Verification Complexity
of Linear Prime Ideals\(^1\)

Peter Bürgisser
Thomas Lickteig

TR-91-039
July 12, 1991

\(^1\)Submitted to *J. of Pure and Applied Algebra.*
Verification complexity of linear prime ideals

Peter Bürgisser* Thomas Lickteig†

Abstract

The topic of this paper is the complexity of algebraic decision trees deciding membership in an algebraic subset $X \subseteq \mathbb{R}^n$ where $\mathbb{R}$ is a real or algebraically closed field. We define a notion of verification complexity of a (real) prime ideal (in a prime cone) which gives a lower bound on the decision complexity. We exactly determine the verification complexity of some prime ideals of linear type generalizing a result by Winograd [Win 70]. As an application we show uniform optimality with respect to the number of multiplications and divisions needed for two algorithms:

- For deciding whether a number is a zero of several polynomials -- if this number and the coefficients of these polynomials are given as input data -- evaluation of each polynomial with Horner's rule and then testing the values for zero is optimal.
- For verifying that a vector satisfies a system of linear equations -- given the vector and the coefficients of the system as input data -- the natural algorithm is optimal.

Key words: Algebraic decision trees, optimality of Horner's rule, Ostrowski complexity, real spectrum, straight line programs.
AMS(MOS) subject classifications: 68C20, 68C25, 14P10.

1 Introduction

The history of algebraic complexity theory begins with a paper by Ostrowski [Ost 54] where he raised the unorthodox question whether Horner's rule for the evaluation of a polynomial $\sum_{j=0}^{d} a_j x^j$ is optimal. He conjectured that there is no general procedure performing this task working with less than $d$ multiplications and divisions. Later Pan [Pan 66] succeeded in proving this conjecture. His proof technique, the so called substitution method, has been developed further by Winograd [Win 70], Strassen [Str 72] and Hartmann-Schuster

*International Computer Science Institute, 1947 Center Street, Suite 600, Berkeley, CA 94704. On leave from the University of Konstanz, Math. Fakultät, D-7750 Konstanz, Germany.
†International Computer Science Institute, 1947 Center Street, Suite 600, Berkeley, CA 94704. On leave from the University of Tübingen, Math. Institut, Auf der Morgenstelle 10, D-74 Tübingen, Germany.
who showed that the natural algorithms for various other computational problems are optimal. In particular the tasks of evaluating several polynomials $f_i$

$$f_i = \sum_{j=0}^{d} a_{ij} x^j \quad (i = 1, \ldots, n)$$

(1)

given $a_{10}, \ldots, a_{nd}, x$ and of computing the value of an affine mapping ($g_1, \ldots, g_n$)

$$g_i = \sum_{j=1}^{d} a_{ij} x_j + a_{i0} \quad (i = 1, \ldots, n)$$

(2)

given $a_{10}, \ldots, a_{nd}, x_1, \ldots, x_d$ require both $dn$ multiplications and divisions.

In this paper we investigate the question of whether the natural algorithms for the computation of the polynomials (1) or (2) are also optimal for testing them for zero, given an arbitrary input vector over some field $R$. If $(R, \leq)$ is an ordered field then we consider algorithms which perform tests for equality and $\leq$-comparisons, otherwise only equality tests are allowed. There are so few lower bounds known for the algorithmic problem of testing membership in an algebraic subset $X \subset R^m$. Strassen's degree bound [Str 83] for algebraically closed $R$ and Ben-Or's result [Ben 83] for real closed $R$ yield only weak lower bounds for the special membership problems

$$Z(f_1, \ldots, f_n) \subset R^{n(d+1)+1}, \quad Z(g_1, \ldots, g_n) \subset R^{n(d+1)+d}$$

we are considering here. In the case of only one equation the results in [Li 90] and [B-L-S 91] show in particular that $d/2$ multiplications and divisions are needed for the problems (3).

In this paper we will prove in both cases, $R$ real or algebraically closed, that any algebraic decision tree deciding membership in $Z := Z(f_1, \ldots, f_n)$ or $Z := Z(g_1, \ldots, g_n)$ requires at least $dn$ multiplications and divisions for any input in $Z$ outside a lower dimensional algebraic subset of $Z$.

The paper is organized as follows: Section 2 recalls some notions from real algebraic geometry. Sections 3, 4 introduce terminology based on these notions and contain definitions from algebraic complexity theory. In section 3 we give a definition of verification complexity of prime ideals (in a prime cone), and in section 4 we show that this notion gives lower bounds on decision complexity. Section 5 contains a lower bound result for verification complexity of prime ideals of a linear type which is applied in section 6 to the membership problems (3).

2 Some concepts from real algebraic geometry

We will discuss complexity questions over the reals in the framework of real algebraic geometry. In this section we recall the definition and some of the basic properties of the real spectrum of a commutative ring as it will be applied later on. For a detailed presentation of this theory we refer the reader to the books by Bochnak–Coste–Roy [B-C-R 87] and Knebusch–Scheiderer [K-S 89].

Let $A$ be a commutative ring.
- The real spectrum $\text{Sper} A$ of $A$ is the set of all pairs $\alpha := (p, \leq)$ where $p \in \text{Spec} A$ and $\leq$ is an ordering of the field $\kappa(p) := Fr(A/p)$ which we also denote by $\leq_\alpha$. One calls $p$ the support of $\alpha$ and writes $p = \text{supp}\alpha$.

- If $\alpha = (p, \leq_\alpha) \in \text{Sper} A$ and $f \in A$ we write $f(\alpha)$ instead of $\rho_p(f)$ where $\rho_p : A \to \kappa(p)$ denotes the canonical morphism. Statements like "$f(\alpha) \geq 0$" always refer to the ordering $\leq_\alpha$ of $\kappa(p)$.

- The Harrison-topology on $\text{Sper} A$ is the topology that has as a basis of open sets

$$\{\{\alpha \in \text{Sper} A : \forall f \in F \ f(\alpha) > 0\} : F \subset A \text{ finite}\}.$$  

$\text{Sper} A$ will always be considered as a topological space in this way.

- The elements of $\text{Sper} A$ can also be considered as certain subsets of $A$: A prime cone $P$ of $A$ is a subset $P \subset A$ satisfying the following conditions:

$$P + P \subset P, \quad PP \subset P, \quad P \cup (-P) = A,$$

$$\forall a, b \in A (a \notin P, b \notin P \Rightarrow -ab \notin P).$$

The map $\alpha = (p, \leq_\alpha) \mapsto \rho_p^{-1}(\{a \in \kappa(p) : 0 \leq_\alpha a\})$ defines a bijection from $\text{Sper} A$ onto the set of prime cones of $A$. (The inverse is given by $p = P \cap (-P), \quad 0 \leq_\alpha \rho_p(a)/\rho_p(b) \Leftrightarrow ab \in P$ for all $a, b \in A, b \notin p$.) We will go back and forth between these two interpretations of an element of $\text{Sper} A$.

- A morphism $\varphi : A \to B$ of commutative rings induces a continuous map

$$\text{Sper}\varphi : \text{Sper} B \to \text{Sper} A, \quad (\text{Sper}\varphi)(P) = \varphi^{-1}(P) \quad \text{for a prime cone } P \text{ of } A.$$ 

So $\text{Sper}$ can be considered as a functor from commutative rings to topological spaces.

- The map $\text{supp}_A : \text{Sper} A \to \text{Spec} A$ is continuous. For any morphism $\varphi : A \to B$ we have $\text{supp}_A \circ \text{Sper}\varphi = (\text{Spec}\varphi) \circ \text{supp}_B$ which means that $\text{supp}$ is a morphism $\text{Sper} \to \text{Spec}$ of functors. For a subset $F \subset A$

$$Z(F) := \{\alpha \in \text{Sper} A : \forall f \in F \ f(\alpha) = 0\}.$$ 

is called the zero set of $F$.

- An element of the Boolean subalgebra of $2^{\text{Sper} A}$ generated by the subsets

$$\{\alpha \in \text{Sper} A : f(\alpha) > 0\} \quad (f \in A)$$

is called a constructible subset of $\text{Sper} A$.

We recall the behaviour of $\text{Sper}$ when passing to a localisation or to a quotient:

- Let $S \subset A$ be a multiplicative subset and $i_S : A \to S^{-1}A$ the canonical morphism. Then $\text{Sper} i_S$ is a homeomorphism of $\text{Sper} S^{-1}A$ onto the subset $\{\alpha \in \text{Sper} A : S \cap \text{supp}\alpha = \emptyset\}$ of $\text{Sper} A$. 

3
Let $I \subset A$ be an ideal and $\pi : A \rightarrow A/I$ the canonical projection. Then $S\pi$ is a homeomorphism of $S\pi A/I$ onto the closed subspace $Z(I) = \{ \alpha \in S\pi A : I \subset suppa \}$.

Accordingly, we will sometimes tacitly consider $S\pi S^{-1}A$, $S\pi A/I$ as subsets of $S\pi A$.

Next we recall some facts about $S\pi A$ when $A$ is the coordinate ring of a real algebraic set. Let $R$ be a real closed field, $X \subset R^n$ an algebraic subset and $A(X)$ its coordinate ring. One can consider $X$ as a subset of $S\pi A(X)$ by identifying a point $\xi \in X$ with the prime cone $P_{\xi} := \{ f \in A(X) : f(\xi) \geq 0 \}$. $S\pi A(X)$ induces on $X$ the strong (Euclidean) topology and the semi-algebraic subsets of $X$ are exactly the traces in $X$ of the constructible subsets $M$ of $S\pi A(X)$. From the Artin-Lang Theorem (resp. Tarski principle) follows the crucial fact that no information gets lost when we pass from a constructible subset $M$ to $X \cap M$.

**Theorem 1** The map

$$\Phi : \{ \text{constructible subsets of } S\pi A(X) \} \rightarrow \{ \text{semialgebraic subsets of } X \}$$

$$M \mapsto X \cap M$$

is an isomorphism of Boolean algebras. $M$ is open (closed) if and only if $X \cap M$ is open (closed).

The inverse of the map $\Phi$ is called operation tilde, one writes $\tilde{Y} = \Phi^{-1}(Y)$ for $Y \subset X$ semi-algebraic ([B–C–R 87, p. 119]).

We will need the following proposition:

**Proposition 2** Let $R$ be a real closed field, $X \subset R^n$ an irreducible algebraic subset and $U$ a semi-algebraic, open subset of $X$. Then the following conditions are equivalent:

1. $U$ is Zariski-dense in $X$,
2. $\exists \alpha \in S\pi A(X) suppa = 0, \alpha \in \tilde{U}$,
3. $U \cap Reg(X) \neq \emptyset$.

**Proof:** $(1) \Rightarrow (3)$ is trivial. $(2) \Rightarrow (1)$ follows from Theorem 1. For the implication $(3) \Rightarrow (2)$ see [B–C–R 87, p. 133, Prop. 7.6.1].

The next lemma will be used in section 5.

**Lemma 3** Let $K$ be a real field and $A$ be a localisation of the polynomial ring $K[y_1, \ldots, y_m]$. Then any nonempty open subset of $S\pi A$ contains a prime cone with support 0. (This is equivalent to saying that $S\pi Fr(A)$ is dense in $S\pi A$.)

**Proof:** W.l.o.g. we may assume that $A = K[y_1, \ldots, y_m]$. If $K$ is real closed the statement follows immediately from Theorem 1 and Proposition 2. Let now $K$ be an arbitrary real field. Assume $W$ being an open subset of $S\pi K[y_1, \ldots, y_m]$ and $\alpha \in W$. The prime cone $\alpha$ induces an ordering of $K$; let $\varphi : K \rightarrow R$ be the corresponding real closure. The morphism $\varphi$ extends to $\varphi : K[y_1, \ldots, y_m] \rightarrow R[y_1, \ldots, y_m]$. We put $W_1 := (S\pi \varphi)^{-1}(W)$ which is easily seen to be a nonempty open subset of $S\pi R[y_1, \ldots, y_m]$. There is a $\beta_1 \in W_1$ satisfying $supp\beta_1 = 0$, hence $\beta := (S\pi \varphi)(\beta_1) \in W$ and $supp\beta = 0$. 

\[ \Box \]
3 Verification complexity

We briefly introduce some terminology following the presentations in [Str 73, Str 83] and [Li 90]. Throughout the following $k$ denotes a field and all $k$-algebras are assumed to be commutative.

We put $\Omega^k := k \cup \{0, 1, +, -, *, /\}$. In every $k$-algebra $A$ an element $\omega \in \Omega^k$ has an obvious interpretation as a partial mapping $\omega_A : A^{\sigma(\omega)} \supset \omega \cdot A \to A$. (Especially $\lambda \in k$ stands for the scalar multiplication with $\lambda$; 0, 1 are constants.) An $\Omega^k$-straight line program $\beta = (\beta_1, \ldots, \beta_r)$ over $n \in \mathbb{N}$ is a sequence of instructions

$$s_1 := \omega_1(s_{j_1,1}, \ldots, s_{j_1,\sigma(\omega_1)}),$$

$$\vdots$$

$$s_r := \omega_r(s_{j_r,1}, \ldots, s_{j_r,\sigma(\omega_r)})$$

where $s_{-n+1}, \ldots, s_r$ are program variables, $\omega_i \in \Omega^k$ and $-n < j_i, \sigma < i$ for all $i, \sigma$. An input for such a program $\beta$ is a pair $(A, x)$ where $A$ is a $k$-algebra and $x \in A^n$. We may assign to the variables $s_i$ the values $x_{n+i}$ ($i = -n + 1, \ldots, 0$) and successively execute the instructions of $\beta$ in the $k$-algebra $A$. If no division by a non-unit in $A$ occurs, the program $\beta$ is said to be executable on the input $(A, x)$ and yields a result sequence $(b_{-n+1}, \ldots, b_r) \in A^{n+l}$ which is given by the final values of the variables $s_i$. We say that a straight line program $\beta$ computes a finite subset $F \subseteq A$ on the input $(A, x)$ if $\beta$ is executable and $F$ is contained in the set of results $\{b_{-n+1}, \ldots, b_r\}$.

**Remark 4** Let $\beta$ be an $\Omega^k$-straight line program $\beta$ over $n$. There is a (unique) universal input $(A_\beta, x_\beta)$ for $\beta$, i.e. an input $(A_\beta, x_\beta)$ satisfying

1. $\beta$ is executable on $(A_\beta, x_\beta)$,
2. if $\beta$ is executable on an input $(A, x)$ then there is a unique $k$-algebra morphism $\varphi : A_\beta \to A$ such that $\varphi \circ x_\beta = x$.

Moreover $A_\beta$ is the localisation $k[X_1, \ldots, X_n]_d$ of the polynomial ring with respect to some element $d$ and $x_\beta = (X_1, \ldots, X_n)$.

The easy proof is left to the reader.

Now let a function $c : \Omega^k \to \mathbb{N}$ be given. ($c(\omega)$ is to be interpreted as the cost for performing the operation $\omega$.) The $c$-length of the straight line program $\beta$ (as above) is defined as $\sum_{i=1}^{r} c(\omega_i)$.

**Definition 5** Let $A$ be a $k$-algebra, $x \in A^n$, $F \subseteq A$ finite and $c : \Omega^k \to \mathbb{N}$ a function. The complexity $L_{k-A}(c, x, F)$ to compute $F$ from $x$ with respect to $c$ is defined as the minimum $c$-length of an $\Omega^k$-straight line program that computes $F$ on the input $(A, x)$. (Since the field $k$ will vary later we write in this notation the $k$-algebra $A$ in the form of its structural morphism.)

Observe that $L_{k-A}(c, x, F)$ is finite if and only if every element of $F$ can be written as a quotient of two elements of $k[x_1, \ldots, x_n] \subseteq A$.

The proof of the following remark is immediate.
Remark 6 Let $\varphi : A \to B$ be a morphism of $k$-algebras, $x \in A^n$ and $c : \Omega^k \to \mathbb{N}$ be a cost function. Then we have:

(a) For every finite subset $F \subset A$

$$L_{k \to B}(c, \varphi \circ x, \varphi(F)) \leq L_{k \to A}(c, x, F).$$

(b) Assume $\varphi^{-1}(B^*) = A^*$ and $\varphi$ surjective. Then there exists for every finite subset $G \subset B$ a finite subset $F \subset A$ such that $\varphi(F) = G$ and

$$L_{k \to B}(c, \varphi \circ x, G) = L_{k \to A}(c, x, F).$$

Note that the condition $\varphi^{-1}(B^*) = A^*$ is satisfied for local morphisms $\varphi : A \to B$ of local rings.

In [Li 90] the notion of verification complexity of prime ideals has been introduced in order to prove lower bounds on the decision complexity of problems solved by equality-branching decision trees. For including also $\leq$-comparisons we will need a real and local analogue of this notion.

Definition 7 Let $A$ be a $k$-algebra, $x \in A^n$, $c : \Omega^k \to \mathbb{N}$ and $p \in \text{Spec}A$.

(a) The verification complexity $VC_{k \to A}(c, x, p)$ of $p$ is defined as

$$VC_{k \to A}(c, x, p) := \min\{L_{k \to A}(c, x, F) : F \subset A \text{ finite}, Z(F) = Z(p)\}.$$  

(Here $Z(F) := \{q \in \text{Spec}A : \forall f \in F \ f(q) = 0\}$.)

(b) Assume $\alpha \in \text{Sper}A$ with $\text{supp}\alpha = p$. The real verification complexity $VC_{r, k \to A}(c, x, \alpha)$ of $p$ in $\alpha$ is defined as

$$VC_{r, k \to A}(c, x, \alpha) := \min\{L_{k \to A}(c, x, F) : F \subset A \text{ finite}, Z(F) \cap W = Z(p) \cap W \text{ for some neighbourhood } W \text{ of } \alpha \text{ in } \text{Sper}A\}.$$  

(It is easy to see that the map

$$S\text{perFr}(A/p) = \{\alpha \in \text{Sper}A : \text{supp}\alpha = p\} \to \mathbb{N},$$

$$\alpha \mapsto VC_{r, k \to A}(c, x, \alpha)$$

is upper semi-continuous. It would be interesting to know under which conditions it is continuous or constant.)

The next lemma follows easily from Remark 6 and tells us about the behaviour of the verification complexities with respect to quotients.

Lemma 8 Let $\varphi : A \to B$ be a surjective morphism of $k$-algebras, $x \in A^n$, $c : \Omega^k \to \mathbb{N}$. Then we have:
(a) For any \( q \in \text{Spec} B \)
\[
VC_{k-B}(c, \varphi \circ x, q) \leq VC_{k-A}(c, x, (\text{Spec}\varphi)(q)).
\]

(b) For any \( \beta \in \text{Sper} B \)
\[
VC_{r,k-B}(c, \varphi \circ x, \beta) \leq VC_{r,k-A}(c, x, (\text{Sper}\varphi)(\beta)).
\]

(c) If \( \varphi^{-1}(B^*) = A^* \) and \( \ker \varphi = \{l_1, \ldots, l_r\} \) for \( l_1, \ldots, l_r \in A \) such that \( L_{k-A}(c, x, \{l_1, \ldots, l_r\}) = 0 \) then in (8(a)) and (8(b)) equality holds.

4 Decision complexity and verification complexity

We recall the definition of a decision tree and introduce some notation. Let \( k \) denote a field, \( \Omega^k = k \cup \{0, 1, +, -, *, /\}, P = \{=\} \) or \( P = \{=, <\}. \)

Let \((V, \prec)\) be a binary tree, \( V = V_0 \cup V_1 \cup V_2 \) the partition of the set of its nodes into the set of leaves, simple and branching nodes. (\( a \prec b \) for \( a, b \in V \) means that \( a \) is a predecessor of \( b \).) Let \( n \in \mathbb{N} \) and \( s_v \) for \( v \in V_1 \cup \{1, \ldots, n\} \) denote variables. An \((\Omega^k, P)\)-decision tree \( T \) over \( n \) is a binary tree \((V, \prec)\) together with a (instruction) function that assigns

- to every \( v \in V_1 \) an operational instruction
  \[
s_v := \omega_v(s_{u_{v,1}}, \ldots, s_{u_{v,m_v}})
  \]
  where \( \omega_v \in \Omega^k \) \( m_v \)-ary, \( u_{v,i} \in \{1, \ldots, n\} \) or \( u_{v,i} \in V_1, u_{v,i} < v \) \( i = 1, \ldots, m_v \),

- to every \( v \in V_2 \) a test instruction
  \[
  \rho_v(s_{u_{v,1}}, s_{u_{v,2}})
  \]
  where \( \rho_v \in P, u_{v,i} \in \{1, \ldots, n\} \) or \( u_{v,i} \in V_1, u_{v,i} < v \) \( i = 1, 2 \),

- to every \( v \in V_0 \) a symbol
  \[
  \delta_v \in \{\text{yes}, \text{no}\}.
  \]

(As we will deal only with membership problems two symbols are sufficient.)

A path \( \pi \) in \( T \) is a path from the root to a node in the underlying binary tree \((V, \prec)\), which we denote by \( V(\pi) \), together with the restriction of the instruction function of \( T \) to \( V(\pi) \). Restriction of the instruction function of \( T \) to \( V(\pi) \cap V_1 \) defines an \( \Omega^k \)-straight line program over \( n \) which we will denote by \( \beta(\pi) \). If additionally a cost function \( c : \Omega^k \cup P \to \mathbb{N} \) is given, we will call
\[
L(c, \pi) := \sum_{v \in V(\pi) \cap V_1} c(\omega_v) + \sum_{v \in V(\pi) \cap V_2} c(\rho_v)
\]
the \( c \)-length of the path \( \pi \). The \( c \)-cost of the tree \( T \) is the maximum \( c \)-length of a path \( \pi \) in \( T \) from the root to a leaf.
An input for such a decision tree $T$ is a pair $(A, x)$ where $A$ is a $k$-algebra (together with an interpretation of $\leq$ if $P = \{-, \leq\}$) and $x \in A^n$. We may assign to the variables $s_i$ the values $x_i$ and execute the instructions of $T$ successively in $A$ according to the partial order $\prec$ as long as no division by a nonunit in $A$ occurs. (If $\rho_v(s_{u_{v,1}}, s_{u_{v,2}})$ gets the value "true" we agree to continue with the right son of $v$, otherwise with the left son.) In this way a unique path $T_{(A, x)}$ in $T$ starting from the root is defined. Should a division by a nonunit in $A$ occur we agree that $T_{(A, x)}$ ends with the instruction prior to the first unexecutable one. We say that $T$ is executable on the input $(A, x)$ if $T_{(A, x)}$ ends with a leaf.

Let $k \to R$ be a field extension. By identifying a prime ideal $p \in \text{Spec} R[y_1, \ldots, y_n]$ with $(\kappa(p), (y_1(p), \ldots, y_n(p)))$ we may consider $p$ as an input for $(\Omega^k, \{=\})$-decision trees $T$. Similarly any prime cone $\alpha \in \text{Sper} R[y_1, \ldots, y_n]$ defines an input $((\kappa(\alpha), \leq_\alpha), (y_1(\alpha), \ldots, y_n(\alpha)))$ for $(\Omega^k, \{=, \leq\})$-decision trees $T$. Via the identification of points $\xi \in R^n$ with its maximal ideals (or with its prime cones $P_\xi = \{f \in R[y_1, \ldots, y_n]: f(\xi) \geq 0\}$, $(R, \leq)$ being an ordered field) we get the usual interpretation of $\xi$ as the input $(R, \xi)$.

Let us assume now that $P = \{-, \leq\}$, $T$ being an $(\Omega^k, P)$-decision tree $T$ over $n$ and $\Pi := V(T_\alpha)$ for some $\alpha \in \text{Sper} R[y_1, \ldots, y_n]$. Let $(k[y_1, \ldots, y_n], y)$ be the universal input for the $\Omega^k$-straight line program $\beta(T_\alpha)$ over $n$. Execution of $\beta(T_\alpha)$ on this universal input yields a result sequence

$$(b_v)_{v \in (\Pi \cap V_2) \cup \{1, \ldots, n\}}.$$

For $v \in \Pi \cap V_2$ we put $f^i_v := b_{u_{v,i}}$ $(i = 1, 2)$. Since $\beta(T_\alpha)$ is executable on $\alpha$ we have $d(\alpha) \neq 0$. If $\max \Pi$ is a leaf we set $e := 0$. Otherwise let $w$ be the "critical" successor of $\max \Pi$ distinguished by $\alpha$; then $w \in V_1$, $\omega_w = /$. In this case we set $e := b_{u_{w,2}}$. Because of the maximality of $\Pi$ we have $e(\alpha) = 0$. We now put for $\rho \in P = \{-, \leq\}$

$$(V_2)_\rho := \{v \in V_2: \rho_v = \rho\}$$

and define partitions

$$\Pi \cap (V_2)_\rho = I_{\rho, \text{true}} \cup I_{\rho, \text{false}}$$

by setting

$$I_{\rho, \text{true}} := \{v \in \Pi \cap (V_2)_\rho: f^1_v(\alpha) \rho f^2_v(\alpha) \text{ is true in } (\kappa(\text{supp} \alpha), \leq_\alpha)\},$$

$$I_{\rho, \text{false}} := (\Pi \cap (V_2)_\rho) \setminus I_{\rho, \text{true}}.$$

It is an easy exercise to prove the following

Remark 9 (a) For all $\beta \in \text{Sper} R[y_1, \ldots, y_n]$ the statement $T_\beta = T_\alpha$ is equivalent to

$$d(\beta) \neq 0, e(\beta) = 0,$$

$$\forall \rho \in P \forall v \in \Pi \cap (V_2)_\rho \ (v \in I_{\rho, \text{true}} \iff f^1_v(\beta) \rho f^2_v(\beta) \text{ is true in } (\kappa(\text{supp} \beta), \leq_\beta)).$$

(b) If $R$ is real closed then the set $\{\beta \in \text{Sper} R[y_1, \ldots, y_n]: T_\beta = T_\alpha\}$ is constructible (even locally closed) and equals $\{\xi \in R^n: T_\xi = T_\alpha\}$.
An analogous statement obviously holds in the situation $P = \{=\}$.

Let $X \subset Y \subset \mathbb{R}^n$ be subsets, $P = \{=\}$ or $P = \{=, \leq\}$ and $R$ be an ordered field. We say that an $(\Omega^k, P)$-decision tree $T$ over $n$ decides membership in $X$ relative to $Y$ if every $\xi \in X$ defines a path ending with a yes-leaf and every $\xi \in Y$ defines a path ending with a no-leaf. The decision complexity $C(c, \{X, Y \setminus X\})$ of the partition $\{X, Y \setminus X\}$ with respect to a cost function $c : \Omega^k \cup P \to \mathbb{N}$ is defined as the minimum $c$-cost of a $(\Omega^k, P)$-decision tree $T$ over $n$ deciding membership in $X$ relative to $Y$.

The next proposition relates decision complexity, paths of certain prime cones and of points $\xi \in \mathbb{R}^n$, and verification complexity as defined in section 3.

**Proposition 10** Let $k \to R$ be a field extension, $R$ real closed, $X \subset Y \subset \mathbb{R}^n$ algebraic subsets and $X$ irreducible. Let $\mathcal{O}_{X,Y} := A(Y)_I(X)$ and $\alpha \in \text{Sper} \mathcal{O}_{X,Y}$ such that $\text{supp} \alpha = I(X)$. Then for every $(\Omega^k, \{=, \leq\})$-decision tree $T$ over $n$ deciding membership in $X$ relative to $Y$ the following holds:

(a) There is an open semi-algebraic subset $U \subset X$ such that $\alpha \in \bar{U}$ and

$$\forall \xi \in U \quad T_\xi = T_\alpha.$$

(b) If a cost function $c : \Omega^k \cup P \to \mathbb{N}$ satisfies $c(\neg) \leq \min \{c(=), c(\leq)\}$ then

$$L(c, T_\alpha) \geq VC_{\Omega^k, -\mathcal{O}_{X,Y}}(c |_{\Omega^k}, y', \alpha)$$

where $y' = (y'_i)$, $y'_i$ denoting the coordinate functions on $Y$. In particular,

$$C(c, \{X, Y \setminus X\}) \geq VC_{\Omega^k, -\mathcal{O}_{X,Y}}(c |_{\Omega^k}, y', \alpha).$$

**Proof:** We adopt the notation of Remark 9 and put $g_v := f_v^2 - f_v$ for $v \in \Pi \cap V_2$. Then

$$L_{k \rightarrow \mathbb{R}[y_1, \ldots, y_n]}(c |_{\Omega^k}, y, \{g_v : v \in \Pi \cap V_2\}) \leq L(c |_{\Omega^k}, T_\alpha) + |\Pi \cap V_2| c(\neg) \leq L(c, T_\alpha).$$

Moreover, by Remark 6

$$L_{k \rightarrow \mathcal{O}_{X,Y}}(c |_{\Omega^k}, y', \{\varphi(g_v) : v \in \Pi \cap V_2\}) \leq L_{k \rightarrow \mathbb{R}[y_1, \ldots, y_n]}(c |_{\Omega^k}, y, \{g_v : v \in \Pi \cap V_2\}),$$

where $\varphi : \mathbb{R}[y_1, \ldots, y_n] \rightarrow \mathcal{O}_{X,Y}$ is the canonical morphism. We put

$$I_{\neg, \text{true}} := \{v \in I_{\neg, \text{true}} : 0 < g_v(\alpha)\}$$

and define a semi-algebraic open subset $W$ of $Y_d$ by

$$W := \{0 \neq g_v : v \in I_{\neg, \text{false}}\} \cap \{0 > g_v : v \in I_{\neg, \text{false}}\} \cap \{0 < g_v : v \in I_{\neg, \text{true}}\} \subset Y_d.$$ 

The set $U := W \cap X_d$ is an open and semi-algebraic subset of $X_d$. Every element of

$$G := \{g_v : v \in I_{\neg, \text{true}}\} \cup \{g_v : v \in I_{\neg, \text{true}} \setminus I_{\neg, \text{true}} \cup \{e\}$$
vanishes on the prime cone $\alpha$ and therefore also on $X_d$. So we get

$$U \subset W \cap Z(G).$$

Furthermore, by Remark 9, we have

$$W \cap Z(G) \subset \{ \xi \in W : T_\xi = T_\alpha \}.$$  

From $\alpha \in \tilde{W}$ we conclude that $\alpha \in \tilde{U}$, in particular $U$ is nonempty. So there is a $\xi \in U$ such that $T_\xi = T_\alpha$, the path $T_\alpha$ therefore ends with a yes-leaf. Since $T$ decides membership in $X$ relative to $Y$ we conclude

$$\{ \xi \in W : T_\xi = T_\alpha \} \subset U.$$  

So we have equality

$$W \cap Z(G) = U = W \cap Z(\text{supp}\alpha),$$

and by Theorem 1

$$\tilde{W} \cap Z(G) = \tilde{W} \cap Z(\text{supp}\alpha) \text{ in } \text{Sper}A(Y)_d.$$  

By intersecting with the subspace $\text{Sper}O_{X,Y} \subset \text{Sper}A(Y)_d$ we see that

$$VC_{r,k-O_{X,Y}}(c|_{\Omega^k}, y', \alpha) \leq L_{k-O_{X,Y}}(c|_{\Omega^k}, y', \{\varphi(g_v) : g_v \in G\})$$

which completes the proof. $\square$

**Remark 11** Note that in Proposition 10 the membership problem $\{X, Y \setminus X\}$ may be replaced by a membership problem $\{X_1, Y_1 \setminus X_1\}$ where $X_1 \subset X$, $Y_1 \subset Y$ are semi-algebraic subsets satisfying

$$X_1 \subset Y_1, \ \alpha \in \tilde{X}_1, \ \tilde{Y}_1 \text{ neighbourhood of } \alpha \text{ in } \text{Sper}A(Y).$$

An analogue of Proposition 10 in the case $P = \{=\}$ can be proved similarly.

**Proposition 12** Let $k \to R$ be a field extension, $R$ algebraically closed, $X \subset Y \subset R^n$ algebraic subsets, $X$ irreducible and $p = I(X) \in \text{Spec}O_{X,Y}$. Then for every $(\Omega^k, \{=\})$-decision tree $T$ over $n$ deciding membership in $X$ relative to $Y$ the following holds:

(a) There is a nonempty Zariski-open subset $U \subset X$ such that

$$\forall \xi \in U \ T_\xi = T_p.$$  

(b) If a cost function $c : \Omega^k \sqcup \{=\} \to \mathbb{N}$ satisfies $c(-) \leq c(=)$ then

$$L(c, T_p) \geq VC_{k-O_{X,Y}}(c|_{\Omega^k}, y', p)$$

where $y' = (y'_i)$, $y'_i$ denoting the coordinate functions on $Y$. In particular,

$$C(c, \{X, Y \setminus X\}) \geq VC_{k-O_{X,Y}}(c|_{\Omega^k}, y', p).$$
Proposition 10 shows that the real verification complexity of the vanishing ideal \( p \) of \( X \) in a prime cone \( \alpha \) with \( \text{supp} \alpha = p \) is a lower bound on the \( c \)-length of any path defined by an element of \( X \) which is sufficiently close to \( \alpha \). By minimizing the real verification complexities over all such prime cones \( \alpha \) we obtain a lower bound which holds for all elements of \( X \) outside a lower dimensional algebraic subset, as in Proposition 12:

**Corollary 13** Let \( k \to R \) be a field extension, \( R \) real closed, \( X \subseteq Y \subseteq R^n \) algebraic subsets and \( X \) irreducible. Let \( S \subseteq X \) be a semi-algebraic subset of dimension \( \text{dim} X \). Assume furthermore that a cost function \( c : \Omega^k \cup \{=, \leq\} \to \mathbb{N} \) satisfying \( c(\cdot) \leq \min\{c(=), c(\leq)\} \) is given. Then for every \( (\Omega^k, \{=, \leq\}) \)-decision tree \( T \) over \( n \) deciding membership in \( X \) relative to \( Y \) there is a semi-algebraic subset \( Z \subseteq S \) such that \( \text{dim} Z < \text{dim} X \) and

\[
\forall \xi \in S \setminus Z \quad L(c, T_\xi) \geq \min\{VC_{r,k-\alpha}^{X,Y}(c |^{\alpha'}, y', \alpha) : \alpha \in \tilde{S}, \text{supp} \alpha = I(X)\}
\]

where \( y' = (y'_1), y'_1 \) denoting the coordinate functions on \( Y \).

**Proof:** The set

\[
T := \{T_\alpha : \alpha \in \tilde{S}, \text{supp} \alpha = I(X)\}
\]

is finite. By Remark 9 the set \( Z := \{\xi \in S : T_\xi \not\in T\} \) is semi-algebraic and \( \tilde{Z} = \{\beta \in \tilde{S} : T_\beta \not\in T\} \). For every \( \xi \in S \setminus Z \) we have by Proposition 10

\[
L(c, T_\xi) \geq \min\{VC_{r,k-\alpha}^{X,Y}(c |^{\alpha'}, y', \alpha) : \alpha \in \tilde{S}, \text{supp} \alpha = I(X)\}.
\]

From [B–C–R 87, Proposition 7.5.8, p. 132] we get

\[
dim Z = \sup\{\text{dim}(R[y_1, \ldots, y_n]/\text{supp} \beta) : \beta \in \tilde{Z}\}
\]

which is strictly smaller than \( \text{dim} X \). This proves the corollary.

\[\square\]

## 5 Verification complexity of linear prime ideals

In this section we will prove a linear lower bound for verification complexity in a special situation generalizing a result by Winograd [Win 70]. We will consider only the Ostrowski cost function \( c_* : \Omega^k \to \mathbb{N} \) which is defined by

\[
c_*(\omega) = \begin{cases} 
1 & \text{if } \omega \in \{*, /\}, \\
0 & \text{otherwise.}
\end{cases}
\]

Before stating our main result we introduce some notation.

(5.1) Let \( k \) be a field and \( A, B \) \( k \)-algebras. An ideal of \( A \otimes_k B \) is said to be defined over \( B \) if it is the extension \( A \otimes_k I \) of some ideal \( I \) of \( B \). For every ideal \( J \) of \( A \otimes_k B \) there is a smallest ideal \( J_B \) which contains \( J \) and is defined over \( B \), since the intersection of ideals defined over \( B \) is again defined over \( B \). Let \( (a_i) \) denote a \( k \)-basis of \( A \), \( (f_\ell) \) a system of generators of \( J \subseteq A \otimes_k B \) and write

\[
f_\ell = \sum a_i \otimes_k f_{ij}, \quad f_{ij} \in B.
\]
Then $J_B$ is generated by the $f_{ij}$.

(5.2) If $\varphi : B \to B'$ is a morphism of $k$-algebras and $J$ an ideal of $A \otimes_k B$ then

$$(1 \otimes_k \varphi)(J_B)(A \otimes_k B') = [(1 \otimes_k \varphi)(J)(A \otimes_k B')]_{B'}.$$ 

(5.3) We call a prime ideal $p$ of a polynomial ring $K[y_1, \ldots, y_m]$ over a field $K$ linear if it is generated by polynomials of degree one. To a linear prime ideal $p$ we associate the homogeneous linear prime ideal $q$ which is generated by the homogeneous linear parts of the elements of $p$ of degree one. If $k \to K$ is a field extension then $K[y_1, \ldots, y_m] = K \otimes_k k[y_1, \ldots, y_m]$ and $q_{k[y_1, \ldots, y_m]}$ is again a homogeneous linear prime ideal. Observe that if $p$ is generated by

$$\sum_{j=1}^{m} g_{ij} y_j + g_1, \ldots, \sum_{j=1}^{m} g_{nj} y_j + g_n, \quad (g_{ij}, g_i \in K)$$

then we can express the heights of $p, q, q_{k[y]}$ in the following way:

$$htp = htw = rk[g_{ij}], \quad htw_{k[y]} = dim_k \sum_{j=1}^{m} (g_{ij} y_j).$$

(5.4) Note furthermore that if $p_0$ is a linear prime ideal in $k[y_1, \ldots, y_m]$ then $K \otimes_k p_0$ is again linear prime and $ht(K \otimes_k p_0) = htp_0$.

In the following we will show that $htw_{k[y]} - htw$ is a lower bound on verification complexity for inputs of “product form” $\xi y := (\xi_1, \ldots, \xi_n, y_1, \ldots, y_m)$ where the $\xi_i \in K$ may be arbitrary.

**Theorem 14** Let $k \to K$ be a field extension, $p$ a linear prime ideal of $A := K[y_1, \ldots, y_m]$ and $q$ the associated homogeneous linear prime ideal. Then:

(a) $$\min \{ VC_{k \to A_p}(c_\xi, \xi y, pA_p) : n \in \mathbb{N}, \xi \in K^n \} \geq htw_{k[y]} - htw.$$  

(b) If $K$ is a real field and $\alpha \in \text{Sper} A_p$ such that $\text{supp} \alpha = pA_p$ then we have

$$\min \{ VC_{r,k \to A_p}(c_\xi, \xi y, \alpha) : n \in \mathbb{N}, \xi \in K^n \} \geq htw_{k[y]} - htw.$$  

**Remark 15** The left and right side in inequalities (5),(6) are invariant under the group of $K$-algebra automorphisms of $A$ having the form

$$y_j \mapsto \sum_{i=1}^{m} \gamma_{ij} y_i + \delta_j$$

where $\gamma \in \text{GL}_m(k)$, $\delta \in K^m$.

**Proof of Theorem 14:** We present a proof for part (b) only, statement (a) can be shown analogously. We proceed by induction on $m = \text{dim} A$. The start “$m = 0$” is trivial. Let us suppose $m > 0$.

**Case 1:** $\exists l \in (\sum_{i=1}^{m} k y_j + K) \cap p_l \neq 0$.

By Remark 15 we can assume without loss of generality that $l = y_1$. We put $A' := A[y_1 A = \ldots$
\[ K[y_2, \ldots, y_n] =: K[y'] \text{ and } p' := \pi(p) \text{ where } \pi: A \to A' \text{ is the canonical projection. Note that } A'_{p'} = A_p/\gamma_1 A_p. \text{ Let } \alpha' \in \text{Sper} A'_{p'} \text{ be the prime cone such that } \alpha = (\text{Sper} \pi_1)(\alpha') \text{ where } \pi_1: A_p \to A_p/\gamma_1 A_p \text{ is induced by } \pi. \text{ Then we have by Lemma 8 for every } \xi \in K^n \]

\[ VC_{r, k - A_p}(c_*, \xi y, \alpha) = VC_{r, k - A'_p}(c_*, \xi y', \alpha') \]

since \( \pi_1 \) is a local morphism of local rings. Let \( q' \) be the homogeneous linear prime ideal associated to \( p' \). Then

\[ q' = \pi(q), \quad (q')_{k[y']} = \pi(q_{k[y]}) \]

(by (5.2)), hence

\[ htq' = htq - 1, \quad ht(q')_{k[y']} = htq_{k[y]} - 1. \]

The desired statement follows therefore from the induction hypothesis.

**Case 2:** \( (\sum_{j=1}^n ky_j + K) \cap p = 0. \)

We first show that the structural map \( k \to A_p \) factors over \( k(y_1) \). Let \( \varphi: k[y_1] \to A \to k(p) \) denote the composition. Because of the linearity of \( p \) the field \( k(p) \) is a rational function field over \( K \) and by our assumption \( \varphi(y_1) \notin K \). So \( \varphi(y_1) \) is transcendental over \( K \) and \( \varphi \) is injective, i.e.

\[ K[y_1] \cap p = 0. \quad (7) \]

In order to reduce \( m \) we now focus on the field extension \( k(y_1) \to K(y_1) \) and put \( A' := K(y_1)[y_2, \ldots, y_n] =: K(y_1)[y'] \). Since \( A' \) is the localisation of \( A \) with respect to the multiplicative set \( K[y_1] \setminus \{0\} \) we conclude from (7) that \( p' := pA' \) is a linear prime ideal in \( A' \) and \( A'_{p'} = A_p. \) By the induction hypothesis we get

\[ \min \{ VC_{r, k(y_1)} - A_p(c_*, \xi y', \alpha) : n \in \mathbb{N}, \xi \in K(y_1)^n \} \geq htq_{k(y_1)[y']} - htq' \quad (8) \]

where \( q' \) is the homogeneous prime ideal associated with \( p' \). Let \( \pi: A \to A/y_1 A = K[y'] \) again denote the canonical projection. Then \( q' = \pi(q) A' \) and by (5.2) we have

\[ (q')_{k(y_1)[y']} = (\pi(q) A')_{k(y)[y']} = \pi(q)_{k[y']} A' = \pi(q_{k[y]}) A'. \quad (9) \]

It is easy to see that \( ht\pi(q) = htq \) and \( ht\pi(q_{k[y]}) \geq htq_{k[y]} - 1. \) From this, (9), and (5.4) we conclude

\[ htq_{k(y_1)[y']} - htq' \geq htq_{k[y]} - htq - 1. \quad (10) \]

We are now going to show that – after a transformation according to Remark 15 –

\[ t := \min \{ VC_{r, k - A_p}(c_*, \xi y, \alpha) : n \in \mathbb{N}, \xi \in K^n \} \]

is strictly larger than the left-hand side of (8), provided that \( t > 0. \) Then (8) and (10) imply the desired inequality in this case. The case "\( t = 0 \)" is treated separately. Assume

\[ t = VC_{r, k - A_p}(c_*, \eta y, \alpha) = L_{k - A_p}(c_*, \eta y, F') \]

for some \( \eta \in K^n \) and a suitable finite subset \( F \subset A_p \) such that

\[ Z(F) \cap W = Z(pA_p) \cap W \]

13
holds for some neighbourhood $W$ of $\alpha$ in $Sper A_p$.

**Case 2.1:** $t > 0$.

Let $\beta = (\beta_1, \ldots, \beta_r)$ be an optimal $\Omega^k$-straight line program that computes $F$ from $\eta y$ and $b_{-N-m+1}, \ldots, b_r$ be the corresponding result sequence. By our assumption $t > 0$ we have

$$\{i : b_i \not\in \sum_{j=1}^m ky_j + K\} \neq \emptyset;$$

let $l$ denote the minimum of this set. The instruction $\beta_i$ must be of the form

$$s_{l} := s_{l_1} * s_{l_2} \text{ or } s_{l} := s_{l_1} / s_{l_2}$$

where $s_{-N-m+1}, \ldots, s_r$ are the program variables and $l_1, l_2 < l$. The results $b_{l_1}, b_{l_2}$ lie in $\sum_{j=1}^m ky_j + K$ but not both of them lie in $K$. We only discuss the case where the division occurs and $b_{l_2} \not\in K$, the other three cases can be settled analogously. By Remark 15 we may assume without loss of generality that $b_{l_2} = y_1$. If we replace the $l$-th instruction $\beta_i$ of $\beta$ by the scalar multiplication instruction

$$s_{l} := y_{l}^{-1} s_{l_1}$$

we get an $\Omega^{k(y_1)}$-straight line program $\beta'$ having the same result sequence as $\beta$ on input $(A_p, \eta y)$; $A_p$ considered as $k(y_1)$- or $k$-algebra, respectively. Therefore

$$t > L_{k(y_1)} \rightarrow A'_{p} (c_*, (\eta y_1)y', F) \geq VC r, k(y_1) \rightarrow A'_{p} (c_*, (\eta y_1)y', \alpha)$$

$$\geq \min \{VC r, k(y_1) \rightarrow A'_{p} (c_*, \xi y', \alpha) : n \in \mathbb{N}, \xi \in K(y_1)^n\},$$

so $t$ is strictly larger than the left-hand side of (8).

**Case 2.2:** $t = 0$.

Since we still assume that $(\sum_{j=1}^m k y_j + K) \cap p = 0$ the condition $t = 0$ implies $F = 0$. So any element of $p A_p$ vanishes on $W$. But by Lemma 3 the open subset $W$ of $Sper A_p$ contains a prime cone with support 0. Therefore $p = 0$, $q = q_{k(y)} = 0$ and the desired inequality is true. 

\[ \square \]

**Remark 16** Let $F = \{f_1, \ldots, f_n\}$ denote the set of functions in (4) and consider the linear prime ideal $p := (z_1 - f_1, \ldots, z_n - f_n)$ of $B := K[y, z]$. Then, by the canonical imbedding $K(y) \hookrightarrow B_p$, we have for all $\xi \in K^N$

$$L_{k \rightarrow K(y)} (c_*, \xi y, F) \geq VC_{k \rightarrow B_p} (c_*, (\xi y)z, p B_p).$$

So Winograd's lower bound [Win 70] follows from Theorem 14.

## 6 Applications

We illustrate the results of sections 4,5 by determining the decision complexity of two basic problems. Let $R$ be an algebraically or real closed field.
Corollary 17 Let \( p_1 \in \text{Spec} R[x_1, \ldots, x_s, y_1, \ldots, y_m] \) be the contraction of a linear prime ideal \( p \in \text{Spec} R(x_1, \ldots, x_s)[y_1, \ldots, y_m] \) and \( q \) be the homogeneous linear prime ideal associated with \( p \). Let \( T \) be an \((\Omega^R, P)\)-decision tree over \( s + m \) deciding membership in \( X := Z(p_1) \subset R^{s+m} \) relative to \( R^{s+m} \). Then in both cases \( P = \{ = \}, R \) algebraically closed, respectively \( P = \{ =, \leq \}, R \) real closed, there is an algebraic subset \( Z \subset X \) with \( \dim Z < \dim X \) and such that

\[
\forall \xi \in X \setminus Z \quad L(c_*, T_\xi) \geq h_\xi - q R[y] - htq.
\]

The proof follows from Proposition 12, Corollary 13, Theorem 14 and the observation

\[
\mathcal{O}_{X,R^{s+m}} = R[x,y]_{p_1} = R(x)[y]_p.
\]

Corollary 18 (a) Let \( X := Z(f_1, \ldots, f_n) \subset R^{n(d+1)+1} \) where

\[
f_i := \sum_{j=0}^d y_{ij} x^j \quad (i = 1, \ldots, n).
\]

Then \( C(c_*, \{ X, R^{n(d+1)+1} \setminus X \}) = dn \).

(b) Let \( X := Z(g_1, \ldots, g_n) \subset R^{n(d+1)+d} \) where

\[
g_i := \sum_{j=1}^d y_{ij} x^j + y_{i0} \quad (i = 1, \ldots, n).
\]

Then \( C(c_*, \{ X, R^{n(d+1)+d} \setminus X \}) = dn \).

The upper bounds in Corollary 18 are obvious. The lower bounds follow from Corollary 17. Note that the algebraic sets \( X \) are graphs of polynomial maps \( R^M \rightarrow R^n \) (\( M \) suitable) and therefore irreducible.

Acknowledgement: We thank Robby Robson and Gilbert Stengle for interesting discussions.

References


Efficiency of Asynchronous Transfer Mode Networks in Transporting Wide-Area Data Traffic

Ramón Cáceres
TR-91-043
July, 1991