MUCHNIK'S PROOF OF TARSKI-SEIDENBERG

HANS SCHOUTENS

ABSTRACT. These notes arose in an attempt to understand a preprint in English by Semenov entitled *Decidability of the Field of Reals* regarding a proof due to Andrej Muchnik of the Tarski-Seidenberg algebraic quantifier elimination over the reals. (At present, I know of two Russian sources in which this proof has appeared: [1] and [2].) The method of proof is extremely simple: it consists of determining from the coefficients of a polynomial, a finite list of polynomial expressions in these coefficients, such that the knowledge of the signs of these expressions yields (in an effective way) the knowledge of the sign table of the original function. These expressions in the coefficients are obtained from the original polynomial by three very simple procedures: (Eucledean) division, differentation, and truncation. As such this proof is truly an *undergraduate* proof of a Theorem that without doubt belongs to the Pantheon of Mathematics. Moreover, the method extends to include an effective quantifier elimination procedure for any algebraically closed field of characteristic zero, as well as of any real closed field.

1. SIGN DIAGRAMS

To a polynomial $p(Y)$ over the reals in the single variable Y we associate its *sign evolution* as follows. Let $\xi_2 < \xi_4 < \cdots < \xi_{2d}$ be its real roots (we ignore their multiplicity). Then the sign of p is constant on each intermediate interval (ξ_{2i}, ξ_{2i+2}). So let ξ_{2i+1} be any point in that interval and let ξ_1 (respectively, ξ_{2d+1}) be any number smaller than ξ_2 (respectively, bigger than ξ_{2d}). The elements ξ_i are called *test points*. Hence we know the sign evolution of p once we know the sign for each test point. For a real number a, let $\operatorname{sgn} a := 0$ if $a = 0$, let $\operatorname{sgn} a := +1$ if $a > 0$, and let $\operatorname{sgn} a := -1$ if $a < 0$. In conclusion, to each polynomial p we will associate its *row of signs*

$$(\operatorname{sgn} p(\xi_1), \operatorname{sgn} p(\xi_2), \ldots, \operatorname{sgn} p(\xi_{2d+1})).$$

Since we need to deal with several polynomials simultanseously, we no longer insist that roots are test points with even index. Namely, let $L := (p_1, \ldots, p_m)$ be a list of polynomials in one variable Y with real coefficients (allowing repetition as well as the zero polynomial) and let $\Xi := (\xi_1, \ldots, \xi_n)$ be a list of test points. Let $\mathfrak{D}$ be an $m \times n$-matrix with entries in $\{-1, 0, 1\}$. We will use the entries of L to label the rows of $\mathfrak{D}$ and the elements of Ξ to label its columns, that is to say, $\mathfrak{D}(p_i, \xi_j)$ is the (i, j)-th entry of $\mathfrak{D}$. We call $\mathfrak{D}$ a *sign diagram* for L, if the following holds. There exists an n-tuple of real numbers $\Xi := (\xi_1, \ldots, \xi_n)$, with $\xi_1 < \cdots < \xi_n$, such that

- any real root of some non-zero p_i is among the ξ_j, and any two such roots are separated by at least one other ξ_j which is not a root of any non-zero polynomial in L;
- $\mathfrak{D}(p_i, \xi_j)$ is the sign of $p_i(\xi_j)$.

Date: 25.02.04.

Key words and phrases. quantifier elimination, Tarski-Seidenberg, semialgebraic sets.

Hence the row labeled p_i contains a row of signs of p_i with possibly the signs in some extra points lying in intervals between its roots. In particular, if p_i is identically zero, the row labeled p_i is also identically zero; we do not exclude this case, but we will refer to such a row as a *zero-row*. A test point which is a root of some non-zero p_i is simply called a *root of* L; the remaining test points are called *non-roots of* L. Two adjacent columns cannot be equal unless their are both labeled by a non-root. Omitting one of these redundant columns then yields again a sign diagram for L. In deleting redundant columns in this way we obtain a unique smallest sign diagram for L, called the *reduced sign diagram* for L and denoted $\operatorname{diag}(L)$. In particular, if all the p_i are constant, then the reduced sign diagram consists of a single column given by the respective signs of these constants.

1.1. *Remark.* If $\mathfrak{D}$ is a sign diagram for L, then by construction, we can find for each $y \in \mathbb{R}$ a column in $\mathfrak{D}$ which gives precisely the signs in y, that is to say, there is a j, such that $\mathfrak{D}(p_i, \xi_j) = \operatorname{sgn} p_i(y)$, for all i.

Another property of a sign diagram is that there can never be two subsequent zero's in a row, unless the row is a zero row, and neither can two adjacent non-zero entries in a row have opposite sign.

2. Muchnik Sets

Let A be a domain and let Y be a single variable. Let

$$p := a_d Y^d + a_{d-1} Y^{d-1} + \dots a_1 Y + a_0$$

be a polynomial in $A[Y]$ of degree d, so that $a_d \neq 0$ (we take up the convention that the zero-polynomial has degree $-\infty$). We will denote by p° the result of omitting the highest degree term of p, that is to say,

$$p^\circ := a_{d-1} Y^{d-1} + \dots a_1 Y + a_0$$

(if p is the zero polynomial, then so is p°). Let $q := b_e Y^e + \dots b_1 Y + b_0$ be a non-zero polynomial in $A[Y]$ with $e \leq d$.

2.1. **Definition** (Pseudo-remainders)**.** Performing Euclidean division on p by q, there are unique polynomials h and r, with r of degree strictly smaller than e, such that

$$b_e^{d-e+1} p = hq + r.$$

We call r the *pseudo-remainder* of p and q, and denote it $\operatorname{rem}(p, q)$.

Let L be a collection of polynomials (including constants) in $A[Y]$.

2.2. **Definition** (Muchnik Sets)**.** We say that L is a *Muchnik set*, if the following three properties hold.

(**T**) If p lies in L, then so does p°.
(**D**) If p lies in L, then so does its derivative p'.
(**R**) If p and q lie in L, then so does their pseudo-remainder $\operatorname{rem}(p, q)$.

2.3. *Remark.* Any Muchnik set contains the zero polynomial; any finite set of constants which includes zero, is Muchnik. We denote the collection of all the constants of a Muchnik set L by L_0. Note that the coefficients of all $p \in L$ are, up to a positive integer multiple (some factorial), among the constants L_0. This is a direct consequence of rules (**T**) and (**D**). However, rule (**R**) will create many more constants which are non-trivial expressions in the original coefficients.

2.4. *Remark.* Note that each of these three operations are closure operations and hence we can form for each set L' of polynomials the smallest Muchnik set containing L', which we then call the *Muchnik closure* of L'. Since each of the three rules yields a polynomial of smaller degree, the Muchnik closure of a finite set is again finite. Exploiting this fact further, we make the following definition.

2.5. **Definition** (Muchnik Lists)**.** Let L be a Muchnik set and enumerate its elements in such way that the degrees are non-decreasing. Any such enumeration will be called a *Muchnik list*.

Hence, if L is a Muchnik list, then it starts with 0, followed by the remaining elements in L_0, listed in some order, and then come the higher degree elements of L.

2.6. **Lemma.** *Let L be a Muchnik list. Then any initial segment of L is again a Muchnik list.*

Proof. We induct on the length of the an initial segment M of L. If M has length 1, then M is just the singleton $\{0\}$ and the statement is clear (in fact, the statement also holds for the initial segment L_0 as already pointed out). For the general case, suppose M is an initial segment of L with last element p. By the inductive argument, we know that $M \setminus \{p\}$ is Muchnik and we need to show that so is M. By rule (**T**), we have $p^\circ \in L$. However, since p° has degree strictly less than p, it must be enumerated in the list L before p° and therefore it must occur in M. A similar argument shows that $p' \in M$. Lastly, if $q \in M$, then both $\operatorname{rem}(p,q)$ and $\operatorname{rem}(q,p)$ have degree less than the degree of p (note that q has degree at most the degree of p since it is enumerated in L before p). Again we conclude that these pseudo-remainders must lie in M, since they lie in L by rule (**R**). □

3. Quantifier Elimination and Decidability

Let $A := \mathbb{R}[X]$, where $X := (X_1, \dots, X_N)$. Let $L := (p_1, \dots, p_m)$ be a list of polynomials p_i in $\mathbb{R}[X][Y]$. For any $\mathbf{x} \in \mathbb{R}^N$, we put

$$L(\mathbf{x}) := (p_1(\mathbf{x}, Y), \dots, p_m(\mathbf{x}, Y))$$

so that $L(\mathbf{x})$ is a list whose entries are polynomials in the single variable Y over $\mathbb{R}$. This applies in particular to a Muchnik list L and its sublist of constants L_0 (with respect to Y). Suppose that the subset L_0 has length m_0. In the next section, I will prove the existence of an effective algorithm, depending on L, with the following property. Let $\mathfrak{C}_0$ be a column labeled by L_0 (in other words, an $(m_0 \times 1)$-matrix) with entries in $\{-1, 0, 1\}$. To each such $\mathfrak{C}_0$, the algorithm assigns an $m \times n$-matrix $\mathcal{A}(\mathfrak{C}_0)$ with entries in $\{-1, 0, 1\}$ (where we take the rows to be labeled by the elements in the list L) with the property that

$$\mathcal{A}(\operatorname{diag}(L_0(\mathbf{x}))) = \operatorname{diag}(L(\mathbf{x}))$$

for each $\mathbf{x} \in \mathbb{R}^N$.

Note that $\operatorname{diag}(L_0(\mathbf{x}))$ is simply the column with entries the $\operatorname{sgn} p(\mathbf{x})$, for $p \in L_0$. In particular, we see that the first m_0 rows of $\mathcal{A}(\mathfrak{C}_0)$, that is to say, those rows labeled by some $p \in L_0$, are constant rows. More precisely, the upper $m_0 \times n$ part of $\mathcal{A}(\mathfrak{C}_0)$ is just n copies of the column $\mathfrak{C}_0$. Note also that if $\mathfrak{C}_0$ does not occur as a column $\operatorname{diag}(L_0(\mathbf{x}))$ for any $\mathbf{x}$, then it does not really matter which matrix the algorithm assigns as $\mathcal{A}(\mathfrak{C}_0)$. However, we do not know in advance that $\mathfrak{C}_0$ is not of the form $\operatorname{diag}(L_0(\mathbf{x}))$, and one of the tasks of the algorithm will be to detect this. All this will be explained in the next section.

Granted we have an algorithm with these properties, we can now prove the celebrated Tarski-Seidenberg Theorem. Recall that the language of ordered fields consists of the usual field language together with a symbol for the ordering. More precisely, we have constant symbols 0 and 1; binary function symbols $+$ for addition, $-$ for subtraction, and $\cdot$ for multiplication; and one binary relation symbol $<$ for the order relation

3.1. **Theorem** (Tarski-Seidenberg)**.** *The field of reals admits elimination of quantifiers in the language of ordered fields.*

Proof. By standard arguments it is enough to show that a formula of the form $(\exists y)\varphi(x,y)$, with $\varphi(x,y)$ quantifier free and $x := (x_1,\dots,x_N)$ and y a single variable, is equivalent with a quantifier free formula. Also, by induction on the number of disjuncts in a disjunctive normal form, we may assume that φ is a conjunction of formulae of the form $\operatorname{sgn} p(x,y) = \varepsilon_p$, with p a real polynomial and $\varepsilon_p \in \{-1,0,1\}$. Let L' be the collection of all polynomials that thus occur in φ and let L be its Muchnik closure, arranged as a Muchnik list. Suppose L has length m. Let us say that an $(m \times n)$-matrix $\mathfrak{D}$ with entries in $\{-1,0,1\}$ is *φ-compatible*, if there exists a column-label ξ, so that $\mathfrak{D}(p,\xi) = \varepsilon_p$, for all $p \in L'$. Using Remark 1.1, we get, for $\mathbf{x} \in \mathbb{R}^N$, that $(\exists y)\varphi(\mathbf{x},y)$ holds if and only if $\operatorname{diag}(L(\mathbf{x}))$ is φ-compatible.

Let $\mathfrak{C}_1,\dots,\mathfrak{C}_l$ be an enumeration of all possible columns of height m_0 with entries in $\{-1,0,1\}$. For $i = 1,\dots,l$, let $\psi_i(x)$ be the quantifier free formula which expresses that

$$\operatorname{diag}(L_0(x)) = \mathfrak{C}_i. \tag{1}$$

Let $\mathcal{A}(\mathfrak{C}_i)$ be the matrix obtained from $\mathfrak{C}_i$ by means of the algorithm from §4. Let $I \subset \{1,\dots,l\}$ be those indices for which $\mathcal{A}(\mathfrak{C}_i)$ is φ-compatible. It follows that

$$(\exists y)\varphi(x,y) \Longleftrightarrow \bigvee_{i\in I} \psi_i(x).$$

This concludes the proof of the Theorem, since the right hand side is quantifier free. □

Note that since the algorithm described in the next section is effective, so is the quantifier elimination process in the above proof. In particular, we obtain the following immediate corollary.

3.2. **Corollary.** *The field of reals is decidable in the language of ordered fields.*

4. The Algorithm $\mathcal{A}$ to Calculate a Sign Diagram

As before, L' is some list of polynomials in $\mathbb{R}[X,Y]$ and L is its Muchnik closure (with respect to the last variable Y). Our goal is to algorithmically calculate a sign diagram for $L(\mathbf{x})$ from $\operatorname{diag}(L_0(\mathbf{x}))$, for any point $\mathbf{x} \in \mathbb{R}^N$. Recall that L_0 is the initial part of L consisting of all polynomials not containing Y (the constants with respect to Y). By Lemma 2.6, each initial segment M of L is again Muchnik. Therefore, we will build by induction a sign diagram for each $M(\mathbf{x})$; it will in general be an augmentation of the previous sign diagram by one more row and several more columns (due to the occurrence of new roots). In conclusion, it suffices to prove the following lemma.

4.1. **Lemma.** *Let $A := \mathbb{R}[X]$, where $X := (X_1,\dots,X_N)$. Let L be a finite Muchnik list in $A[Y]$ of length m and let p be a non-constant polynomial in $A[Y]$. Suppose that $L^+ := L \cup \{p\}$ is again a Muchnik list. There exists an effective algorithm $\mathcal{A}$ which assigns to any $(m \times n)$-matrix $\mathfrak{C}$ with entries in $\{-1,0,1\}$ an $(m+1) \times n'$-matrix $\mathcal{A}(\mathfrak{C})$ with entries in $\{-1,0,1\}$ (where $n \leq n'$), such that for each $\mathbf{x} \in \mathbb{R}^N$, we have that*

$$\mathcal{A}(\operatorname{diag}(L(\mathbf{x}))) = \operatorname{diag}(L^+(\mathbf{x})).$$

Proof. Our goal is twofold. Firstly, given a matrix $\mathfrak{C}$ with entries -1, 0 or 1, with rows labeled by the Muchnik list L (from top to bottom) and columns labeled by test points ξ, we want to assign a matrix $\mathfrak{C}^+ := \mathcal{A}(\mathfrak{C})$ with one additional row at the bottom, labeled p, and some additional columns. Secondly, if $\mathbf{x} \in \mathbb{R}^N$ and $\mathfrak{C} = \operatorname{diag}(L(\mathbf{x}))$, then we have to verify that $\mathfrak{C}^+$ is a sign diagram for $L^+(\mathbf{x})$ (after which we can trim it to become a reduced sign diagram). At several stages, we might run into an inconsistency of $\mathfrak{C}$ that excludes it from being of the form $\operatorname{diag}(L(\mathbf{x}))$ for some $\mathbf{x}$, and then we will *reject* this matrix.

Suppose p has degree $d \geq 1$ in Y and let $a \neq 0$ be its highest degree coefficient (so that $a \in \mathbb{R}[X]$). Note that $d!\, a$, p° and p' all belong to L by definition of Muchnik list. Fix also $\mathbf{x} \in \mathbb{R}^N$ and let ξ be a test point. We will define $\mathfrak{C}^+(p, \xi)$, depending on various cases.

Case 1. The row in $\mathfrak{C}$ labeled $d!\, a$ is not a constant row. This is impossible if $\mathfrak{C}$ is of the form $\operatorname{diag}(L(\mathbf{x}))$, so we reject this matrix.

Case 2. The row in $\mathfrak{C}$ labeled $d!\, a$ is the zero row. If $\mathfrak{C}$ is of the form $\operatorname{diag}(L(\mathbf{x}))$, then this means that $a(\mathbf{x}) = 0$ and hence $p(\mathbf{x}, Y)$ and $p^\circ(\mathbf{x}, Y)$ have the same sign evolution. Therefore, we let the last row of $\mathfrak{C}^+$ be a copy of the row labeled p° in $\mathfrak{C}$, and we are done in this case.

Hence, we may in addition assume that the row in $\mathfrak{C}$ labeled $d!\, a$ is a constant row with value $\alpha \neq 0$. If $\mathfrak{C}$ only consists of a single column, then we double this column at this point.

Case 3. The column labeled by ξ is either the first or the last column. If $\mathfrak{C}$ is of the form $\operatorname{diag}(L(\mathbf{x}))$, then $\mathfrak{C}^+(p, \xi)$ ought to be the sign of $p(\mathbf{x}, Y)$ at minus or plus infinity respectively. Therefore, we put $\mathfrak{C}^+(p, \xi)$ equal to $(-1)^d \alpha$ and α respectively, and we are done for these columns. So we may assume in addition that ξ is the label of an internal column.

Case 4. The point ξ represents a root of L, that is to say, there is some $q \in L$ such that $\mathfrak{C}(q, \xi) = 0$ but the row labeled q in $\mathfrak{C}$ is not a zero row. If $\mathfrak{C}$ is of the form $\operatorname{diag}(L(\mathbf{x}))$, then this means that $q(\mathbf{x}, \xi) = 0$ but $q(\mathbf{x}, Y)$ is not identically zero. Choose a $q \in L$ of minimal possible degree with these properties. Let e be its degree and b its leading coefficient, so that $e!\, b \in L$. If the row labeled by $e!\, b$ in $\mathfrak{C}$ is not a constant row, we again reject this matrix, so we may assume that it has constant value β.

Case 5. Suppose $\beta = 0$. If $\mathfrak{C}$ is of the form $\operatorname{diag}(L(\mathbf{x}))$, then this means that $b(\mathbf{x}) = 0$. However, since $q = bY^e + q^\circ$, we get that $q^\circ(\mathbf{x}, \xi)$ is also zero. Since $q^\circ \in L$ has degree less than e, minimality implies that the row in $\mathfrak{C}$ labeled q° must be a zero row, that is to say, that $q^\circ(\mathbf{x}, Y)$ is identically zero. However, so is then $q(\mathbf{x}, Y)$, contradiction. Therefore, we reject any matrix with this property, so that we may assume in addition that $\beta \neq 0$.

Let r be the pseudo-remainder of p by q, so that $b^{d-e+1}p = hq + r$, for some polynomials $h, r \in \mathbb{R}[X, Y]$ with r of degree at most $e - 1$. If $\mathfrak{C}$ is of the form $\operatorname{diag}(L(\mathbf{x}))$, then $b(\mathbf{x})^{d-e+1}p(\mathbf{x}, \xi) = r(\mathbf{x}, \xi)$. Therefore, we set

$$\mathfrak{C}^+(p, \xi) := \beta^{d-e+1} \cdot \mathfrak{C}(r, \xi),$$

and we are done in this case.

So we may assume that ξ represents a non-root of L. Let ξ_- and ξ_+ denote the respective labels of the column just preceding and just following it. Since in a reduced sign diagram, roots alternate with non-roots, ξ_- and ξ_+ must represent roots, and therefore the signs $\varepsilon_- := \mathfrak{C}^+(p, \xi_-)$ and $\varepsilon_+ := \mathfrak{C}^+(p, \xi_+)$ have already been defined.

Case 6. Suppose $\varepsilon_- = \varepsilon_+ = 0$. If $\mathfrak{C}$ is of the form $\operatorname{diag}(L(\mathbf{x}))$, this means that $p(\mathbf{x}, \xi_-) = p(\mathbf{x}, \xi_+) = 0$. By the Intermediate Value Theorem, there is some η in the open interval (ξ_-, ξ_+) such that $p'(\mathbf{x}, \eta) = 0$. By definition of sign diagram, since $p' \in L$, its roots must occur as column labels, and hence $\eta = \xi$. By the assumption on ξ, the entire row labeled p' in $\mathfrak{C}$ must then be a zero row, which means that $p'(\mathbf{x}, Y)$ is identically zero. This in turn means that $p(\mathbf{x}, Y)$ is constant, and this constant therefore must be zero, a case already dealt with. In other words, if $\varepsilon_- = \varepsilon_+ = 0$, we reject $\mathfrak{C}$.

Case 7. Suppose ε_- and ε_+ have opposite sign and are non-zero. If $\mathfrak{C}$ is of the form $\operatorname{diag}(L(\mathbf{x}))$, then this means that $p(\mathbf{x}, \xi_-)$ and $p(\mathbf{x}, \xi_+)$ have opposite sign. By the Intermediate Value Theorem, there is some η in the open interval (ξ_-, ξ_+) such that $p(\mathbf{x}, \eta) = 0$. There is no reason why this η should agree with ξ, so that we encounter a new situation, in which an additional root has to be added to the labels. However, since we should alternate roots with non-roots, we have to replace the single ξ-column of $\mathfrak{C}$ by three copies of it and then put in the bottom row of $\mathfrak{C}^+$ the three values $(\varepsilon_-, 0, \varepsilon_+)$ to reflect the new sign behaviour.

Therefore, we are also done in that case, so that we may assume that exactly one among the $\varepsilon_-, \varepsilon_+$ is zero or that they have both the same sign. I claim that if $\mathfrak{C}$ is of the form $\operatorname{diag}(L(\mathbf{x}))$, then $p(\mathbf{x}, Y)$ has no root in the open interval (ξ_-, ξ_+). Assuming the claim, the sign on that interval must therefore be the same everywhere and equal to the sign in an endpoint which is not a root. In conclusion, our algorithm is sound, if we put $\mathfrak{C}^+(p, \xi)$ equal to the non-zero value among $\varepsilon_-, \varepsilon_+$.

So all that remains is to prove the claim. Suppose towards a contradiction, that there is some η in the open interval (ξ_-, ξ_+) such that $p(\mathbf{x}, \eta) = 0$. If one of the endpoints is also a root, then again by the Intermediate Value Theorem, we would have also a root of p' in that interval, and we have already ruled this out. Hence $p(\mathbf{x}, Y)$ has the same sign at the endpoints of the interval, say, for the sake of argument, that it is positive at both ends. For $p(\mathbf{x}, Y)$ to become zero, it therefore has to decrease and then again increase. This would mean that p' changes sign at that interval and hence in particular must have a root there, again an impossibility. □

Some further remarks. The proof is in fact independent of the real numbers and holds equally in any real closed field, since the only non-trivial property used is the Intermediate Value Theorem. Moreover, since the quantifier free formula obtained by this process depends only on the coefficients of the polynomials in the original formula, we obtain that any formula defined over some ordered field is equivalent (in its real closure) with a quantifier free formula defined over that field.

As for the complexity, a rough calculation yields that if a formula $\chi(x)$ with one existentially quantified variable consisting of l polynomial inequalities, each of degree at most d (so that the cardinality of L' in the proof is l), then we end up with a quantifier free formula $\Psi(x)$ consisting of a number of inequalities of the order $O(l^{2^{d-1}})$. More precisely, the cardinality of L and L_0 is $O(m)$ where $m = l^{2^{d-1}}$. This leaves us with 3^m possible sign assignments which might or might not lead to a compatible formula. The algorithm apparently is polynomial in the degree and the cardinality of L, so that the reduction of χ to Ψ is in time of order a polynomial in m times 3^m.

However, if we fix the degree d and seek for an algorithm that determines whether a sentence χ (with quantifiers) in which the number of quantified variables is bounded and all occurring polynomials have degree at most d (and coefficients in some effective ordered field K) is true or false, then this can be done in non-deterministic polynomial time, if we assume that any arithmetic operation in the field K can be carried out in time $O(1)$. Indeed, we need only guess non-deterministically a sign assignment for the elements in L_0. All other constructions are now carried out in a time depending polynomially on l, the number of inequalities in the sentence.

5. Quantifier Elimination for algebraically closed fields of characteristic zero

The techniques of Muchnik sets can also be used to prove quantifier elimination for $\mathbb{C}$ (of course, this is less hard a theorem and admits many other elegant proofs). I will explain the case for $\mathbb{C}$, but the same argument works for any algebraically closed field of characteristic zero–the proof unfortunately collapses in positive characteristic. We start with defining the analogue of sign diagram in this situation.

Root Diagrams. Let $p \in \mathbb{C}[Y]$ with Y a single variable. If p is not the zero polynomial, then a *row of roots* for p is simply a row of 0's and 1's such that (a) at least one entry is equal to 1; and (b), the number of entries equal to 0 is equal to the number of distinct roots of p in $\mathbb{C}$. Any zero-row is a row of roots for the zero polynomial. We label the entries of a row of roots by some complex numbers ξ with the convention that the entry labeled by ξ is 0 if and only if $p(\xi) = 0$. Contrary to the real case, we do not care about the order in which we list the ξ.

If L is a list of polynomials (allowing repetitions as well as the zero polynomial), then a *root diagram* for L is a matrix of 0's and 1's with rows labeled by the polynomials $p \in L$ and columns labeled by some complex numbers ξ, having the property that each row is a row of roots for its label and moreover, there is at least one column in which the only 0's come from zero-rows. If there are more columns of the latter type, then we can safely delete these and still have a root diagram. Moreover, any permutation of the columns yields another root diagram for L. Apart from these permutations and redundant columns, the root diagram of L is uniquely determined and we will denote it again by $\operatorname{diag}(L)$.

As in the case of the reals, it suffices to prove the following analogue of Lemma 4.1 to obtain an effective quantifier elimination procedure for $\mathbb{C}$ (details are left to the reader; I will only prove the lemma).

5.1. **Lemma.** *Let $A = \mathbb{C}[X]$, where $X = (X_1, \dots, X_N)$. Let L be a finite Muchnik list in $A[Y]$ of length m and let p be a non-constant polynomial in $A[Y]$. Suppose $L^+ = L \cup \{p\}$ is again Muchnik. There exists an effective algorithm $\mathfrak{C} \longmapsto \mathfrak{C}^+$ which assigns to any $(m \times n)$-matrix $\mathfrak{C}$ with entries in $\{0,1\}$ an $(m+1) \times n'$-matrix $\mathfrak{C}^+$ with entries in $\{0,1\}$ (where $n \leq n'$), such that for each $\mathbf{x} \in \mathbb{C}^N$, we have that*

$$\operatorname{diag}(L(\mathbf{x})) \longmapsto \operatorname{diag}(L^+(\mathbf{x})).$$

Proof. Let $\mathbf{x} \in \mathbb{C}^N$. Suppose p has degree $d \geq 1$ in Y and let $a \in \mathbb{C}[X]$ be its highest degree coefficient. Note that $d!\, a \in L$ by rule (**D**). If the row in $\mathfrak{C}^+$ is not constant, it should be rejected as in Case 1 of the previous proof. If the row in $\mathfrak{C}$ corresponding to $d!\, a$ is a zero-row, we do exactly as in Case 2 in the previous proof. So we may assume that this row has constant value 1; if $\mathfrak{C}$ is of the form $\operatorname{diag}(L(\mathbf{x}))$, this means that $a(\mathbf{x}) \neq 0$. Let ξ be the label of a column of $\mathfrak{C}$.

Assume first that the column of $\mathfrak{C}$ with label ξ contains a 0 other than those 0's coming from zero-rows. Let $q \in L$ be of minimal degree e with the property that $\mathfrak{C}(q, \xi) = 0$ but the row labeled by q is not a zero-row. If $\mathfrak{C}$ is of the form $\operatorname{diag}(L(\mathbf{x}))$, then this means that $q(\mathbf{x}, \xi) = 0$, but $q(\mathbf{x}, Y)$ is not identically zero. Let b be the leading coefficient of q.

By the same argument as in Case 5, we may reject the matrix if the row labeled by $e!\,b$ is not constant or is a zero-row. In particular, we may assume that $\mathfrak{C}(e!\,b,\xi) = 1$. Letting $r := \operatorname{rem}(p,q)$, we put $\mathfrak{C}^+(p,\xi) := \mathfrak{C}(r,\xi)$, and we are done in this case by the same argument as before.

In the remaining case, when the only zero's in the column labeled by ξ come from zero rows, we reason as follows. If $\mathfrak{C}$ is of the form $\operatorname{diag}(L(\mathbf{x}))$, then any new root of p must have multiplicity 1, for otherwise it would also be a root of $p' \in L$ whence would have appeared in some column of $\mathfrak{C}$. To determine how many new roots p has, we count, this time with multiplicity, the roots of p so far marked. In other words, if η is a column for which we already determined $\mathfrak{C}^+(p,\eta) = 0$, then we let $e(\eta)$ be the multiplicity of that root (and otherwise we put $e(\eta) := 0$). To calculate $e(\eta)$, we simply look for successive derivatives $p', p'', p^{(3)}, \dots$ of p (which all belong to L and at least one is a non-zero constant) and see whether there is also a 0 in the row labeled by these derivatives. More precisely, $e(\eta)$ is equal to the smallest l for which $\mathfrak{C}(p^{(l)},\eta) = 1$. To conclude the construction of $\mathfrak{C}^+$, let e be the difference between d (=the degree of p) and the sum of the $e(\eta)$. Add e new columns to the matrix so far obtained, all with a 0 in the bottom row and a 1 everywhere else, except in zero-rows. □

References

1. A. Semenov, *Decision procedues for logical theories*, Cybernetics and computer technology **2** (1986), 134–146 (Russian).
2. A. Shen and N.K. Vereshchagin, *Languages and calculi*, Moscow Center for Continuous Mathematical Education, 2000 (Russian).

Department of Mathematics, NYC College of Technology, CUNY,
E-mail address: hschoutens@citytech.cuny.edu