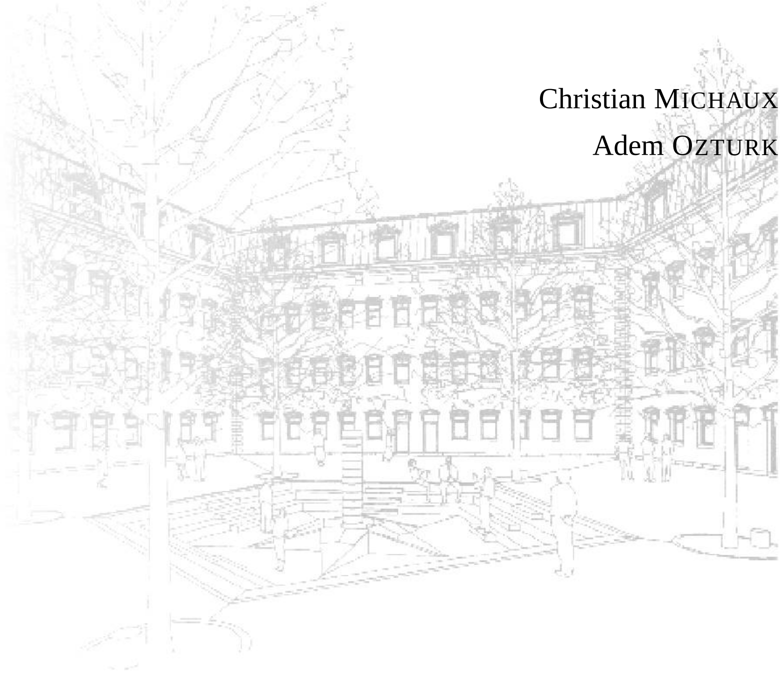
Preprint #10
April 11, 2002

Quantifier Elimination following Muchnik

Christian MICHAUX
Adem OZTURK



Université de Mons-Hainaut
Institut de Mathématique
Phone: +32 65 37 35 07 — Fax: +32 65 37 33 18
Web: http://www.umh.ac.be/math/institut

Quantifier Elimination following Muchnik[*]

Christian Michaux Adem Ozturk

christian.michaux@umh.ac.be ozturk@umh.ac.be

Université de Mons-Hainaut
Institut de Mathématique
B-7000 Mons, Belgium.

To Denis Richard for his sixtieth birthday

Abstract. This paper describes a very simple (high school level) algorithm of quantifier elimination for real closed fields and algebraically closed fields following an idea of A. Muchnik. The algorithm essentially relies on intermediate value property, pseudo-euclidean division and sign change table for univariate polynomials over $\mathbb{R}$. Surprisingly this algorithm exhibits some more general feature and it can be very naturally turned into an algorithm of quantifier elimination for algebraically closed fields too.

Mathematics Subject Classification:
Keywords and phrases: Quantifier elimination

[*] This work has been supported by Esprit working group 27150 NeuroCOLT2, by Intas project 2000-447 and by a grant from the National Bank of Belgium.

Genesis

In 1996, Alexei Semënov and Denis Richard showed to the first author a short draft [S] sketching a very elementary algorithm (high school level) of “quantifier elimination” for real closed fields following an idea of A. Muchnik. To our knowledge, it was never expanded into a paper. The second author, under the direction of the first one, transformed it into a coherent text as a part of his “mémoire de licence” [Oz]. The algorithm essentially relies on intermediate value property, pseudo-euclidean division and sign change table for univariate polynomials over $\mathbb{R}$.

It was then realized that this algorithm exhibits some more general feature and that it can be very naturally turned into an algorithm of quantifier elimination for algebraically closed fields too. We think that this algorithm deserves to be better known.

In section 2, we describe the algorithm for real closed fields and prove its correctness. Then, in section 3, we show how to turn it into an algorithm for algebraically closed fields. Although the algorithm presented here is not substantially different from the one proposed in the book [BCR], we believe it is quite simpler in its presentation. We do not precisely analyse its complexity but we suspect that it is far from being efficient w.r.t. the fast algorithms of quantifier elimination for real closed fields recently discovered by Renegar and other authors (see [Re]).

1 A brief history

One can probably say that the logical study of the field of real numbers began with the work of Alfred Tarski on quantifier elimination. A modern formulation of his result of quantifier elimination for the reals is the following:

> To any formula $\varphi(x_1, \ldots, x_n)$ in the vocabulary $\{0, 1, +, \ldots, <\}$ one can effectively associate two objects: (i) a quantifier free formula $\overline{\varphi}(x_1, \ldots, x_n)$ in the same vocabulary, and (ii) a proof of the equivalence $\varphi \leftrightarrow \overline{\varphi}$ that uses only the axioms of ordered fields together with the intermediate value property for polynomials (that is the axioms for real closed fields[1]).

We will refer it in the sequel as Tarski's Theorem.

A precise formulation of this fundamental theorem and a clear outline of its proof were announced in **The completeness of elementary algebra and geometry** [T1], but the publication was interrupted by the war. A detailed proof of the fundamental theorem finally appeared under the title **A decision method for elementary algebra and geometry** [T2].

Tarski's original proof relies on an algorithm which tests the solvability of a system of polynomial equations and inequations in several unknowns in $\mathbb{R}$, it is a kind of generalized Sturm's theorem (which itself generalizes sign change's rule). In his proof, he only uses the axioms of real closed fields. But Tarski does not mention the result in full generality, he only states it for the fields of real numbers and real algebraic numbers. In [T2] the emphasis was put on a decision procedure for elementary Euclidean geometry which is a byproduct of his theorem of quantifier elimination for the field of real numbers.

Also, Tarski never seems to have explicitly mentioned in his publications that the theory of algebraically closed fields admits quantifier

[1] We recall that Rolle's Theorem is valid for real closed fields

elimination. Obviously, he knew this result, but he was only interested in decidability and completeness in each characteristic.

After the algorithm proposed by Tarski, different authors introduced new ones. Among these, let us cite Seidenberg [Se], a colleague of Tarski in Berkeley, and Hörmander [Hö]. The purpose of Seidenberg was to make Tarski's result much more accessible to mathematicians. Seidenberg's proof does not use the logical formalism, he describes the proof in a geometric and algebraic context. That explains why Tarski's Theorem restricted to the field $\mathbb{R}$, is generally known as Seidenberg's Theorem (or as the Seidenberg-Tarski's Theorem).

Quantifier elimination made important contributions to the logical study of the field of real numbers, but also to algebra. As A. Robinson shows in [Ro], quantifier elimination for real closed fields permits to give an easy alternative proof to Hilbert's Seventeenth Problem. In real algebraic geometry, Tarski's Theorem implies e.g. that the projection of semi-algebraic set is semi-algebraic and that the closure of a semi-algebraic set is semi-algebraic. Similarly for algebraically closed fields, Chevalley's Constructibility Theorem, asserting that the projection of a constructible set is constructible, is a particular formulation of quantifier elimination. The reader can find plenty of details about history of Tarski's Theorem, its proofs and uses in mathematics, logic and computer science in [D] which was very influential when writing this short introduction.

2 Muchnik's algorithm

In this section, we describe the algorithm together with a proof of its correctness. Let us remind the reader that a real closed field is an ordered field[2] with the intermediate value property for univariate poly-

[2] A field endowed with a linear ordering compatible with field operations

nomials. For simplicity of the exposition, we describe the algorithm for the field of real numbers. As it can be easily checked, the same proof holds for any real closed field.

Through this paper we consider polynomials of the form $p(\vec{Y}, X)$ with coefficients in $\mathbb{Z}$ and where X and $\vec{Y} = (Y_1, \ldots, Y_m)$ are variables. Such polynomials can also be seen as polynomials in the variable X with coefficients in the ring $\mathbb{Z}[Y_1, \ldots, Y_m]$. The notation $\deg p$ is used for the degree of $p(\vec{Y}, X)$ with respect to the variable X. In the sequel we will use the following four operations which apply to polynomials with nonzero degree.

Let $p(X) = a_n X^n + \cdots + a_0 \in \mathbb{Z}[\vec{Y}][X]$ with $n \geqslant 1$ and $a_n \neq 0$.

(i) *Derivative*: $\mathrm{D}(p) = \frac{\partial}{\partial X} p$

(ii) *Extracting the leading coefficient*: $\mathrm{E}(p) = a_n$

(iii) *Omitting the leading term*: $\mathrm{O}(p) = a_{n-1} X^{n-1} + \cdots + a_0$

(iv) *Modified remainder* : it is applied to a couple of polynomials $p = a_n X^n + \cdots + a_0$ and $q = b_m X^m + \cdots + b_o$ such that $n = \deg p \geqslant \deg q = m$, $q \neq p$ and provides the unique polynomial r in $\mathbb{Z}[\vec{Y}][X]$ with $\deg r < \deg q$ such that

$$\begin{aligned} & (b_m)^{n-m+1} \cdot p = q \cdot \ell + r \\ \text{i.e.,} \qquad & E(q)^{n-m+1} \cdot p = q \cdot \ell + r \end{aligned}$$

for some ℓ in $\mathbb{Z}[\vec{Y}][X]$. We will denote r by $\mathrm{MR}(p, q)$.

We want to define the closure of a finite set[3] of polynomials in $\mathbb{Z}[\vec{Y}][X]$ under the four operations. For any finite sets S, S' of poly-

[3] The same definitions and results hold if we replace set by list; this remark will be useful because we will have further to consider the list of polynomials which appear in a formula.

nomials $\in \mathbb{Z}[\vec{Y}][X]$, we define

$$\begin{aligned}
\mathrm{D}(S) &:= \{D(p) : p \in S,\ \deg p \geqslant 1\} \\
\mathrm{E}(S) &:= \{E(p) : p \in S,\ \deg p \geqslant 1\} \\
\mathrm{O}(S) &:= \{O(p) : p \in S,\ \deg p \geqslant 1\} \\
\mathrm{MR}(S, S') &:= \{\mathrm{MR}(p, q) : (p, q) \in S \times S^{'},\ p \neq q,\ \deg p \geqslant \deg q \geqslant 1\} \\
C(S, S^{'}) &:= \mathrm{D}(S^{'}) \cup \mathrm{E}(S^{'}) \cup \mathrm{O}(S^{'}) \cup \mathrm{MR}(S, S^{'}) \cup \mathrm{MR}(S', S) \\
\deg S &:= \max_{p \in S} \deg p
\end{aligned}$$

Proposition 2.1. *Let S be a set of polynomials in $\mathbb{Z}[\vec{Y}][X]$. Then*

(i) $\#\mathrm{D}(S), \#\mathrm{E}(S), \#\mathrm{O}(S) \leqslant \#S$

(ii) $\#\mathrm{MR}(S, S') \leqslant (\#S)(\#S')$

(iii) $\deg C(S, S') < \deg S'$

where $\#S$ denote the cardinal of the set S.

Proof. The claims are obvious. □

We claim that the closure of a finite set S of polynomials under the four operations is finite. Let us define $S_0 = S$ and $S_n = C(\bigcup_{i=0}^{n-1} S_i, S_{n-1})$, $n \geqslant 1$.

Proposition 2.2. *Let S be a finite set of polynomials $\in \mathbb{Z}[\vec{Y}][X]$ and let* $\mathrm{CS} = \bigcup_{n \in \mathbb{N}} S_n$. *Then*

(i) CS *is the closure of S by the operations* $\mathrm{D}, \mathrm{E}, \mathrm{O}, \mathrm{MR}$.

(ii) CS *is a finite set.*

(iii) CS *can be effectively build within a finite number of steps from S.*

Proof. The first claim is immediate from the construction of CS. Let us consider the second one. Since each of the operations $\mathrm{D}, \mathrm{E}, \mathrm{O}, \mathrm{MR}$ decreases the degree of polynomials, it results that if $\deg S_n \geqslant 1$ then $\deg S_{n+1} < \deg S_n$. Therefore there exists $k \in \mathbb{N}$ such that $\deg S_k = 0$ and so the process stops. On the other hand, for any $n \in \mathbb{N}$ we have $\# S_n < \infty$ since S_0 is finite. Hence CS is finite. This proves the second claim. The last one is now trivial. $\square$

Let BCS be the subset of CS which consists of all polynomials of degree zero w.r.t. the variable X. By a **sign condition** on BCS, we mean that we fix the sign at each element of BCS. If $\mathrm{BCS} = \big\{t_1(\vec{Y}\,), \ldots, t_s(\vec{Y}\,)\big\}$ then we associate to a sign condition on BCS the following formula

$$\Delta(\vec{Y}\,) := t_1(\vec{Y}\,)\Delta_1 0 \wedge \cdots \wedge t_s(\vec{Y}\,)\Delta_s 0 \tag{1}$$

where $\Delta_i \in \{<, =, >\}$. Sometimes we will say that the column $\Delta := (\Delta_1 \ \cdots \ \Delta_s)^t$ is a sign condition on BCS.

A sign condition Δ on BCS is said **satisfiable** if there exists $\vec{a}$ such that formula $\Delta(\vec{a}\,)$ is true i.e.

$$\mathbb{R} \models (\exists \vec{a})\big(t_1(\vec{a})\Delta_1 0 \wedge \cdots \wedge t_s(\vec{a})\Delta_s 0\big)$$

It is equivalent to say that the system of polynomial inequalities appearing in the formula $\Delta(\vec{Y}\,)$ has a solution $\vec{a}$ in $\mathbb{R}^m$. Sometimes we will use the terminology "$\vec{a}$ satisfies Δ on BCS" or "formula $\Delta(\vec{a})$ is true".

Let $S = \{p_1(\vec{Y}, X), \ldots, p_\ell(\vec{Y}, X)\}$ be a finite set of polynomials $\in \mathbb{Z}[\vec{Y}][X]$ and let $\gamma_0 = -\infty < \gamma_1 < \gamma_2 < \cdots < \gamma_n < \gamma_{n+1} = +\infty$ be in $\mathbb{R} \cup \{-\infty, +\infty\}$. We now consider tables T on S with ℓ rows labelled by $p_1, \ldots, p_\ell$ and $2n+1$ columns labelled by

$$]\gamma_0, \gamma_1[,\ \gamma_1,\ ]\gamma_1, \gamma_2[,\ \ldots,\ \gamma_n,\ ]\gamma_n, \gamma_{n+1}[$$

such that the entries of the table are in $\{<,=,>\}$ and, for each γ_j with $1 \leqslant j \leqslant n$, there exists i such that the entry in position (p_i, γ_j) is "$=$". Such a table is called **a sign change table**[4] for S and it is a visual representation of the following formula[5]

$$T(\vec{Y}) := (\exists \gamma_1, \dots, \gamma_n) \bigwedge_{i=1}^{\ell} \Bigg[\Big(\bigwedge_{j=1}^{n} p_i(\vec{Y}, \gamma_j) \nabla_{ij} 0 \Big) \\ \wedge \Big(\bigwedge_{j=1}^{n+1} (\forall z) \left(\gamma_{j-1} < z < \gamma_j \rightarrow p_i(\vec{Y}, z) \nabla'_{ij} 0 \right) \Big) \Bigg]$$

where ∇_{ij}, ∇'_{ij} are respectively entries of the table in position (p_i, γ_j) and $(p_i,]\gamma_{j-1}\gamma_j[)$. Sometimes it will be useful to say that the sign of p_i at γ_j is ∇_{ij} to express that ∇_{ij} is the sign in position (p_i, γ_j).

We say that **a table T on S is satisfied at $\vec{a} \in \mathbb{R}^m$**, or that $\vec{a}$ satisfies the table T on S, if the formula $T(\vec{a})$ is true. Let us remark that, when $T(\vec{a})$ is true, it expresses the sign changes of the polynomials $p_i(\vec{a}, X)$'s on the real line w.r.t. the interval subdivision given by the γ_i's and that $\gamma_1, \dots, \gamma_n$ are all zeros of non zero polynomials among $p_1(\vec{a}, X), \dots, p_\ell(\vec{a}, X)$; or in other words, the visual representation of $T(\vec{a})$ is exactly the sign change table (in the classical sense) of the polynomials $p_1(\vec{a}, X), \dots, p_\ell(\vec{a}, X)$.

Key Lemma. *Let be S and* BCS *as above. Any satisfiable sign condition Δ on* BCS *determines in a unique way a sign change table T_Δ for* CS *(and so for S) such that*

(i) The table T_Δ can be effectively computed from S and Δ.

[4] These signs tables with $-, 0, +$ instead of $<,=,>$ are well-known among high school students when they study curve-sketching techniques for functions.

[5] When $j = 1$, $\gamma_{j-1} < z < \gamma_j$ is replaced by $z < \gamma_1$, similarly for $j = n + 1$.

(ii) for any $\vec{a} \in \mathbb{R}^m$, $\vec{a}$ satisfies Δ on BCS *iff $\vec{a}$ satisfies T_Δ on* CS*,*
i.e., for any $\vec{a} \in \mathbb{R}^m$, $\Delta(\vec{a})$ is true iff $T_\Delta(\vec{a})$ is true
or again $\mathbb{R} \models \forall \vec{Y}, \big(\Delta(\vec{Y}) \leftrightarrow T_\Delta(\vec{Y})\big)$

Before proving the lemma, let us show how it gives a proof of Tarski's Theorem

Proof of Tarski's Theorem. First let us recall an elementary fact about quantifier elimination. To prove quantifier elimination for any formula we only need to prove it for formulas with one existential quantifier; indeed when we know how to eliminate one quantifier we can proceed by induction on the number of quantifiers. Moreover the existential quantifier distributes disjonctions. So for the theory of real numbers in the natural language of ordered fields, we just need to show how to eliminate the quantifier in formulas of the following type

$$\varphi(\vec{Y}) := (\exists X)\big(p_1(Y_1, \dots, Y_m, X)\nabla_1 0 \wedge \cdots \\ \cdots \wedge p_\ell(Y_1, \dots, Y_m, X)\nabla_\ell 0\big)$$

where $\nabla_i \in \{<, =, >\}$ and $p_i(\vec{Y}, X) \in \mathbb{Z}[\vec{Y}][X]$ for $i \in \{1, \dots, \ell\}$. Let us denote[6] $L := \{p_1(\vec{Y}, X), \dots, p_\ell(\vec{Y}, X)\}$. Let us remark that to know whether the formula $\varphi(\vec{a})$ is true for a given $\vec{a} \in \mathbb{R}^m$ is equivalent to know whether the column $\nabla = (\nabla_1 \ \cdots \ \nabla_n)^t$ appears in the sign change table of the list $p_1(\vec{a}, X), \dots, p_\ell(\vec{a}, X)$. In view of the key lemma, the answer to this question is equivalent to the existence of a sign condition Δ on BCL such that $\Delta(\vec{a})$ is true and the sign change table T_Δ on L contains the column ∇. To achieve the proof it remains to show that the existence of such Δ can be expressed by a formula without quantifier.

[6] In general L will be a list (with some repetitions), but all the results stated before are true for a list, as already mentionned.

Let $\mathcal{F}$ be the set of all sign conditions Δ on BCL such that the sign change table T_Δ on L contains ∇ amongst its columns. From key lemma and the previous remark, it is clear that for all $\vec{a} \in \mathbb{R}^m$ and for all $\Delta \in \mathcal{F}$ we have $\Delta(\vec{a})$ is true implies that $\varphi(\vec{a})$ is true. Conversely it is clear that if $\varphi(\vec{a})$ is true then $\Delta(\vec{a})$ is true for some Δ in $\mathcal{F}$ (Δ is given by the signs of the elements of BCL evaluated in $\vec{a}$). Hence we have that

$$\mathbb{R} \models \forall \vec{Y} \left(\varphi(\vec{Y}) \longleftrightarrow \bigvee_{\Delta \in \mathcal{F}} \Delta(\vec{Y}) \right)$$

Since the formula $\Delta(\vec{Y})$ are quantifier free the theorem is proved. □

Proof of Key Lemma. First for the given S, we construct CS and BCS and let $\mathrm{BCS} = \{t_1, \ldots, t_s\}$ and $\mathrm{CS} = \mathrm{BCS} \,\dot{\cup}\, \{q_1, \ldots, q_{s'}\}$. From the construction of CS and BCS we can be easily convinced that we can choose an ordering for $q_1, \ldots, q_{s'}$ such that the following property is satisfied: for any q_i, $i = 1, \ldots, s'$ and p among $q_1, \ldots, q_{i-1}$, we have $\mathrm{D}(q_i), \mathrm{E}(q_i), \mathrm{O}(q_i)$ and $\mathrm{MR}(q_i, p) \in \mathrm{CS}_{i-1} = \mathrm{BCS} \cup \{q_1, \ldots, q_{i-1}\}$.[7] This property can be restated in the following form: for any $j \in \{1, \ldots, s'\}$ the set CS_j is closed under the four operations $\mathrm{D}, \mathrm{E}, \mathrm{O}, \mathrm{MR}$. This property will be called "the closure property" hereafter.

Now the proof consists in a proof by induction on j by building a sign change table for CS_j with the properties (i) and (ii) (for $j \in \{1, \ldots, s'\}$). From the construction it will be clear that there is a unique way to do it. The existence of this unique table for CS_j together with the closure property is called hereafter the "invariant" of the proof.

Let Δ be $(\Delta_1 \;\cdots\; \Delta_s)^t$ a satisfiable sign condition on BCS. It is immediate from the definitions that to fix Δ on BCS is equivalent to

[7] We put $\mathrm{CS}_0 = BCS$.

fix the following sign change table[8] for BCS

	$-\infty$		$+\infty$
t_1	Δ_1	Δ_1	Δ_1
$\vdots$	$\vdots$	$\vdots$	$\vdots$
t_s	Δ_s	Δ_s	Δ_s

Let $j = 0$. let us remark that the sign change table on BCS defined above from Δ satisfies properties (i) and (ii) and so the invariant. Since by assumption CS_1 satisfies the closure property, the polynomial q_1 is necessarily of degree 1, and so $\mathrm{E}(q_1)$ and $\mathrm{O}(q_1)$ are in BCS. So, q_1 is equal to $t_i X + t_j$ where $t_i, t_j \in BCS$.

If the sign of t_i is "$=$" in the sign condition Δ then $q_i = t_j$; in this case it is clear that we get a sign change table for CS_1 by copying the row labelled by t_j with a new label q_1:

q_1	Δ_j	Δ_j	Δ_j

If the sign of t_i is not "$=$" then for any $\vec{a} \in \mathbb{R}^m$ satisfying Δ we have $t_i(\vec{a}) \neq 0$. Thus $q_1 = t_i(\vec{a})X + t_j(\vec{a})$ has a root in $\mathbb{R}$. We split then the column labelled $]-\infty, +\infty[$ in three columns labelled by $]-\infty, \gamma[$, γ and $]\gamma, +\infty[$ and we obtain the following table for CS_1:

X	$-\infty$		γ		$+\infty$
t_1	Δ_1	Δ_1	Δ_1	Δ_1	Δ_1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
t_s	Δ_s	Δ_s	Δ_s	Δ_s	Δ_s
q_1	$-\Delta_i$	$-\Delta_i$	$=$	Δ_i	Δ_i

[8] For convenience of the proof we add two columns to the table for BCS labelled by $+\infty$ and $-\infty$.

In both cases it is easy from the construction to check that properties (i) and (ii) are true for this table. This proves the initial step of the induction.

Let us assume that we have built the table for CS_j which satisfies the invariant. Again the closure property guarantees that the $\mathrm{D}(q_{j+1})$, $\mathrm{E}(q_{j+1})$ and $\mathrm{O}(q_{j+1})$ are in CS_j.

If the sign of the leading coefficient of q_{j+1} is "$=$" in the table CS_j, the extension is obtained as in the case $j = 0$: we add at the bottom of the table a row labelled by q_{j+1} which is a copy of the row with the label $\mathrm{O}(q_{j+1})$ in the table for CS_j.

If the sign of the leading coefficient of q_{j+1} is not "$=$", let us assume that the labels of the columns of the table for CS_j are $-\infty = \gamma_0,\ ]\gamma_0, \gamma_1[,\ \gamma_1, \ldots,\ ]\gamma_n, \gamma_{n+1}[,\ \gamma_{n+1} = +\infty$.[9] Obviously the table for CS_{j+1} will have one more row at the bottom labelled by q_{j+1} and also will have additional columns.

We now describe the construction of this table. For this purpose, we need to find the sign of q_{j+1} at $\gamma_0, \ldots, \gamma_{n+1}$. From the sign of the leading coefficient of q_{j+1} (which is given by Δ), it is easy to compute the sign of q_{j+1} at $\gamma_0 = -\infty$ and $\gamma_{n+1} = +\infty$. To get the sign of q_{j+1} at $\gamma \in \{\gamma_1, \ldots, \gamma_n\}$ we use our modified remainder operation; let us choose q in $\{q_1, \ldots, q_j\}$ such that the sign in position (q, γ) in the table for CS_j is "$=$" and let us perform the division of q_{j+1} by q. Then we have

$$\mathrm{E}(q)^m \cdot q_{j+1} = h.q + \mathrm{MR}(q_{j+1}, q)$$

where $m = 1 + \deg q_{j+1} - \deg q$.

[9] Since property (ii) is true by assumption for the table for CS_j, we have that this table is exactly the sign change table for the polynomials $q_1(\vec{a}, X), \ldots, q_j(\vec{a}, X)$ for any $\vec{a} \in \mathbb{R}^m$ satisfying the table, i.e. the γ_i's can be seen as all the roots in $\mathbb{R}$ of the nonzero polynomials among $q_1(\vec{a}, X), \ldots, q_j(\vec{a}, X)$.

By induction the signs of $\mathrm{E}(q), q, \mathrm{MR}(q_{j+1}, q)$ at γ are known. Hence the sign of q_{j+1} at γ is given by

$$(\text{sign of } \mathrm{E}(q)^m \text{ at } \gamma) \cdot (\text{sign of } \mathrm{MR}(q_{j+1}, q) \text{ at } \gamma)$$

As the table for CS_j satisfies property (ii), we have that the signs of $E(q), q, MR(q_{j+1}, q)$ at $\gamma \in \{\gamma_0, \ldots, \gamma_{n+1}\}$ are constant on

$$\mathcal{V} := \{\vec{a} \in \mathbb{R}^m : \mathbb{R} \models \Delta(\vec{a})\}$$

Therefore the sign of q_{j+1} at γ is constant on $\mathcal{V}$. So for the remaining of the proof we can choose for $\vec{Y}$ a value $\vec{a} \in \mathcal{V}$.

Now we expand the table for CS_j into a table for CS_{j+1}. Assume that signs of $q_{j+1}(\vec{a}, X)$ at γ_i and γ_{i+1} are "$=$". Then the derivative of q_{j+1} would have a root in $]\gamma_i, \gamma_{i+1}[$ since between two roots of a polynomial there is a root of its derivative (Rolle's theorem). So, this root would be also a root of the derivative. But the derivative of q_{j+1} belongs to CS_j, this contradicts the fact that $\gamma_1, \ldots, \gamma_n$ are all the roots of the nonzero polynomials among $q_1(\vec{a}, X), \ldots, q_j(\vec{a}, X)$. The same argument shows that there is at most one root of q_{j+1} in each interval $[\gamma_i, \gamma_{i+1}]$.

If the signs of q_{j+1} in γ_i and γ_{i+1} are $(>, >)$ or $(<, <)$, there is no root of q_{j+1} between these. Otherwise q_{j+1} would have a root of multiplicity at least two in $]\gamma_i \gamma_{i+1}[$. So, this root would be also a root of the derivative. This gives a contradiction as above. Finally, if signs of q_{j+1} at γ_i and γ_{i+1} are opposite then[10] q_{j+1} has a root ρ in $]\gamma_i, \gamma_{i+1}[$. In this case we split the column labelled by $]\gamma_i, \gamma_{i+1}[$ in three columns labelled by $]\gamma_i, \rho[$, ρ and $]\rho, \gamma_{i+1}[$, and we put "$=$" in the position (q_{j+1}, ρ).

[10] It is here that the intermediate value property for polynomials is used.

Now it is easy to find signs of q_{j+1} between all columns of the table and thus to finish the whole procedure. If in the row labelled by q_{j+1} we have an empty place between "$(>,>)$", or "$(>,=)$" or "$(=,>)$", we put "$>$" into it. In the other cases we put "$<$". Let us remark that each row labelled by $t_1, \ldots, t_s, q_1, \ldots, q_j$ contains empty places in added columns. It easy to fill them since the introduction of roots for q_{j+1} does not change the signs of the other polynomials. □

3 Muchnik's algorithm and algebraically closed fields

One of main advantages of Muchnik's algorithm developed in the key lemma is the facility to apply it to algebraically closed fields. Obviously, there is some differences because in these fields there is no notion of ordering and also, polynomials of degree d have exactly d roots counted with multiplicities. Therefore, we have to change the definition of sign change table introduced before.

Let K be an algebraically closed field of any characteristic. Let $S = \{p_1, \ldots, p_\ell\}$ a finite list of polynomials $K[\vec{Y}, X]$ and let $\gamma_1, \ldots, \gamma_m$ in K. We consider tables T on S with ℓ rows and m columns labelled by

$$\gamma_1, \ldots, \gamma_m$$

such that the entries of the table are in $\{\neq, =\}$. Such a table is called **a sign change table** for S. With this definition, a natural analogue of the previous key lemma can be stated, we leave this easy task to the reader. As in the case of real closed fields, the proof that algebraically closed fields in the language $\{+, -, \ldots, 1, 0\}$ admit quantifier elimination is based upon the modified key lemma.

We sketch now the proof of the modified key lemma. More exactly, we explain the difference with the previous proof. For this reason, we keep the same notations.

The main difference appears when we add columns to sign change table of $\mathrm{BCS} \dot{\cup} \{q_1, \ldots, q_j\}$ which corresponds to new roots of q_{j+1}. In the previous case, the number of added columns to the table is determined by the signs of q_{j+1} in $\gamma_1, \ldots, \gamma_n$. In the algebraically closed case, we use the fact that polynomials of degree d have exactly d roots counted with multiplicities. So, in order to determine the number of new columns to add, it is sufficient to determine which among $\gamma_1, \ldots, \gamma_n$ are roots of q_{j+1} (with their multiplicity). Indeed, if we denote μ_i the multiplicity of γ_i as a root of q_{j+1} with the convention that $\mu_i = 0$ if $q_{j+1}(\gamma_i) \neq 0$, then the number of new columns is given by[11]

$$\deg q_{j+1} - \sum_{i=1}^{k} \mu_i \,.$$

By the modified remainder operation, it's easy to find the roots of q_{j+1} among $\gamma_1, \ldots, \gamma_k$. And knowing the sign change table for CS_j, we can read the multiplicity of a root γ_i of q_{j+1} among $\{\gamma_1, \ldots, \gamma_n\}$ by looking at the sign of the derivatives of q_{j+1} at γ_i. Thereby, we obtain a natural μ_i such that

$$\big(\mathrm{D}^{\mu_i - 1}(q_{j+1})\big)(\gamma_i) = 0 \quad \text{and} \quad \big(\mathrm{D}^{\mu_i}(q_{j+1})\big)(\gamma_i) \neq 0.$$

Obviously, μ_i is the multiplicity of γ_i. The proof of the modified key lemma is now trivial.

[11] Let us remark that a new root of q_{j+1} is of multiplicity 1 because otherwise this root will already be a root of its derivative $D(q_{j+1})$ and so it will be one of the γ_i's.

References

[BCR] J. Bochnak, M. Coste, and M. F. Roy, *Géométrie algébrique réelle*, Springer Verlag (1986).

[D] L. van den Dries, *Alfred Tarski's elimination theory for real closed fields*, J. of Symbolic Logic, 53 (1988), 7–19.

[Hö] L. Hörmander, *The analysis of linear partial differential operators*, Vol. 2, Springer Verlag (1983).

[Oz] A. Öztürk, *Théorème de Sturm, généralisations et corps exponentiels*, Mémoire de fin d'études, Université de Mons-Hainaut (1997).

[Re] J. Renegar, *On the computational complexity and geometry of the first-order theory of the reals, part I,II & III*, J. of Symbolic Computation, 13 (1992), 255–352.

[Ro] A. Robinson, *On ordered fields and definite functions*, Math. Ann. 130 (1955), 257–271.

[Se] A. Seidenberg, *A new decision method for elementary algebra*, Annals of Mathematics 60 (1954), 365–374.

[S] A. L. Semënov, *Decidability of the Field of Reals*, unpublished draft (1996).

[T1] A. Tarski, *The completeness of elementary algebra and geometry*, Institut Blaise Pascal, Paris, (1967) iv+50pp. (A reprint from page proofs of a work scheduled to appear in 1940 in *Actualités scientifiques et industrielles*, Hermann & C$^{\text{ie}}$, Paris, but which did not appear due to the wartime conditions.)

[T2] A. Tarski, *A decision method for elementary algebra and geometry* (prepared for publication by J. C. C. Mc Kinsey), U.S. Air Force Project RAND, R-109, the RAND Corporation, Santa Monica, California, (1948) iv+60pp.

Recent preprints

[1] *Maurice Boffa's 60th Birthday Workshop*, March 23, 2000.

[2] Catherine FINET, *Perturbed minimization principles in partially ordered Banach spaces*, June 29, 2000.

[3] Arnaud MAES, Corinne CERF, *A family of brunnian links based on Edwards' construction of Venn diagrams*, July 15, 2000.

[4] Catherine FINET & Lucas QUARTA & Christophe TROESTLER, *Vector-valued Variational Principles*, January 19, 2001.

[5] Gilles GODEFROY, *Montons les degrés*, 8 mars 2001.

[6] Paul VAN PRAAG, *Quaternions as reflexive skew fields*, 22 mars 2001.

[7] Maurice BOFFA, *Théorie des ensembles et dualité*, 17 avril 2001.

[8] Paul VAN PRAAG, *Pedro Nuñez, Simon Stevin, et le plus grand commun diviseur des polynômes*, 17 avril 2001.

[9] TROESTLER C., *Equivalence of BSS scalar- and vector-recursion*, June 4, 2001.

You can find more informations as well as download the preprints of the *Institut de Mathématique* on the web site: `http://www.umh.ac.be/math/preprints/`. Printed copies are available upon request by writing to:

Institut de Mathématique
Université de Mons-Hainaut
« Le Pentagone », 6 av. du champ de Mars
7000 Mons, Belgique