligned} \tag{3.16}$$

and (3.7) is proved.

Statement (3.8) can be shown as (3.6), and for infinite k statement (3.9) can be proved as (3.7). We will show now (3.9) for finite k by a reduction to the case of an infinite ground field k.

So assume k being finite, let t be transcendental over R and denote by R' the perfect closure of $R(t)$. We show first that the extension p' of p with respect to the canonical ring morphism $\varphi : R \otimes_k A \to R' \otimes_k A$ is prime. Namely, we have

$$R' \otimes_{R(t)} [R(t) \otimes_R ((R \otimes_k A)/p)] = (R' \otimes_k A)/p'.$$

Since $R \to (R \otimes_k A)/p$ is separable and $R \to R(t)$ is purely transcendental, $E := R(t) \otimes_R ((R \otimes_k A)/p)$ is an integral domain which is separable over $R(t)$; moreover, $R(t) \to R'$ is purely inseparable which implies that also $R' \otimes_{R(t)} E$ is an integral domain, hence p' is prime (cf. Jacobson [8, p. 545, Thm. 8.46, Thm. 8.47]). Since φ is flat we have $\operatorname{ht} p' = \operatorname{ht} p$ (cf. [15, p. 116, Thm. 15.1]). Moreover

$$\operatorname{def}_{R'/k(t)}(p') = k(t)\operatorname{def}_{R'/k}(p') = k(t)\operatorname{def}_{R/k}(p),$$

thus $\operatorname{tr.deg}_{k(t)}\operatorname{def}_{R'/k(t)}(p') = \operatorname{tr.deg}_k \operatorname{def}_{R/k}(p)$. Now, by taking into account

$$VC_{k \to (R \otimes_k A)_p}(c_*, \zeta a, p(R \otimes_k A)_p) \geq VC_{k(t) \to (R' \otimes_k A)_{p'}}(c_*, \zeta a, p'(R' \otimes_k A)_{p'}),$$

we obtain statement (3.9) for the k-algebra A and $p \in \operatorname{Spec} R \otimes_k A$ from the corresponding statement for the $k(t)$-algebra $k(t) \otimes_k A$ and $p' \in \operatorname{Spec} R' \otimes_{k(t)} (k(t) \otimes_k A)$. □

Let us summarize the consequences of the above theorem for R-preconditioned decision complexity.

COROLLARY 3.4. *Let R be an algebraically or real closed field, $X \subset Y \subseteq R^m$ algebraic subsets and X irreducible. Moreover, let k be a subfield of R over which the vanishing ideal $I(Y)$ of Y is defined. Then:*

1. *For real closed R and an open semi-algebraic subset $U \subseteq R^m$ satisfying $\operatorname{Reg}(X) \cap U \neq \emptyset$ we have*

$$C_R(c_{+,\leq}, \{X \cap U, (Y \setminus X) \cap U\}) \geq \operatorname{tr.deg}_k \operatorname{def}_{R/k}(I(X)), \quad (3.17)$$

$$C_R(c_{*,\leq}, \{X \cap U, (Y \setminus X) \cap U\}) \geq \tfrac{1}{2}(\operatorname{tr.deg}_k \operatorname{def}_{R/k}(I(X)) + 1), \quad (3.18)$$

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

2. *For algebraically closed R and a Zariski-open subset $U \subseteq R^m$ we have*

$$C_R(c_{+,=}, \{X \cap U, (Y \setminus X) \cap U\}) \geq \mathrm{tr.deg}_k \mathrm{def}_{R/k}(I(X)), \quad (3.19)$$

$$C_R(c_{*,=}, \{X \cap U, (Y \setminus X) \cap U\}) \geq \tfrac{1}{2}(\mathrm{tr.deg}_k \mathrm{def}_{R/k}(I(X)) + \max_{Y' \in \mathcal{Y}} \mathrm{codim}_{Y'} X), \quad (3.20)$$

where $\mathcal{Y}$ denotes the set of irreducible components of Y containing X and $c_{+,=} := 1_{\{+,-,=\}}$, $c_{*,=} := 1_{\{*,/,=\}}$.

PROOF. Define $A := k[x]/(I(Y) \cap k[x])$ and denote by p the image of $I(X)$ under the canonical morphism $R[x] \to R[x]/I(Y) = R \otimes_k A$. Then $\mathrm{def}_{R/k}(p) = \mathrm{def}_{R/k}(I(X))$ and $\mathcal{O}_{X,Y} = (R \otimes_k A)_p$.

1. We first show statement (3.17). Let $\alpha \in \tilde{U} \cap \mathrm{Spec}_r \mathcal{O}_{X,Y}$ with $\mathrm{supp}\, \alpha = I(X)$ (such a prime cone exists by [4, p. 133, Prop. 7.6.1]). Furthermore let T be an $(\Omega^k, \{=, \leq\})$-decision tree over m deciding membership in $X \cap U$ relative to $Y \cap U$. Then by [5, Prop. 11, Rem. 12] we have

$$L(c_{+,\leq}, T_\alpha) \geq VC_{r,k \to \mathcal{O}_{X,Y}}(c_+, x', \alpha)$$

where $x' = (x'_i)$, x'_i denoting the coordinate functions on Y; moreover there is an open semi-algebraic subset $U_1 \subseteq U$ with $\alpha \in \tilde{U}_1$ and such that $T_\xi = T_\alpha$ for all $\xi \in U_1$. This implies

$$C(c_{+,\leq}, \{X \cap U, (Y \setminus X) \cap U\}) \geq L(c_{+,\leq}, T_\alpha) \geq VC_{r,k \to \mathcal{O}_{X,Y}}(c_+, x', \alpha). \quad (3.21)$$

For this we did not use that $I(Y)$ is defined over k. Applying (3.21) to the algebraic subsets $\{\zeta\} \times X \subset \{\zeta\} \times Y \subseteq R^{s+m}$ ($\zeta \in R^s$), the open semi-algebraic subset $R^s \times U$ and to the prime cone determined by α via the canonical isomorphism

$$\mathcal{O}_{\{\zeta\} \times X, \{\zeta\} \times Y} \simeq \mathcal{O}_{X,Y}$$

we obtain immediately from the definition of R-preconditioned decision complexity that

$$C_R(c_{+,\leq}, \{X \cap U, (Y \setminus X) \cap U\}) \geq \min_{s \in \mathbf{N}} \min_{\zeta \in R^s} VC_{r,k \to \mathcal{O}_{X,Y}}(c_+, \zeta x', \alpha). \quad (3.22)$$

Theorem 3.1 yields now the asserted bound (3.17).

We turn to the proof of (3.18). Let $\zeta \in R^s$, $\alpha \in \widetilde{R^s \times U} \cap \mathrm{Spec}_r \mathcal{O}_{\{\zeta\} \times X, \{\zeta\} \times Y}$ with $\mathrm{supp}\, \alpha = I(\{\zeta\} \times X)$, and let T be an $(\Omega^k, \{=, \leq\})$-decision tree over $s+m$ deciding membership in $\{\zeta\} \times (X \cap U)$ relative to $\{\zeta\} \times (Y \cap U)$. As before we have

$$C(c_{*,\leq}, \{\{\zeta\} \times (X \cap U), \{\zeta\} \times ((Y \setminus X) \cap U)\}) \geq L(c_{*,\leq}, T_\alpha).$$

The proof of Prop. 11 in [5] shows that there exists $F \subseteq \mathcal{O}_{X,Y} \simeq \mathcal{O}_{\{\zeta\}\times X,\{\zeta\}\times Y}$ such that

$$L(c_*, T_\alpha) \geq L_{k\to\mathcal{O}_{X,Y}}(c_*, \zeta x', F), \qquad L(1_{\{=,\leq\}}, T_\alpha) \geq |F|$$

and

$$Z(F) \cap W = Z(p) \cap W \text{ in } \mathrm{Spec}_r\, \mathcal{O}_{X,Y}$$

for some neighbourhood W of α in $\mathrm{Spec}_r\, \mathcal{O}_{X,Y}$. Similarly as in the proof of Theorem 3.1, (3.16) we get that (for this estimate we do not need Kronecker's trick)

$$\mathrm{tr.deg}_k \mathrm{def}_{R/k}(p) \leq 2L_{k\to\mathcal{O}_{X,Y}}(c_*, \zeta x', F) + |F|. \tag{3.23}$$

Observing that $L(1_{\{=,\leq\}}, T_\alpha) \geq 1$ we conclude

$$\mathrm{tr.deg}_k \mathrm{def}_{R/k}(p) < 2L(c_*, T_\alpha) + 2L(1_{\{=,\leq\}}, T_\alpha) = 2L(c_{*,\leq}, T_\alpha) \tag{3.24}$$

and assertion (3.18) follows.

2. The statements (3.19), (3.20) can be demonstrated similarly as (3.17), (3.18). For the proof of (3.20) note that the condition

$$Z(F) \cap W = Z(p) \cap W \text{ in } \mathrm{Spec}\,(R \otimes_k A)_p$$

for a subset $F \subseteq R \otimes_k A$ means that p is a minimal prime divisor of the ideal (F), hence by Krull's principal ideal theorem (cf. [15, p. 100, Thm. 13.5]) $\mathrm{ht}\, p \leq |F|$. Instead of (3.24) we therefore get from (3.23) the estimate

$$\mathrm{tr.deg}_k \mathrm{def}_{R/k}(p) + \mathrm{ht}\, p \leq 2L(c_{*,=}, T_\alpha).$$

Moreover, it is clear that $\mathrm{ht}\, p = \max_{Y'} \mathrm{codim}_{Y'} X$ where Y' varies over all the irreducible components of Y containing X. □

In the following sections we will give examples $\{X, Y \setminus X\}$ where Corollary 3.4 leads to sharp lower bounds.

4. Generic complete intersections

Let $k \to R$ be a field extension, $A := R[x_1, \ldots, x_m]$ and

$$S := R[x_0, x_1, \ldots, x_m] = \bigoplus_{\ell\in\mathbb{N}} S^{(\ell)}$$

be the standard N-graduation. Let $f_1, \ldots, f_r \in A$ (resp. $\in S$) be (homogeneous) polynomials of degrees $d_1, \ldots, d_r$. We call $(d_1, \ldots, d_r)$ the *degree format*

of the sequence $f_1, \ldots, f_r$; this sequence is called *k-generic of degree format* $(d_1, \ldots, d_r)$ if

$$\mathrm{tr.deg}_k \mathrm{coeff}_{R/k}(\{f_1, \ldots, f_r\}) = \sum_{i=1}^{r} \binom{d_i + m}{m}.$$

Let R be an algebraically closed or real closed field, $X \subset R^m$ an irreducible algebraic subset, $r := \mathrm{codim}_{R^m} X < m$. We call X a *k-generic complete intersection of polynomials of degrees* $d_1, \ldots, d_r$ if $X = Z(f_1, \ldots, f_r)$ for some k-generic $f_1, \ldots, f_r \in A$ of degree format $(d_1, \ldots, d_r)$.

In order to find the transcendence degree $\mathrm{tr.deg}_k \mathrm{def}_{R/k}(I(X))$ of the vanishing ideal $I(X) \subseteq A$ we will work in the homogeneous setting and recall therefore first some facts to be used later. For $f \in A$

$$^h f := x_0^{\deg f} f(x_1/x_0, \ldots, x_m/x_0) \qquad (^h 0 := 0)$$

is called the *homogenization* of f; for homogeneous $f \in S$

$$^a f := f(1, x_1, \ldots, x_m)$$

is called the *dehomogenization* of f. For ideals I in A, $^h I \subseteq S$ denotes the homogeneous ideal generated by all $^h f$, $f \in I$. Conversely, $^a J \subseteq A$ denotes the image of a homogeneous ideal J in S under dehomogenization. One has a 1-1 correspondence between ideals I in A and homogeneous ideals J in S having the property that x_0 is no zero-divisor of S/J. We remark that

$$\mathrm{def}_{R/k}(I) = \mathrm{def}_{R/k}(^h I). \tag{4.25}$$

The *Hilbert function* of a homogeneous ideal J in S is defined as

$$H(J; \cdot) : \mathrm{N} \to \mathrm{N}, \quad H(J, \ell) = \dim_R (S/J)^{(\ell)}.$$

(Here and in the sequel we use the notation $M^{(\ell)} := M \cap B^{(\ell)}$ for any subset M of some N-graded $B = \bigoplus_{\mathrm{N}} B^{(\ell)}$.) Consider for $r \leq m$ and $d_1, \ldots, d_r \in \mathrm{N}$ the R-subspaces

$$S(d_1, \ldots, d_r) := \{g \in S : \deg_{x_1} g < d_1, \ldots, \deg_{x_r} g < d_r\}$$

of S. It is clear that $H((x_1^{d_1}, \ldots, x_r^{d_r}); \ell) = \dim_R S(d_1, \ldots, d_r)^{(\ell)}$.

Let $f_1, \ldots, f_r \in S$ be a regular sequence of homogeneous polynomials of degree format $(d_1, \ldots, d_r)$ and put $S_j := S/(f_1, \ldots, f_j)$. Then we have the canonical exact sequence of graded S-modules

$$0 \to S_{j-1} \xrightarrow{\cdot f_j} S_{j-1} \to S_j \to 0,$$

and by considering homogeneous parts we get for all $j \geq 1, \ell \in \mathrm{Z}$

$$\dim_R S_j^{(\ell)} = \dim_R S_{j-1}^{(\ell)} - \dim_R S_{j-1}^{(\ell-d_j)}.$$

Hence the Hilbert function of $(f_1, \ldots, f_j)$ is completely determined by the Hilbert function of $(f_1, \ldots, f_{j-1})$ and the number d_j. Therefore $H((f_1, \ldots, f_r); \cdot)$ depends only on the degree format $(d_1, \ldots, d_r)$ and we conclude by considering the regular sequence $x_1^{d_1}, \ldots, x_r^{d_r}$ that

$$\forall \ell \in \mathrm{N} \quad H((f_1, \ldots, f_r); \ell) = \dim_R S(d_1, \ldots, d_r)^{(\ell)}. \tag{4.26}$$

Assume $f_1, \ldots, f_r \in S$ being k-generic of degree format $(d_1, \ldots, d_r)$. Then this sequence is regular, and we have for all $s \leq r$ the direct sum decomposition

$$(f_1, \ldots, f_s, x_{s+1}^{d_{s+1}}, \ldots, x_r^{d_r})^{(\ell)} \oplus S(d_1, \ldots, d_r)^{(\ell)} = S^{(\ell)}. \tag{4.27}$$

(Proof: The condition that $S^{(\ell)}$ is the sum of the above subspaces can be expressed by the nonvanishing of certain polynomials over Z on the coefficients of $f_1, \ldots, f_s$ (determinantal criterion). It is therefore sufficient to verify the condition for some specific $f_1, \ldots, f_r$. However $f_i = x_i^{d_i}$ do the job. The above sum decomposition is direct because of (4.26).) If $r < m$, then $(f_1, \ldots, f_r)$ is a homogeneous prime ideal in S of height r and ${}^a(f_1, \ldots, f_r)$ is a prime ideal in A of the same height. (This follows from Bertini's Theorem, cf. Lang [13, p. 211–216, Thm. 7, Prop. 12] or Jouanolou [9, p. 66, Thm. 6.3].) Note that if R is real closed, then ${}^a(f_1, \ldots, f_r)$ is a real prime ideal if and only if its zeroset has codimension r in R^m.

LEMMA 4.1. *If $f_1, \ldots, f_r \in S$ is k-generic of format $(d_1, \ldots, d_r)$, $r < m$, $p = (f_1, \ldots, f_r)S$, then*

$$\begin{aligned}
\mathrm{tr.deg}_k \mathrm{def}_{R/k}({}^a p) &= \mathrm{tr.deg}_k \mathrm{def}_{R/k}(p) = \sum_{i=1}^{r} H(p; d_i) \\
&= \sum_{i=1}^{r} \dim_R S(d_1, \ldots, d_r)^{(d_i)} \\
&\geq \sum_{i=1}^{r} \left[\binom{d_i + m}{m} - \sum_{j: d_j \leq d_i} \binom{d_i - d_j + m}{m} \right],
\end{aligned}$$

the latter being an equality if $\max d_i < 2 \min d_i$. *Moreover,* $p = (f_1', \ldots, f_r')S$ *for some* $f_i' \in x_i^{d_i} + S(d_1, \ldots, d_r)^{(d_i)}$.

PROOF. The lower bound estimate for $\sum_{i=1}^r \dim_R S(d_1,\ldots,d_r)^{(d_i)}$ is obvious. By (4.25) and (4.26) it is sufficient to prove the middle equality $\mathrm{tr.deg}_k \mathrm{def}_{R/k}(p) = \sum_i H(p;d_i)$.

Let $(f_{ij})_j$ be a vector space basis of $p^{(d_i)} \cap \mathrm{def}_{R/k}(p)[y_0,\ldots,y_m]$ and write

$$f_i = \sum_{j=1}^{\dim_R p^{(d_i)}} \lambda_{ij} f_{ij} \qquad (\lambda_{ij} \in R).$$

Hence $\mathrm{coeff}_{R/k}(\{f_1,\ldots,f_r\})$ lies in the compositum of the subfields $\mathrm{def}_{R/k}(p)$ and $k(\lambda_{ij} : 1 \le i \le r, 1 \le j \le \dim_R p^{(d_i)})$ of R. Therefore, by taking trancendence degrees

$$\sum_{i=1}^r \binom{d_i+m}{m} \le \mathrm{tr.deg}_k \mathrm{def}_{R/k}(p) + \sum_{i=1}^r \dim_R p^{(d_i)},$$

which is equivalent to

$$\sum_{i=1}^r H(p;d_i) \le \mathrm{tr.deg}_k \mathrm{def}_{R/k}(p).$$

For the reverse inequality we remark that the above mentioned direct sum decompositions (4.27) of $S^{(d_i)}$ allow to find a basis $f_1',\ldots,f_r'$ of p with the property that for $i = 1,\ldots,r$

$$f_i' \in x_i^{d_i} + S(d_1,\ldots,d_r)^{(d_i)},$$
$$(f_j : d_j \le d_i)S = (f_j' : d_j \le d_i)S. \qquad \square$$

THEOREM 4.2. *Let R be a real closed field, $r < m$. If $X \subset R^m$ is a k-generic complete intersection of polynomials in $A = R[x_1,\ldots,x_m]$ of degrees $d_1,\ldots,d_r$, then*

$$C_R(c_{+,\le}, \{X, R^m \setminus X\}) = \sum_{i=1}^r \dim_R S(d_1,\ldots,d_r)^{(d_i)},$$
$$C_R(c_{*,\le}, \{X, R^m \setminus X\}) \ge \frac{1}{2}\sum_{i=1}^r \dim_R S(d_1,\ldots,d_r)^{(d_i)}.$$

For $\max_i d_i \to \infty$

$$C_R(c_{*,\le}, \{X, R^m \setminus X\}) \sim \frac{1}{2}\sum_{i=1}^r \dim_R S(d_1,\ldots,d_r)^{(d_i)},$$
$$C_R(1_{\Omega^k \sqcup P}, \{X, R^m \setminus X\}) \sim \frac{3}{2}\sum_{i=1}^r \dim_R S(d_1,\ldots,d_r)^{(d_i)}.$$

(Analogously for algebraically closed fields R and $c_{+,=}$, resp. $c_{*,=}$.)

PROOF. The lower bounds follow from Corollary 3.4 and Lemma 4.1. For the upper bounds define for $e = (e_1, \ldots, e_m) \in \mathrm{N}^m$ and a cost function $c : \Omega^k \to \mathrm{N}$

$$\mathrm{Max}_{R/k}(c; e; \ell) := \max_{f \in {}^aS(e)^{(\ell)}} \min_{s \in \mathrm{N}} \min_{\zeta \in R^s} L_{k \to A}(c, \zeta x, f)$$

(here ${}^aS(e)^{(\ell)} := \{{}^af : f \in S(e)^{(\ell)}\}$). By Lemma 4.1 it is sufficient to show that

$$\mathrm{Max}_{R/k}(c_+; e; \ell) < \dim_R S(e)^{(\ell)},$$

which is clear, and that

$$\mathrm{Max}_{R/k}(c_*; e; \ell) \leq \frac{1}{2}\dim_R S(e)^{(\ell)} + (m+1)\frac{e_1 \cdots e_m}{\max_i e_i}, \tag{4.28}$$

$$\mathrm{Max}_{R/k}(1_{\Omega^k}; e; \ell) \leq \frac{3}{2}\dim_R S(e)^{(\ell)} + 3m\frac{e_1 \cdots e_m}{\max_i e_i}. \tag{4.29}$$

(Choose $e = (d_1, \ldots, d_r, \max d_i + 1, \ldots, \max d_i + 1) \in \mathrm{N}^m$ and use the rough estimate

$$\dim_R S(e)^{(\ell)} \geq m^{-m} e_1 \cdots e_m \qquad (\ell \geq \max e_i - 1)$$

in order to show that the relative error tends to zero.) We prove (4.28) by induction on m. W.l.o.g. we may assume $e_1 \geq e_2 \geq \ldots \geq e_m$. The start "$m = 1$" is covered by Eve [7] (see also Knuth [11, p. 474]). Since

$${}^aS(e_1, \ldots, e_m)^{(\ell)} = \bigoplus_{j=0}^{e_m - 1} ({}^aS(e_1, \ldots, e_{m-1})^{(\ell-j)} \cap R[x_1, \ldots, x_{m-1}])x_m^j,$$

we get with Horner's rule and the induction hypothesis

$$\begin{aligned}
&\mathrm{Max}_{R/k}(c_*; e_1, \ldots, e_m; \ell) \\
&\leq \sum_{j=0}^{e_m - 1} [\frac{1}{2}\dim_R(S(e_1, \ldots, e_{m-1})^{(\ell-j)} \cap R[x_1, \ldots, x_{m-1}]) \\
&\qquad + me_2 \cdots e_{m-1}] + e_m - 1 \\
&\leq \frac{1}{2}\dim_R S(e_1, \ldots, e_m)^{(\ell)} + (m+1)e_2 \cdots e_m.
\end{aligned}$$

Statement (4.29) can be proved similarly. □

5. Partial and continued fractions

In this section we apply Corollary 3.4 to test problems related to partial or continued fractions, thus extending some results by Strassen [18].

Let $k \to R$ be a field extension, R real closed (resp. algebraically closed), and let g/h be a rational function with $g, h \in R[x_1, \ldots, x_m]$ relatively prime and g irreducible. We will study the R-preconditioned decision complexity of the partition

$$\Pi_{g,h} := \{\{\xi \in R^m : g(\xi) = 0, h(\xi) \neq 0\}, \{\xi \in R^m : g(\xi) \neq 0, h(\xi) \neq 0\}\}.$$

Let us introduce the notation

$$f^+_\lambda := f(\lambda_1 x_1, \ldots, \lambda_m x_m), \; f^*_\lambda := f(x_1 + \lambda_1, \ldots, x_m + \lambda_m)$$

for $f \in R[x_1, \ldots, x_m]$ and $\lambda \in (R^\star)^m$. It is clear[B from the definition that

$$\begin{array}{rcl} C_R(c_{+,\leq}, \Pi_{g,h}) & = & C_R(c_{+,\leq}, \Pi_{g^+_\lambda, h^+_\lambda}), \\ C_R(c_{*,\leq}, \Pi_{g,h}) & = & C_R(c_{*,\leq}, \Pi_{g^*_\lambda, h^*_\lambda}) \end{array} \tag{5.30}$$

for all $\lambda \in (R^\star)^m$. From (3.5) and Corollary 3.4 we obtain

$$\begin{array}{rcl} C_R(c_{+,\leq}, \Pi_{g^+_\lambda, h^+_\lambda}) & \geq & \mathrm{tr.deg}_k \mathrm{coeff}_{R/k}(g^+_\lambda) - 1, \\ C_R(c_{*,\leq}, \Pi_{g^*_\lambda, h^*_\lambda}) & \geq & \frac{1}{2}\mathrm{tr.deg}_k \mathrm{coeff}_{R/k}(g^*_\lambda) \end{array} \tag{5.31}$$

under the condition that $gR[x]$ is real.

Let us now consider the (standard) partial fraction of length n

$$a_0 + \sum_{i=1}^{n} \frac{a_i}{x - b_i} \in R(a, b, x)$$

and its reduced numerator g_n and denominator h_n

$$g_n := a_0 \prod_{j=1}^{n}(x - b_j) + \sum_{i=1}^{n} a_i \prod_{j \neq i}(x - b_j).$$

$$h_n := \prod_{j=1}^{n}(x - b_j).$$

We denote the corresponding partition Π_{g_n, h_n} by PFR_n. The polynomial g_n, viewed as an element of $R(b, x)[a]$, is linear and has content one. Therefore

$g_n \in R[a,b,x]$ is irreducible. Moreover the ideal $g_n R[a,b,x]$ is real, since the field of fractions of $R[a,b,x]/(g_n)$ is isomorphic to the field of fractions of

$$R(a_1,\ldots,a_n,b_1,\ldots,b_n,x)[a_0]/(a_0+\sum_i a_i/(x-b_i))$$

which is is a rational function field over R.

Let $\lambda=(\alpha_0,\ldots,\alpha_n,\beta_1,\ldots,\beta_n,1)\in(R^\star)^{2n+1}$. Using

$$g_n = xg_{n-1}-b_ng_{n-1}+a_nh_{n-1}$$

and noting that g_{n-1},h_{n-1} do not depend on a_n,b_n, we easily see by induction on n that

$$\mathrm{coeff}_{R/k}((g_n)^+_\lambda)=\mathrm{coeff}_{R/k}((g_n)^*_\lambda)=k(\alpha_0,\ldots,\beta_n).$$

As we may assume w.l.o.g. $\mathrm{tr.deg}_k R > 2n$, this implies together with (5.30) and (5.31) the following

COROLLARY 5.1. *If R is real closed, then the partition PFR_n satisfies*

$$C_R(c_{+,\le},\mathrm{PFR}_n)=2n,\quad C_R(c_{*,\le},\mathrm{PFR}_n)=n+1.$$

(Analogously for algebraically closed R and $c_{+,=}$, resp. $c_{*,=}$.)

In the same way one can study the (standard) continued fraction in $R(a,b,x)$ of length n

$$b_n+\cfrac{a_{n-1}}{x+b_{n-1}+\cfrac{a_{n-2}}{x+b_{n-2}+\quad\ddots\quad+\cfrac{a_0}{x+b_0}}}. \tag{5.32}$$

In order to get a representation of this continued fraction as a quotient of two relatively prime polynomials we recursively define a sequence of polynomials $f_i\in R[a_0,\ldots,a_{i-1},b_0,\ldots,b_i,x]$ by setting $f_{-1}:=1$, $f_0:=x+b_0$ and for $i\ge 1$

$$f_i := (x+b_i)f_{i-1}+a_{i-1}f_{i-2}. \tag{5.33}$$

Let g_i be the polynomial obtained from f_i by substituting b_i-x for b_i and put $h_i:=f_0f_1\cdots f_{i-1}$. It is easy to see that g_n/f_{n-1} equals the continued fraction (5.32) and we denote the partition Π_{g_n,h_n} by CFR_n.

COROLLARY 5.2. *If R is real closed, then the partition CFR_n satisfies*

$$C_R(c_{+,\le},\mathrm{CFR}_n)=2n,\quad C_R(c_{*,\le},\mathrm{CFR}_n)=n+1.$$

(Analogously for algebraically closed R and $c_{+,=}$, resp. $c_{*,=}$.)

PROOF. The upper bounds are trivial. (Note that our assumption that h_{n-1} does not vanish on inputs guarantees that no denominator in the continued fraction (5.32) will vanish.)

For the lower bounds we may assume w.l.o.g. that $\mathrm{tr.deg}_k R > 2n$. From the recursion

$$f_i = b_i f_{i-1} + a_{i-1} f_{i-2} + x f_{i-1},$$

observing that f_{i-1}, f_{i-2} do not depend on a_{i-1}, b_i and taking into account $\deg f_i = i + 1$, one easily deduces by induction on i that

$$\mathrm{coeff}_{R/k}((f_i)^+_\lambda) = \mathrm{coeff}_{R/k}((f_i)^*_\lambda) = k(\alpha_0, \ldots, \beta_i)$$

for $\lambda = (\alpha_0, \ldots, \alpha_{i-1}, \beta_0, \ldots, \beta_i, 1) \in (R^*)^{2i+1}$. By induction on i one readily shows irreducibility of f_i; namely f_i, viewed as an element of

$$R[a_0, \ldots, a_{i-2}, b_0, \ldots, b_{i-1}, x][a_{i-1}, b_i],$$

is linear and its three coefficients $f_{i-1}, f_{i-2}, x f_{i-1}$ are relatively prime by the induction hypothesis. The field of fractions of $R[a, b, x]/(f_i)$ is isomorphic to a rational function field over R, the ideal (f_i) is therefore real. The asserted lower bounds follows now from (5.30) and (5.31). (The properties proved for f_i are also valid for g_i.) □

Acknowledgements

The author is grateful to Thomas Lickteig and Michael Shub for many interesting and stimulating discussions. Special thanks go to Thomas Lickteig for numerous critical comments which improved the presentation of the paper.

This work has been sponsored by the Schweizerischer Nationalfonds. Part of the research has been done while the author visited the Department of Mathematical Sciences at the T. J. Watson Research Center of IBM , New York. Their financial support is gratefully acknowledged.

References

[1] W. BAUR AND M. O. RABIN, Linear disjointness and algebraic complexity, in *"Logic and Algorithmic: An international Symp. held in honour of Ernst Specker"*, Monogr. No. 30 de l'Enseign. Math. (1982), 35–46.

[2] E. G. BELAGA, Evaluation of polynomials of one variable with preliminary processing of the coeficients, *Problemy Kibernetiki* **5** (1961), 7–15.

[3] M. Ben-Or, Lower bounds for algebraic computation trees, Proceedings 15th ACM STOC, Boston (1983), 80–86.

[4] J. Bochnak, M. Coste, and M.-F. Roy, *Géométrie algébrique réelle*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band 12, Springer Verlag, 1987.

[5] P. Bürgisser and T. Lickteig, Verification complexity of linear prime ideals, *J. Pure and Applied Algebra* **81** (1992), 247–267.

[6] P. Bürgisser, T. Lickteig, and M. Shub, Test complexity of generic polynomials, *J. of Complexity* **8** (1992), 203–215.

[7] J. Eve, The evaluation of polynomials, *Numerische Mathematik* **6** (1964), 17–21.

[8] N. Jacobson, *Basic Algebra II*, W. H. Freeman and Company, New York, 1989.

[9] J.-P. Jouanolou, *Théorèmes de Bertini et Applications*, Progress in Mathematics, Vol. 42, Birkhäuser, 1983.

[10] M. Knebusch, and C. Scheiderer, *Einführung in die reelle Algebra*, Vieweg-Studium 63: Aufbaukurs Mathematik (Vieweg, Braunschweig, 1989).

[11] D.E. Knuth, *The art of computer programming*, Vol. II: Seminumerical algorithms, Addison-Wesley, 2nd edition, 1980.

[12] E. Kunz, *Einführung in die kommutative Algebra und algebraische Geometrie*, Vieweg-Studium 46: Aufbaukurs Mathematik (Vieweg, Braunschweig, 1980).

[13] S. Lang, *Introduction to Algebraic Geometry*, Interscience Tracts in Pure and Applied Mathematics, Num. 5, Interscience Publishers, 1958.

[14] T. Lickteig, *On semialgebraic decision complexity*, Tech. Rep. TR-90-052 Int. Comp. Science Inst., Berkeley, 1990.

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

[16] T. S. Motzkin, Evaluation of polynomials, *Bull. Am. Soc.* **61** (1955), 163.

[17] E. M. Reingold and I. Stocks, Simple proofs for polynomial evaluation, in: *Complexity of Computer Computations*, R. Miller and J. Thatcher (Eds.), Plenum Press, 1972, 21–30.

[18] V. Strassen, Evaluation of rational functions, in: *Complexity of Computer Computations*, R. Miller and J. Thatcher (Eds.), Plenum Press, 1972, 1–10.

[19] O. Zariski and P. Samuel, *Commutative algebra*, Vol. II, Van Nostrand, Princeton, 1958, 1960.

Peter Bürgisser
Institut für Informatik V
Universität Bonn
Römerstr. 164
D-5300 Bonn
Germany
buerg@cs.bonn.edu