ELSEVIER

Mathematics and Computers in Simulation 42 (1996) 429–438

MATHEMATICS AND COMPUTERS IN SIMULATION

Complexity bounds in elimination theory – A survey

Pablo Solernó [1]

Departamento de Matemáticas, Fac. de Ciencias Exactas, Univ. de Buenos Aires, 1428 Buenos Aires, Argentina

Abstract

This paper is devoted to some last algorithmic progress in classical elimination theory from the complexity point of view. These results will be presented as a short survey (without proofs) treating essentially upper and lower bounds problems. The first aim of this paper is to show that the upper bounds results – as much progress as they may represent – seem not to solve satisfactorily the basic problems we are considering. On the other hand we shall also show how both the improvement of general algorithms and the research of lower bounds are related to certain mathematical tools as duality theory or arithmetic intersection theory.

Keywords: Complexity; Straight line program; Algebraic variety

1. Notations and definitions

1.1. Notations

Let k be an infinite and perfect field, $\bar{k}$ an algebraic closure of k and let $X_1, \ldots, X_n$ be indeterminates over k. By $\mathbb{A}^n := \mathbb{A}^n(\bar{k})$ we denote the n-dimensional affine space over $\bar{k}$ endowed with its Zariski topology. The inputs of the algorithms we are going to consider will be polynomials $F, F_1, \ldots, F_s \in k[X_1, \ldots, X_n]$ $(n \geqslant 2)$ where the total degrees $\deg F_j$ $(1 \leqslant j \leqslant s)$ are bounded by an integer $d \geqslant 2$.

We denote by $(F_1, \ldots, F_s)$ the ideal generated by $F_1, \ldots, F_s$ in $k[X_1, \ldots, X_n]$ and by $V := \{F_1 = 0, \ldots, F_s = 0\} := \{x \in \mathbb{A}^n; F_1(x) = \cdots = F_s(x) = 0\}$ the algebraic variety of $\mathbb{A}^n$ defined by these polynomials. Let $V = C_1 \cup \cdots \cup C_t$ be the decomposition of V in irreducible components. For $1 \leqslant j \leqslant t$ we define dimension and degree of C_j as usually and denote these quantities by $\dim C_j$ and $\deg C_j$. The dimension of V is defined as $\dim V := \max\{\dim C_j; 1 \leqslant j \leqslant t\}$ and its degree – less customarily – as $\deg V := \sum_j \deg C_j$ (see [19] for details).

[1] Département de Mathématiques, Université de Limoges, 123 Av. A. Thomas, F-87060 Limoges, France (till 31 July 1993). E-mail: psolerno@dm.uba.ar.

PII S0378-4754(96)00017-1

1.2. On the algorithmic models

The inputs of our algorithms (multivariate polynomials with coefficients in the ground field k) will be represented in three different ways: by all their coefficients (*dense representation*), by arithmetical circuits which allow their evaluations (*straight line program representation*) or by their nonzero coefficients (*sparse representation*). The algorithms use only arithmetical operations (addition, subtraction, multiplication, division), comparisons in k, selections of elements of k (associated to comparisons) and boolean operations (if $\mathrm{char}(k) = p > 0$ we shall also include as basic arithmetical operations the extraction of pth roots in k). Everyone of these algorithmic ground steps is counted at unit cost. Sometimes we shall also consider straight line programs in $k[X_1, \ldots, X_n]$ or in $k(X_1, \ldots, X_n)$. A suitable algorithmic model for our purpose is given by the notion of an arithmetical network over k ([15], see also [33,34] for precisions on straight line programs).

In order to compute the complexities of the algorithms we consider them as families of arithmetical networks parametrized by the quantities s, d, n (number of elements, maximal degree, number of variables) and others (length of straight line programs, sparsity) which measure the size of the polynomial input. Thus we obtain immediately two complexity measures: sequential time (network size) and parallel time (network depth). We consider these complexity measures as real-valued functions depending on the input parameters of the given problem and we try to analyze their asymptotic behavior.

1.3. Some basic problems

In order to illustrate the complexity results we shall consider some basic general algorithmic problems of algebraic geometry and commutative algebra:

(1) *The ideal triviality problem.* Decide whether $V = \emptyset$ holds and if this is the case find $P_1, \ldots, P_s \in k[X_1, \ldots, X_n]$ such that the identity $1 = P_1F_1 + \cdots + P_sF_s$ is satisfied.

(2) *The radical membership problem.* Decide whether F vanishes on V and if this is the case find $N \in \mathbb{N}$ and $P_1, \ldots, P_s \in k[X_1, \ldots, X_n]$ such that $F^N = P_1F_1 + \cdots + P_sF_s$ holds.

(3) *The ideal membership problem for complete intersections.* Suppose that $F_1, \ldots, F_s$ form a regular sequence of $k[X_1, \ldots, X_n]$. Decide whether F belongs to the ideal generated by $F_1, \ldots, F_s$ in $k[X_1, \ldots, X_n]$ and if this is the case find $P_1, \ldots, P_s \in k[X_1, \ldots, X_n]$ such that $F = P_1F_1 + \cdots + P_sF_s$ holds.

(4) *The zero-dimensional elimination problem.* Let Y be a given linear form of $k[X_1, \ldots, X_n]$. Compute $\dim V$ and if $\dim V = 0$ find a nonzero one-variate polynomial $Q \in k[Y]$ and n-variate polynomials $P_1, \ldots, P_s \in k[X_1, \ldots, X_n]$ such that $Q(Y) = P_1F_1 + \cdots + P_sF_s$ holds.

(5) *The general elimination problem.* Let $0 \leqslant m < n$ and let $\pi: \mathbb{A}^n \to \mathbb{A}^m$ be the projection map $\pi(x_1, \ldots, x_n) = (x_1, \ldots, x_m)$. Find polynomials $Q_1, \ldots, Q_t \in k[X_1, \ldots, X_m]$ and a quantifier free formula Φ in the first order language of fields with constants from k, involving only the polynomials $Q_1, \ldots, Q_t$ as basic terms, such that Φ defines the set $\pi(V)$.

2. The dense representation model

In this section we suppose that all polynomials occurring as inputs, outputs or intermediate results of our algorithms are given in *dense representation*: the data structure which represents a polynomial is supplied

with one unit of memory space for each possible coefficient in it; in other words we represent a polynomial $G \in k[X_1, \ldots, X_n]$ of degree at most δ by the vector of all its $\binom{\delta+n}{n}$ possible coefficients. Since $\binom{\delta+n}{n} \leqslant e\delta^n$, we observe that to the polynomial G corresponds in dense representation a data structure of size $O(\delta^n)$. In particular in problems (1)–(5) the input polynomials $F_1, \ldots, F_s$ are represented by a vector of total length $O(sd^n)$, the polynomial F by one of length $O((\deg F)^n)$ and the linear form Y by one of length n.

The quantities d, n, s are the natural parameters for the complexity of the algorithms considered in this section.

From a fundamental paper of Grete Hermann [23] one deduces that the problems (1)–(5) can be solved in *sequential time* which depends polynomially on $d, s, \deg F$ and in *doubly exponential* manner on the number of variables n of the problem. This result (shown by Hermann by means of classic elimination theory arguments) can also be obtained by rewriting techniques (Gröebner basis calculations).

The apparition in 1986 of a single exponential version of the affine Nullstellensatz in characteristic 0 by Brownawell [5] and its generalization for an arbitrary field in [6,7,27] is the essential tool which allows the obtention of more precise complexity bounds for (1)–(5):

An effective Nullstellensatz for ideal triviality. The ideal $(F_1, \ldots, F_s)$ is trivial iff there exist $P_1, \ldots, P_s \in k[X_1, \ldots, X_n]$ satisfying the conditions $1 = \sum_j P_j F_j$ and $\max_j\{\deg P_j F_j\} \leqslant d^n$.

A well-known example due to Mayr and Meyer [29] shows that the fact that one considers the membership problem for the polynomial 1 is essential for the single exponential nature of the problem. However the same kind of bounds can be obtained for an important particular case:

An effective Nullstellensatz for complete intersections. Suppose that $F_1, \ldots, F_s$ form a regular sequence in $k[X_1, \ldots, X_n]$. Then F belongs to $(F_1, \ldots, F_s)$ iff there exist polynomials $P_1, \ldots, P_s \in k[X_1, \ldots, X_n]$ such that $F = \sum_j P_j F_j$ and $\max_j\{\deg P_j F_j\} \leqslant \deg F + d^s \leqslant \deg F + d^n$ holds.

See [11] for a proof. Somewhat different versions of the effective Nullstellensatz for complete intersections and generalizations of it are contained in [1,3,8,32].

Let us also remark that the degree bounds of type d^n which appear in the quoted Nullstellensätze are almost optimal (see [5], where this fact is illustrated by an example due to Mora, Lazard, Masser and Philippon).

Joining these two Nullstellensätze with parallelizable algorithms for basic linear algebra (see [4,30]) one obtains the following theorem.

Theorem 1 ([11,13]). *There exist uniform algorithms (realized by uniform families of networks over k) which solve problems (1) and (4) in sequential time $s^{O(1)}d^{O(n^2)}$ and parallel time $O(n^4 \log^2 sd)$; problems (2) and (3) in sequential time $s^{O(1)}(\max\{d, \deg F\})^{O(n^2)}$ and parallel time $O(n^4 \log^2(s \max\{d, \deg F\}))$ and problem (5) in sequential time $s^{O(1)}d^{O((n-m)^2 m)}$ and parallel time $O((n-m)^4 m \log^2 sd)$.*

The statements of this theorem and their proofs are contained in the quoted papers [11,13] or can be easily deduced from their content. For the same type of complexity result concerning problem (5) by a somewhat different algorithm we refer to [24].

Let us mention that the complexity bounds of Theorem 1 are at present the best ones for *uniform* algorithms solving problems (1)–(5).

Observe also that the complexity bounds given in Theorem 1 are not polynomial in the size of the input

(essentially $O(sd^n)$ for the input size versus $s^{O(1)}d^{O(n^2)}$ for the complexity) and from this point of view, they are unsatisfactory algorithms.

On the other hand the problems (1)–(5) involve all polynomials in their outputs which may have degree of order $\Omega(d^n)$ (this is a consequence of the example of Mora, Lazard, Masser and Philippon mentioned before for the problems (1)–(4) and of Bezout's Theorem for (5)). Therefore the outputs of problems (1)–(5) may have size $\Omega(sd^{n^2})$ or at least size $\Omega(d^{n^2})$. This implies that the sequential time bounds of Theorem 1 are polynomial in the size of the output of problems (1)–(5) (recall that the output polynomials are given in dense representation).

An improvement of the order of complexity in Theorem 1 is therefore only possible if changing the data structure representing the polynomials we deal with.

In a first attempt to solve this problem one can think on representing the polynomials *sparsely*. Although considerable effort has been spent in this direction (see e.g. [18]) no result at present is known which connects in a satisfactory way sparse representation of polynomials with elimination theory. This may be due to the fact that the sparse representation of a polynomial may become dense when transforming the variables linearly.

A different efficient representation of polynomials without this defect is given by straight line programs (arithmetical circuits). This representation has been used in the past by several authors implicitly and explicitly (see e.g. [20,21,26]). It is crucial for the statements and their proofs in the next section.

3. A mixed model

3.1. A mixed model: dense representation and straight line programs

In Section 2 we explained the constraints of the dense representation in order to obtain "good" complexities for the problems (1)–(5). Unfortunately the simple change of the data structure "dense representation" by "straight line programs" does not seem to be the good solution. A factible intermediate answer is proposed by Giusti and Heintz [16]: roughly speaking, the inputs are considered in dense representation, the parameters agree with those of dense representation model (exceptionally some input polynomials are given by straight line programs with an upper bound for their lengths as a new parameter) and the output is a finite collection of straight line programs.

This model, although apparently somewhat artificial, seems to be well adapted to this kind of algorithms, where the variables play often the role of elements of the ground field (parameters). In fact, this model allows to solve problems (1)–(4) in "good time", i.e. polynomial in the input size.

3.2. Correct test sequences

A crucial point in algorithms treating with polynomial expressions is the "equality checking" between two polynomials which appear as intermediate results. Suppose for the moment that one wishes to know if an n-variate polynomial G with degree δ produced by a suitable arithmetical circuit is the zero polynomial. A straightforward procedure for this purpose consists in the succesive evaluation of the arithmetical circuit in the integer points of a box of cardinality $(\delta + 1)^n$ (interpolation) and is therefore exponential in the degree of G.

This main difficulty can be partially avoided by means of a fine result due to Heintz and Schnorr [21].

Let δ, L be nonnegative integers. We consider the set $W(\delta, n, L)$ of all polynomials in $k[X_1, \ldots, X_n]$ of degree bounded by δ which can be evaluated by an arithmetic circuit in $k(X_1, \ldots, X_n)$ of size bounded by L. Let $m \in \mathbb{N}$, we say that a sequence $\gamma := (\gamma_1, \ldots, \gamma_m)$ (where $\gamma_i \in k^n$ for $1 \leqslant i \leqslant m$) is a *correct test sequence for* $W(\delta, n, L)$ if the polynomial 0 is the unique polynomial of the set $W(\delta, n, L)$ that annihilates $\gamma_1, \gamma_2, \ldots$ and γ_m.

With these notations we have the following proposition.

Proposition 1 ([21, Theorem 4.4]). *Let $\Gamma \subset k$ be of cardinality $2L(\delta+1)^2$, $m := 6(L+n)(L+n+1)$ and note $\sigma(\delta, n, L, \Gamma)$ the subset of k^{nm} of all the correct test sequences of $W(\delta, n, L)$ contained in Γ^{nm}. Then the following inequality holds:*

$$(\#\Gamma)^{nm}\left(1-(\#\Gamma)^{-m/6}\right) \leqslant \#\sigma(\delta, n, L, \Gamma).$$

Suppose now that $G \in k[X_1, \ldots, X_n]$ is an arbitrary polynomial whose degree is bounded by δ and which can be computed by an arithmetical circuit in $k[X_1, \ldots, X_n]$ without divisions of size L and depth l. From the previous proposition one deduces the following corollary.

Corollary 1 ([14, Corollaire 2.1]). *There exists an arithmetical network over k of size $O(Lm) = O(L(L+n)^2)$ and depth $O(l)$ which decides if G is the polynomial zero. Moreover, this network can be constructed by a probabilistic algorithm in sequential time $O(L(L+n)^2)$ and parallel time $O(l)$; its failure probability is smaller than $\varepsilon = 1/262144$.*

Let us remark here some interesting consequences of these results for the algorithmic model:

- Proposition 1 guarantees the existence of at least one correct test sequence of size m which depends polynomially on the parameters (and not exponentially as in interpolation). Unfortunately no uniform polynomial time algorithm which produces correct test sequences is known up to now and this unsolved question gives the nonuniform character of the algorithms we will consider. However the construction of correct test sequences is absolutely independent of the type of the problem and depends only on the parameters; therefore if one knows a priori upper bounds for all the intermediate results in the algorithm, it is quite natural to consider the construction of the correct test sequences as a preprocessing, computed once for ever.
- Corollary 1 introduces a probabilistic algorithm (chosing randomly the correct test sequence) which unfortunately has a failure probability ($\varepsilon < \frac{1}{2}$): if one is interested in the application of this procedure in order to check if a given polynomial is zero, the answer NO is always true but YES involves a failure probability smaller than ε. In this sense the algorithm is more interesting than those of Monte Carlo type but it is not a Las Vegas algorithm (there are wrong answers). It produces random algorithms which solve the elimination problems (1)–(5) with a more precise model than those based in generic selections of parameters in Zariski open sets.

3.3. Upper bounds

In this section we present new results concerning upper complexity bounds for our list of problems (1)–(5). Proofs can be found in [14,16,17]. Throughout this section we shall suppose $d \geqslant n \geqslant 2$.

Let $V = \{F_1 = 0, \ldots, F_s = 0\}$ be the variety defined by the polynomials $F_1, \ldots, F_s$, which we think to be given in dense representation or alternatively by a division free straight line program of length L and depth l. Let $r := \dim V$.

We say that the variables $X_1, \ldots, X_n$ are in *Noether position* with respect to V if for each $r < i \leqslant n$ there exists a polynomial of $k[X_1, \ldots, X_r, X_i]$ which is monic in X_i and vanishes on V.

Theorem 2 ([16, Théorème 3.5 and Théorème 3.7.2]). *There exists an arithmetical network of size* $L' = s^{O(1)}L^{O(1)}d^{O(n-r)}$ *and depth* $l' = O((n-r)^2 \log^2 sd + l)$ *which computes the following items:*

(i) *the dimension* $r = \dim V$ *of the algebraic variety defined by* $F_1, \ldots, F_s$ *in* $\mathbb{A}^n$.

(ii) *a nonsingular* $n \times n$ *matrix* M *with entries from* k *such that the variables* $Y_1, \ldots, Y_n$ *which we obtain transforming* $X_1, \ldots, X_n$ *by means of* M, *are in Noether position with respect to* V.

There exists a random algorithm which constructs the arithmetical network above in sequential time L' *and parallel time* l'.

Theorem 2 implies that for $0 < s \leqslant n$ one can test in sequential time $L^{O(1)}d^{O(n-s)}$ and parallel time $O((n-s)^2 \log^2 d + l)$ whether the polynomials $F_1, \ldots, F_s$ form a regular sequence in $k[X_1, \ldots, X_n]$. This leads to the following result related to problem (3).

Theorem 3 ([14, Théorème 4.1 and Remarque 4.2.7.]). *Let* $0 < s \leqslant n$ *and suppose that for any index* $n - s \leqslant i < n$ *the polynomials* $F_1, \ldots, F_{n-i}$ *form a regular sequence and generate a radical ideal in* $k[X_1, \ldots, X_n]$. *Let* F *be represented by a division free straight line program in* $k[X_1, \ldots, X_n]$ *of length* L *and depth* l.

Then there exists an arithmetical network over k *of size* $L' := L^6(\deg F)^2 d^{O(s)}$ *and depth* $l' := O(l^2 \log(\deg F) s^7 \log^4 d)$ *which decides whether* F *belongs to the ideal. If this is the case, the network constructs a division free straight line program* β *in* $k[X_1, \ldots, X_n]$ *of length* $(L \deg F)^2 d^{O(s)}$ *and depth* $O(l^2 \log(\deg F) s^7 \log^4 d)$ *representing polynomials* $P_1, \ldots, P_s \in k[X_1, \ldots, X_n]$ *satisfying the following conditions:*

- $F = P_1F_1 + \cdots + P_sF_s$,
- $\max\{\deg P_1, \ldots, \deg P_s\} = (\deg F)d^{O(s)}$.

There exists a random algorithm which constructs the arithmetical network above in sequential time L' *and parallel time* l'.

Remark 1 ([31]). In fact, if $\mathrm{char}(k) = 0$ one obtains the more precise upper bound $3sd^s + d^{s-1} \max\{\deg F, d\}$ for the degrees of P_i $(1 \leqslant i \leqslant s)$ (also assuming that $(F_1, \ldots, F_s)$ is a regular ideal a similar bound holds for arbitrary characteristics).

From Theorems 2 and 3 and their proofs one infers a series of consequences which we formulate in subsequent propositions of this section.

Proposition 2 ([14, Théorème 5.2 and Proposition 5.2], see also [17]).

(i) *There exists an arithmetical network over* k *of size* $s^{O(1)}d^{O(n)}$ *and depth* $O(n^2 \log^2 sd)$ *which decides whether the ideal* $(F_1, \ldots, F_s)$ *is trivial. If this is the case the network constructs a division free straight line program* β *in* $k[X_1, \ldots, X_n]$ *which represents polynomials* $P_1, \ldots, P_s \in k[X_1, \ldots, X_n]$ *such that the following conditions are fulfilled:*

- *the length of* β *is* $s^{O(1)}d^{O(n)}$ *and its depth is* $O(n^2 \log^2 sd)$,
- *the polynomials* $P_1, \ldots, P_s$ *are of degree* $d^{O(n)}$ *and satisfy* $1 = P_1F_1 + \cdots + P_sF_s$.

(ii) *Increasing the depth in the statement* (i) *to* $O(n^{12} \log^9 sd)$ *an arithmetical network as above can be constructed by a random algorithm in sequential time* $s^{O(1)}d^{O(n)}$ *and parallel time* $O(n^{12} \log^9 sd)$.

Remark 2 ([31]). Refining the methods of [14] one obtains more precise upper bounds for the polynomials P_i: $4nd^n$ (if $\text{char}(k) = 0$) and $4n(d+1)^n$ (for all characteristics).

Remark 3. From Proposition 2 one deduces by Rabinowitsch's Trick the following fact: suppose that F is given in dense representation, one can decide whether F belongs to the radical of the ideal $(F_1, \ldots, F_s)$ in nonuniform time $L := s^{O(1)}(\max\{d, \deg F\})^{O(n)}$ and parallel time $l := O(n^2 \log^2(s \max\{d, \deg F\}))$. If this is the case one finds in sequential time L and parallel time l a natural number N of order $d^{O(n)}$ and a division free straight line program β in $k[X_1, \ldots, X_n]$ of length L and depth l which satisfies the following condition: β represents polynomials $P_1, \ldots, P_s \in k[X_1, \ldots, X_n]$ of degree $(\deg F)d^{O(n)}$ such that $F^N = P_1F_1 + \cdots + P_sF_s$ holds.

Proposition 3 ([16, Section 3.4.7 and Lemma 3.6.]). *There exists a random algorithm which constructs in sequential time* $s^{O(1)}d^{O(n)}$ *and in parallel time* $O(n^2 \log^2 sd)$ *the following items:*

- *a nonzero polynomial* $Q(Y) \in k[Y]$ *represented by its (dense) coefficient vector;*
- *a nonsingular matrix* M *which entries from* k *which transforms the variables* $X_1, \ldots, X_n$ *into new ones* $Y_1, \ldots, Y_n$*;*
- *polynomials* $G_1, \ldots, G_n$ *in the variables* $Y_1, \ldots, Y_n$ *given by their coefficients in sparse representation, such that* $Q(Y)$ *belongs to the ideal* $(F_1, \ldots, F_s)$*, the degree of the polynomials* $G_1, \ldots, G_n$ *is bounded by* $\deg V \leqslant d^n$ *and they form a reduced Gröbner basis of the radical of* $(F_1, \ldots, F_s)$ *with respect to the lexicographic monomial ordering* $Y_1 < \cdots < Y_n$.

Proposition 4. *Let* $0 \leqslant m < n$ *and let* $\pi: \mathbb{A}^n \to \mathbb{A}^m$ *be the canonical projection* $\pi(x_1, \ldots, x_n) = (x_1, \ldots, x_m)$*. We consider* $F_1, \ldots, F_s$ *as elements of* $k[X_1, \ldots, X_m][X_{m+1}, \ldots, X_n]$*, i.e. as polynomials in the variables* $X_{m+1}, \ldots, X_m$ *with coefficients which themselves are elements of* $k[X_1, \ldots, X_m]$*. We suppose that* $F_1, \ldots, F_s$ *are given with respect to the variables* $X_{m+1}, \ldots, X_n$ *in dense representation whereas their coefficients, being polynomials of* $k[X_1, \ldots, X_m]$*, are given by a division free straight line program in* $k[X_1, \ldots, X_m]$ *of length* L *and depth* l*. Then there exists an arithmetic network over* k *of size* $L' := L^2 s^{O(1)} d^{O(n-m)}$ *and depth* $l' := O(l + (n-m)^2 \log^2 sd)$ *which constructs a quantifier free formula* Φ *in the first order language of fields with constants from* k *such that the following conditions are satisfied:*

- *The terms contained in the formula* Φ *are polynomials of* $k[X_1, \ldots, X_m]$ *of degree* $d^{O(n-m)}$ *represented by a division free straight line program in* $k[X_1, \ldots, X_m]$ *of length* L' *and depth* l'.
- Φ *defines the projection set* $\pi(V)$.

The arithmetic network above can be constructed by a probabilistic Monte Carlo algorithm in sequential time L' *and parallel time* l'.

A proof of Proposition 4 in the nonuniform complexity model is implicitly contained in [16].

The next proposition illustrates a general duality existing between the number of variables n and the number of equations s in problems (1)–(5).

Proposition 5 ([2]). *There exist random algorithms which determine the dimension of the variety V in sequential time $s^{O(1)}d^{O(n)}$ and parallel time $O(n^2 \log^2 sd)$ or in sequential time $L^{O(1)}(nd)^{O(s)}$ and parallel time $O(s^2 \log^2 nd + l)$.*

4. Some relative lower bounds

In this section we discuss whether it is possible to obtain polynomial sequential complexity results when we represent the input polynomials $F_1, \ldots, F_s$ by straight line programs or when we give them in sparse representation. All proofs can be found in [20].

4.1. The $\mathcal{U}$-resultant

For the moment let $U_0, \ldots, U_n$ and X_0 be new indeterminates and let $G_1, \ldots, G_s$ be homogeneous polynomials of $k[X_0, \ldots, X_n]$ of degree at most d defining a projective variety W of dimension zero. We recall main properties of the $\mathcal{U}$-resultant R of $(G_1, \ldots, G_s)$:

- $R \in k[U_0, \ldots, U_n]$;
- $\deg R = \deg(G_1, \ldots, G_s) \leqslant d^n$;
- for any point $(u_0, \ldots, u_n) \in \mathbb{A}^{n+1}$ the projective variety defined by the forms $G_1, \ldots, G_s, u_0X_0 + \cdots + u_nX_n$ is nonempty iff $R(u_0, \ldots, u_n) = 0$;
- if $s = n$ then R is the ordinary resultant of the homogeneous polynomials $G_1, \ldots, G_n, U_0X_0 + \cdots + U_nX_n$ with respect to the variables $X_0, \ldots, X_n$.

For more details on $\mathcal{U}$-resultants and ordinary resultants we refer to [10; 25; 35, Kapitel 11, Section 79]

The improved complexity bounds in the last section are all based on the following fundamental result essentially due to Lazard (see [10,16,28]).

Proposition 6. *The $\mathcal{U}$-resultant of the homogeneous ideal $(G_1, \ldots, G_s)$ in the polynomial ring $k[X_0, \ldots, X_n]$ can be evaluated by a division free straight line program β in $k[U_0, \ldots, U_n]$ of length $s^{O(1)}d^{O(n)}$ and depth $O(n^2 \log^2 sd)$. The nonscalar depth of β is $O(n \log d)$. The circuit β can be constructed from the input $G_1, \ldots, G_s$ (which is given in dense representation) in uniform sequential time $s^{O(1)}d^{O(n)}$ and parallel time $O(n^2 \log^2 sd)$. The nonscalar parallel time of the algorithm is $O(n \log d)$. If k is the field of rational numbers $\mathbb{Q}$ then the binary length of the parameters used during the procedure is of order $O(nt \log d)$, where t denotes the maximal binary length of the coefficients of $G_1, \ldots, G_s$.*

Let us observe that Proposition 9 entails a (partial) answer for the projective version of problem (4).

In [20] the following lower bound result for the evaluation of the $\mathcal{U}$-resultant is obtained.

Proposition 7. *Let $G_1, \ldots, G_s$ be given by a well parallelizable straight line program of length L. If there exists a* uniform *well parallelizable algorithm which is polynomial in L and n and which constructs a division free straight line program in $k[U_0, \ldots, U_n]$ of the same complexity class for the evaluation of the $\mathcal{U}$-resultant of the homogeneous ideal generated by $G_1, \ldots, G_s$, then $P = NP$ holds.*

4.2. The zero-dimensional elimination problem

Proposition 8. *Let $k := \mathbb{Q}(Z_{ij};\ 1 \leqslant i, j \leqslant n)$ and let the polynomials $F_1, \ldots, F_s$ in the ring $k[X_1, \ldots, X_n]$ be given by a division free straight line program in $k[X_1, \ldots, X_n]$ of length L. Suppose that there exists an arithmetic network of size $(Ln)^{O(1)}$ which uses only parameters from $\mathbb{Q}$ and which solves the affine zero-dimensional elimination problem (problem (4)) for any input $F_1, \ldots, F_s$ in the following way: if the algebraic variety defined by $F_1, \ldots, F_s$ is zero-dimensional, the network produces a monotone division free straight line program β in $k[Y]$ of length $(Ln)^{O(1)}$ which represents the (unique) monic polynomial $Q(Y)$ of minimal degree which belongs to $(F_1, \ldots, F_s)$.*
Then the $n \times n$-permanent over $\mathbb{Q}$ can be evaluated by an arithmetic circuit of length $n^{O(1)}$.

4.2.1. A difficult zero-dimensional elimination problem

Theorem 4 ([20, Theorem 18 and Theorem 19]). *Let $F_1 := X_1^2 - X_1, \ldots, F_n := X_n^2 - X_n$, $F_{n+1} := Y^2 - \sum_{1 \leqslant i \leqslant n} 2^{i-1} X_i$, $F_{n+2} := Y$ and $V_n := \{F_1 = 0, \ldots, F_n = 0, F_{n+1} = 0, F_{n+2} \geqslant 0\}$. We consider the family $(\{F_1, \ldots, F_{n+2}\})_{n \in \mathbb{N}}$ of sets of polynomials $F_1, \ldots, F_{n+2} \in \mathbb{Q}[X_1, \ldots, X_n, Y]$ and the family $(V_n)_{n \in \mathbb{N}}$ of semialgebraic subsets V_n of $\mathbb{R}^{n+1}$. Let $\pi_n := \mathbb{R}^{n+1} \to \mathbb{R}$ be the projection map $\pi_n(x_1, \ldots, x_n, y) = y$.*

Denote by Q_n the unique monic polynomial of $\mathbb{R}[Y]$ of minimal degree which defines $\pi_n(V_n)$.

Then the polynomials $F_1, \ldots, F_{n+2}$ can be represented by a division free straight line program in $\mathbb{Q}[X_1, \ldots, X_n, Y]$ of length $O(n)$ and depth $O(1)$.

However, any algorithm which produces a division free straight line program in $\mathbb{R}[Y]$ evaluating the polynomial Q_n needs sequential time $\Omega\left(2^{n/2}/n\right)$ and parallel time $\Omega(n)$ for the representation of the output.

Let us remark that in the formulation of the example of Theorem 19 of [20] the output is given exactly by the polynomial Q_n of minimal degree while the usual output of a quantifier elimination procedure applied to the obvious formula defining V_n would be the quantifier formula ψ_n in the first order language of ordered fields given by $(P(Y^2) = 0 \wedge Y > 0)$, where $P = \prod_{0 \leqslant j < 2^n} (Y - \sqrt{j})$.

Remark 4. Suppose for the moment that the family of polynomials $(\prod_{0 \leqslant j < d} (Y - j))_{d \in \mathbb{N}}$ is hard to evaluate (up to now this remains an open question). Then either the zero-dimensional elimination problem (problem (4)) is hard to solve for $k = \mathbb{Q}$ and $\bar{k} = \mathbb{C}$ when inputs and outputs are given by division free straight line programs, or greatest common divisor computations of univariate polynomials given in the same way are difficult.

References

[1] F. Amoroso, Test d'appartenance d'après un théorème de Kollár, C. R. Acad. Sci. Paris Sér. I 309 (1989) 691–694.
[2] I. Armendáriz, La complejidad del cálculo de la dimensión de una variedad algebraica, Master Thesis, Universidad de Buenos Aires, 1992.
[3] C. Berenstein and A. Yger, Bounds for the degrees in the division problem, Michigan Math. J. 37 (1990) 25–43.
[4] S.J. Berkowitz, On computing the determinant in small parallel time using a small number of processors, Inform. Process. Lett. 18 (1984) 147–150.
[5] W.D. Brownawell, Bounds for the degrees in the Nullstellensatz, Ann. Math. (Second Series) 126 (3) (1987) 577–591.
[6] L. Caniglia, A. Galligo and J. Heintz, Borne simple exponentielle pour les degrés dans le théorème des zéros sur un corps de caractéristique quelconque, C. R. Acad. Sci. Paris Sér. I 307 (1988) 255–258.

[7] L. Caniglia, A. Galligo and J. Heintz, Some new effectivity bounds in computational geometry, in: T. Mora, ed., Proc. 6th Internat. Conf. Applied Algebra, Algebraic Algorithms and Error Correcting Codes AAECC–6 (Rome, 1988) Lecture Notes in Computer Science 357 (Springer, Berlin, 1989) 131–151.
[8] L. Caniglia, J.A. Guccione and J.J. Guccione, Local membership problems for polynomial ideals, in: T. Mora and C. Traverso, eds., Effective Methods in Algebraic Geometry MEGA 90, Progress in Mathematics, Vol. 94 (Birkhäuser, Basel, 1991) 31–45.
[9] J. Canny, Some algebraic and geometric computations in PSPACE, in: Proc. 20th Ann. ACM Symp. Theory of Computing (1988) 460–467.
[10] J. Canny, Generalized characteristic polynomials, in: P. Gianni, ed., Proc. Internat. Symp. on Symbolic and Algebraic Computation ISSAC'88 (Roma, 1988) Lecture Notes in Computer Science 358 (Springer, Berlin, 1989) 293–299.
[11] A. Dickenstein, M. Giusti, N. Fitchas and V. Sessa, The membership problem for unmixed polynomial ideals is solvable in single exponential time, Discrete Appl. Math. 33 (1991) 73–94.
[12] N. Fitchas and A. Galligo, Nullstellensatz effectif et conjecture de Serre (théorème de Quillen–Suslin) pour le Calcul Formel, Math. Nachr. 149 (1990) 231–253.
[13] N. Fitchas, A. Galligo and J. Morgenstern, Precise sequential and parallel complexity bounds for the quantifier elimination over algebraically closed fields, J. Pure Appl. Algebra 67 (1990) 1–14.
[14] N. Fitchas, M. Giusti and F. Smietanski, Sur la complexité du théorème des zéros, Preprint Ecole Polytechnique Palaiseau, 1992.
[15] J. von zur Gathen, Parallel arithmetic computations: a survey, in: Proc. 13th Conf. MFCS, Lecture Notes in Computer Science 233 (Springer, Berlin, 1986) 93–112.
[16] M. Giusti and J. Heintz, La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial, in: Proc. Internat. Meeting on Commutative Algebra, Cortona, 1991, To appear.
[17] M. Giusti, J. Heintz and J. Sabia, On the efficiency of effective Nullstellensätze, Computational Complexity, To appear.
[18] D. Grigor'ev, M. Karpinski and M. Singer, The interpolation problem for k-sparse sums of eigenfunctions of operators, Research Report 8538–CS, Universität Bonn, 1989.
[19] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theoret. Comput. Sci. 24 (1983) 239–277.
[20] J. Heintz and J. Morgenstern, On the intrinsic complexity of elimination theory, Depart. de Mat. y Estad. Comput., Universidad de Cantabria No.2, 1993.
[21] J. Heintz and C.P. Schnorr, Testing polynomials which are easy to compute, in: Proc. 12th Ann. ACM Symp, Theory of Computing (1980) 262–280.
[22] J. Heintz and M. Sieveking, Absolute primality of polynomials is decidable in random polynomial time in the number of variables, in: S. Even and O. Kariv, eds., Proc. 8th Colloquium on Automata, Languages and Programming ICALP 81 (Akko, 1981) Lecture Notes in Computer Science 115 (Springer, Berlin, 1981) 16–28.
[23] G. Hermann, Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, Math. Ann. 95 (1926) 736–788.
[24] D. Ierardi, Quantifier elimination in the theory of an algebraically-closed field, in: Proc. 21st Ann. ACM Symp. Theory of Computing (1989) 138–147.
[25] J.P. Jouanolou, Le formalisme du résultant, Preprint IRMA, Université de Strasbourg, 1990.
[26] E. Kaltofen, Greatest common divisors of polynomials given by straight line programs, J. ACM 35 (1) (1988) 234–264.
[27] J. Kollár, Sharp effective Nullstellensatz, J. AMS 1 (1988) 963–975.
[28] D. Lazard, Résolution des systèmes d'équations algébriques, Theoret. Comput. Sci. 15 (1981) 77–110.
[29] E. Mayr and A. Meyer, The complexity of the word problem for commutative semigroups and polynomial ideals, Adv. in Math. 46 (1982) 305–329.
[30] K. Mulmuley, A fast parallel algorithm to compute the rank of a matrix over an arbitrary field, in: Proc. 18th Ann. Symp. Theory of Computing (1986) 338–339.
[31] J. Sabia and P. Solernó, A bound for the trace in complete intersections and the degrees in the Nullstellensatz, Preprint, 1993.
[32] B. Shiffman, Degree bounds for the division problem in polynomial ideals, Michigan Math. J. 36 (1989) 163–171.
[33] H.-J. Stoss, On the representation of rational functions of bounded complexity, Theoret. Comput. Sci. 64 (1989) 1–13.
[34] V. Strassen, Berechnung und Programm I, Acta Inform. 1 (1972) 320–334.
[35] B.L. van der Waerden, Moderne Algebra, Vol II (Springer, Berlin, 1940).