On the intrinsic complexity of elimination theory

Joos Heintz, Jacques Morgenstern

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

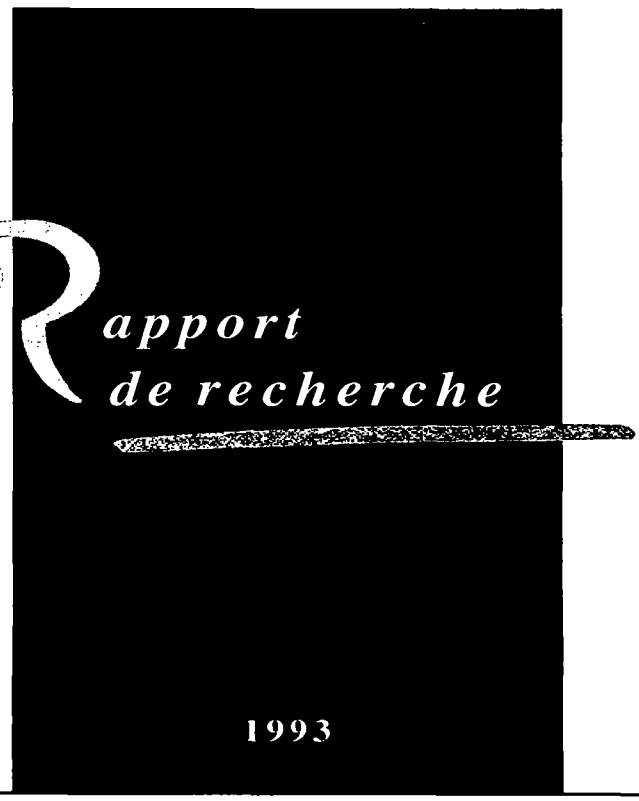
On the intrinsic complexity of elimination theory

Joos HEINTZ
Jacques MORGENSTERN

N° 1923
MAI 1993

PROGRAMME 2

Calcul symbolique,
programmation
et génie logiciel



On the Intrinsic Complexity of Elimination Theory.

Sur la complexité intrinsèque de l'élimination

Joos HEINTZ
Departemento de Matemàticas
Estadística y Computación
Faculdad de Ciencias
Universidad de Cantabria
E-39071 Santander,España

Jacques MORGENSTERN
Projet SAFIR
INRIA Sophia Antipolis,I3S
06560 Valbonne,France

On the Intrinsic Complexity of Elimination Theory

JOOS HEINTZ* and JACQUES MORGENSTERN**

Dedicated to John Traub for his 60th birthday and to Claude Labro

Abstract

We consider the intrinsic complexity of selected algorithmic problems of classical elimination theory in algebraic geometry. The inputs and outputs of these problems are given by finite sets of polynomials which we represent alternatively in dense forme or by straight line programs

We begin with an overview on the known upper bounds for the sequential and parallel time complexity of these problems and show then that in the most important cases these bounds are tight. Our lower bound results include both the relative and the absolute viewpoint of complexity theory. On one side we give reductions of fundamental questions of elimination theory to NP- and $P^{\#}$ - complete problems and on the other side we show that some of these questions may have exponential size outputs. In this way we confirm the intrinsically exponential character of algorithmic problems in elimination theory whatever the type of data structure may be.

Résumé

Nous considérons la complexité intrinsèque d'un certains nombre de problèmes algorithmiques de l'élimination classique provenant de la géométrie algébrique. Les entrées et les sorties sont données ici par des ensembles finis de polynômes en plusieurs variables qui seront représentés soit sous forme dense soit par des programmes directs d'évaluation.

*Departamento de Matemáticas, Estadística y Computación. Facultad de Ciencias, Universidad de Cantabria. E-39071 Santander, España. heintz@ccucvx.unican.es

**Projet SAFIR, INRIA, rue des Lucioles, et I3S, Université de Nice, Sophia Antipolis, F-06560 Valbonne, France. morgenstern@sophia.inria.fr

Nous commençons par un exposé sur les majorations connues des complexités séquentielle et parallèles de ces problèmes et nous montrons que dans les cas essentiels ces majorations sont optimales. Nos résultats sur les minorations sont relatives ou absolues. D'une part nous montrons la réduction de questions fondamentales de la théorie de l'élimination à des problèmes NP- et $P^{\#}$ - completset, d'autre part nous montrons que certaines de ces questions ont des sorties exponentielles. Nous confirmons ainsi le caractère intrinsèquement exponentiel de la complexité de problèmes algorithmiques dans la théorie de l'élimination indépendemment de la structure de données choisie.

Key words. elimination theory, algebraic variety, complexity, arithmetical network, straight line program, uniform algorithm, random algorithm.

0. Introduction

Let us start this paper with a short account of some selected problems and recent results concerning the complexity of algorithms in classical algebraic geometry and commutative algebra. These results will be presented in expository manner in the form of a short survey, since proofs may be found elsewhere. The aim of this paper is to show that these results – as much progress as they may represent – are not solutions of the basic problems we are considering and which are all closely related to classical elimination theory in algebraic geometry.

We shall give evidence that this lack of genuine solutions has objective reasons which resist the power of positive thinking in modern science. Thus instead of fortifying Thebes playing lyre like Zethos, we follow rather the example of the trumpets of Jericho with respect to the so called Calcul Formel/Computer Algebra.

Throughout this paper we shall maintain the notations which follow now. Let k be an infinite and perfect field, $\overline{k}$ an algebraic closure of k and let $X_1, \ldots, X_n$ be indeterminates over k. By $\mathbf{A}^n := \mathbf{A}^n(\overline{k})$ we denote the n-dimensional affine space over $\overline{k}$ endowed with its Zariski topology. We suppose that polynomials $F, F_1, \ldots, F_s$ and a nonzero linear form Y of $k[X_1, \ldots, X_n]$ are given. Let d be an upper bound for the degrees of $F_1, \ldots, F_s$. In the sequel we shall suppose that the parameters d, s, n are fixed subject to the condition $d \geq 2$ and $n \geq 2$. Similarly, we think the polynomials $F, F_1, \ldots, F_s$ with $d \geq \max\{\deg F_1, \ldots, \deg F_s\}$ and the linear form Y of $k[X_1, \ldots, X_n]$ as given inputs of the algorithmic problems we are going to consider (here $\deg G$ denotes the total degree of the polynomial $G \in k[X_1, \ldots, X_n]$).

Let $V := \{F_1 = 0, \ldots, F_s = 0\} := \{x \in \mathbf{A}^n ; F_1(x) = \ldots = F_s(x) = 0\}$ the algebraic subvariety of $\mathbf{A}^n$ defined by the polynomials $F_1, \ldots, F_s$. Let $V = C_1 \cup \ldots \cup C_t$ its decomposition in irreducible components. For $1 \leq j \leq t$ we define dimension and degree of C_j as usually and denote these quantities by $\dim C_j$ and $\deg C_j$. Then the dimension of V is defined as $\dim V := \max\{\dim C_j ; 1 \leq j \leq t\}$ and its degree –less customarily– as $\deg V := \sum_{1 \leq j \leq t} \deg C_j$ (see [He 83] for details).

We denote the cardinality of a set M by $\#M$ and we write log for the

logarithm to the the base 2.

We consider the following fundamental algorithmic problems of algebraic geometry and commutative algebra:

(i) *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.

(ii) *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.

(iii) *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.

(iv) *the (affine) zero dimensional elimination problem.* 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.

(v) *the general case of the elimination problem.* Let $0 \leq m < n$ and $\pi : \mathbf{A}^n \to \mathbf{A}^m$ the projection map defined by $\pi(x_1, \ldots, x_n) = (x_1, \ldots, x_m)$ for $(x_1, \ldots, x_n) \in \mathbf{A}^n$. The main problem of algorithmic elimination theory can be formulated as follows: 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 $\pi(V)$.

We would like to solve the problem (i)–(v) algorithmically by using only arithmetical operations (addition, substraction, multiplication, division), comparisons in k, selectors of elements of k (associated to comparisons) and boolean operations. If the characteristic of k is positive, say p, we shall also include the extraction of p-th roots in k in our list of basic arithmetical operations. Everyone of these algorithmic ground steps is counted at unit cost. We shall also include straight line programs (arithmetical circuits) in $k[X_1, \ldots, X_n]$ or in $k(X_1, \ldots, X_n)$ into our considerations. A suitable algorithmic model for

our purpose is given by the notion of an arithmetical network over k. ([vz Ga 86]. See also [Stra 72], [Sto 89] or [He 89] for precisions on straight line programs.)

We shall think our algorithms as families of arithmetic networks parametrized by the quantities s, d, n and others which measure the size of the input given by $F, F_1, \ldots, F_s$ and Y. 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 analyse their asymptotic behavior. All statements in our algorithmic model will be transferable mutatis mutandis to boolean networks and circuits but for expository reasons we shall not insist on this point.

For more details concerning our algorithmic model we refer to [Gi-He 91] and [Fi-Gi-Smi 92]. In this introductory section we suppose that all polynomials occurring as inputs, outputs or intermediate results of our algorithms are given in dense representation. That means that we associate upper bounds for the number of variables and the degree with any polynomial. The data structure which represents the polynomial is supplied with one unit of memory space for each possible coefficient in it. In other words we represent a polynomial $F \in k[X_1, \ldots, X_n]$ of degree almost δ by the vector of all is $\binom{\delta+n}{n}$ possible coefficients. Let us observe that there is a constant, namely the number e, such that $\binom{\delta+n}{n} \leq e\delta^n$ holds. Thus to F there corresponds in dense representation a data structure of size $O(\delta^n)$ (which is given by a vector with entries from k of the same length). In particular, 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.

¿From classical elimination theory one infers immediately that the problems (i)–(v) are all algorithmically solvable in primitive recursive sequential and parallel time (i.e. by means of uniform families of arithmetic networks over k whose size and depth depends in a primitive recursive way on d, s, n and possibly on the degree of F).

¿From a fundamental paper of Grete Hermann (1926) ([Her 26]) one de-

duces even more: the problems (i)–(v) can be solved in sequential time which depends polynomially on $d, s, \deg F$ and (or however) in doubly exponential manner on n, the number of the variables of the problem. The parallel time is polylogarithmic in $d, s, \deg F$ and depends in singly exponential way on n. Since in our model parallel time can easily be translated into working space (see [Ba-Dí-Ga 90], Theorem 4.2), this result means that the problems (i)–(v) can be solved within in singly exponential space (see [He 83] and [Fi-Ga-Mo 90a] for details concerning proof methods).

Let us also mention that the problems (i)–(v) can be solved in the same order of sequential time by means of rewriting techniques (Gröbner basis computations). This is due to a fundamental result on the complexity of Gröbner basis calculations (see [Gi 84], [Du 90], [Kri-Lo 91]). A detailed account of Gröbner basis algorithms and their applications can be found in [Bu 85].

Although there was some evidence that the problems (i)–(v) admit a more precise complexity analysis (see [Chi-Gri 83] and [Gri 87]) the mentioned time bounds were the best ones known until 1987.

Progress was only made when so called effective (affine) Nullstellensätze appeared for the first time ([Bro 87], [Ca-Ga-He 88], [Ca-Ga-He 89], [Ko 88]. See also [Ber-Yg 91] and [Ber-Yg 90]).

We quote here two typical examples of such effective Nullstellensätze. We put for the moment $d := \max\{\deg F_j : 1 \leq j \leq s\}$ and suppose $d > 2$ and $n > 1$. We denote the ideal generated by $F_1, \ldots, F_s$ in $k[X_1, \ldots, X_n]$ by $(F_1, \ldots, F_s)$.

<u>*An effective Nullstellensatz for ideal triviality.*</u>

The ideal $(F_1, \ldots, F_s)$ is trivial iff there exist polynomials $P_1, \ldots, P_s \in k[X_1, \ldots, X_n]$ satisfying the conditions $1 = \sum_{1 \leq j \leq s} P_j F_j$ and $\max\{\deg P_j F_j ; 1 \leq j \leq s\} \leq d^n$.

<u>*An effective Nullstellensatz for complete intersections.*</u>

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 $F = \sum_{1 \leq j \leq s} P_j F_j$ and $\max\{\deg P_j F_j : 1 \leq j \leq s\} \leq \deg F + d^s \leq \deg F + d^n$ holds.

For elementary proofs of these Nullstellensätze see [Phi 88], [Fi-Ga 90], [Di-Fi-Ga-Se 91], [Ca-Gu-Gu 91]. Somewhat different versions of the effective Nullstellensatz for complete intersections and generalisations of it are contained in [Ber-Yg 90], [Shi 89], [Ca-Gu-Gu 91], [Am 89].

We remark also that the degree bounds of type d^n which appear in the quoted Nullstellensätze are almost optimal (see [Bro 87], where this fact is illustrated by an example due to Mora, Lazard, Masser and Philippon). These two Nullstellensätze are the basic tool to the following attempt to solve problems (i)–(v).

THEOREM 1 ([Di-Fi-Gi-Se 91], [Fi-Ga-Mo 90a,b]). *There exist uniform algorithms (realized by uniform families of networks over k) which solve problems (i), (iv) in sequential time $s^{O(1)}d^{O(n^2)}$ and parallel time $O(n^4 \log^2 sd)$, problems (ii), (iii) 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 (v) 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 [Di-Fi-Gi-Se 91] and [Fi-Ga-Mo 90a,b] or can be easily deduced from their content. For the same type of complexity result concerning problem (v) by a somewhat different algorithm we refer to [Ie 89]. A first solution of problems (i), (ii) and (iv) with slightly weaker bounds is contained in [Ca-Ga-He 89].

Let us also mention that the complexity bounds of Theorem 1 are at present the best ones for *uniform* algorithms solving problems (i)–(v). In particular Theorem 1 implies that these problems are all in P–space.

Let us observe that the problems (i)–(v) involve all polynomials in their outputs. The polynomials of the outputs of problems (i)–(iv) may have degree of order $\Omega(d^n)$. This is a consequence of the example of Mora, Lazard, Masser and Philippon mentioned before. The same is true for problem (v) as a consequence of Bezout's Theorem. Therefore the outputs of problems (i)–(v) 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 (i)–(v) (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 we change the data structure representing the polynomials we deal with.

In a first attempt to solve this problem one could think on representing the polynomials sparsely. Although considerable effort has been spent in this direction (see e.g. [Gri-Kar-Si 89]) 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. However transforming variables is crucial for almost all common techniques of manipulating polynomials in algebraic geometry and commutative algebra. A different efficient representation of polynomials without this defect is given by straight time programs (arithmetical circuits). This representation has been used in the past by several authors implicitely and explicitely (see e.g. [He-Schn 82], [He-Sie 81], [Ka 88]). It is crucial for the statements and their proofs in the next section.

Let us finally observe that the representation of polynomials by straight line programs generalizes the sparse one since every sparse polynomial of not to high degree can be evaluated fast.

2. Sharp upper bounds for algorithmic problems in elimination theory.

In this section we present and comment still unpublished results concerning upper complexity bounds for our list of problems (i)–(v). Proofs can be found in the papers [Gi-He 91], [He-Gi-Sa 91] and [Fi-Gi-Smi 92].

Throughout this section we shall suppose $d \geq n \geq 2$.

Let $V = \{F_1 = 0, \ldots, F_s = 0\}$ be the closed subvariety of $\mathbf{A}^n$ 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 $r := \dim V$ be the dimension of V. Thus $n - r$ is the codimension of V.

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

Our basic results are contained in the following two theorems.

THEOREM 2 ([Gi-He 91], Théorème 3.5 and Théorème 3.7.2]). *There exists a random algorithm which computes in sequential time* $s^{O(1)}L^{O(1)}d^{O(n-r)}$ *and parallel time* $O((n-r)^2\log^2 sd + \ell)$ *the following items:*

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

(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.

We remark here that the statement of this theorem is not circular. The algorithm stops spontaneously after $s^{O(1)}L^{O(1)}d^{O(n-r)}$ sequential and $O((n-r)^2\log^2 sd + \ell)$ parallel steps without knowing in advance what the dimension r of V is. Of course we have the rough estimates $s^{O(1)}L^{O(1)}d^{O(n-r)} = s^{O(1)}d^{O(n)}$ and $O((n-r)^2\log^2 sd + \ell) = O(n^2\log^2 sd)$. In fact $s^{O(1)}d^{O(n)}$ and $O(n^2\log^2 sd)$ are the bounds appearing in the corresponding [Gi-He 91], Théorème 3.5 and Théorème 3.7.2. This coarser complexity result is shown in the mentioned paper with reference to the model of nonuniform algorithms. Our refinement of the bounds follows by simple inspection of the proofs in [Gi-He 91]. In the same way one obtains a restatement of this nonuniform result in terms of probabilistic (random) algorithms.

Theorem 2 implies that for $0 < s \leq n$ one can test in sequential time $L^{O(1)}d^{O(n-s)}$ and parallel time $O((n-s)^2\log^2 d + \ell)$ by a random algorithm 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.

THEOREM 3 ([Fi-Gi-Smi 92], Theorem 4.1 and Remark 3.2.7.). *Let* $0 < s \leq n$ *and suppose that for any index* $n-s \leq i < n$ *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 arithmetic network over k *of size* $L' := L^6(\deg F)^2 d^{O(s)}$ *and depth* $\ell' := O(\ell^2\log(\deg F)s^7\log^4 d)$ *which decides whether* F *belongs*

to the ideal $(F_1, \ldots, F_s)$. *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* $O(\ell^2 \log(\deg F) s^7 \log^4 d)$ *which represents polynomials* $P_1, \ldots, P_s \in k[X_1, \ldots, X_n]$ *satisfying the following conditions:*

- $F = P_1 F_1 + \cdots + P_s F_s$
- $\max\{\deg P_1, \ldots, \deg P_s\} = (\deg F) d^{O(s)}$.

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

¿From $d^{O(s)} = d^{O(n)}$ we deduce as before the estimates $L' = L^6 (\deg F)^2 d^{O(n)}$ and $\ell' = O(\ell^2 \log(\deg F) n^7 \log^4 d)$. This is the way how the theorem above is presented in [Fi-Gi-Smi 92].

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

PROPOSITION 4 ([Fi-Gi-Smi 92], Théorème 4.2 and Proposition 4.2. See also [Gi-He-Se 91]).
(i) There exists an arithmetic 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* $1 = P_1 F_1 + \cdots + P_s F_s$.

(ii) Increasing the depth in the statement (i) to $O(n^{12} \log^9 sd)$ *an arithmetic 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 5. From Proposition 4 one deduces by Rabinowitsch's Trick the following fact: suppose that F is given in dense representation. In non-uniform time $L := s^{O(1)} (\max\{d, \deg F\})^{O(n)}$ and parallel time $\ell := O(n^2 \log^2 (s \max\{d, \deg F\}))$ one can decide whether F belongs to the radical of the ideal $(F_1, \ldots, F_s)$. If this is the case one finds in sequential time L and parallel time 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 6 ([Gi-He 91], Section 3.4.7 and Lemma 3.6. See also [Fi-Gi-Smi 92], Proposition 1.3). *There exists a random algorithm which constructs in sequential time $s^{O(1)}d^{O(n)}$ and parallel time $O(n^2 \log^2 sd)$ the following items:*

- *a non zero polynomial $Q(Y) \in k[Y]$ represented by its (dense) coefficient vector*
- *a non singular 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 the following conditions are satisfied:*

  (i) $Q(Y)$ belongs to the ideal $(F_1, \ldots, F_s)$

  (ii) the degree of the polynomials $G_1, \ldots, G_n$ is bounded by $\deg V \leq d^n$

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 7. *Let $0 \leq m < n$ and let $\pi : \mathbf{A}^n \to \mathbf{A}^m$ the canonical projection defined by $\pi(x_1, \ldots, x_n) = (x_1, \ldots, x_m)$ for $(x_1, \ldots, x_n) \in \mathbf{A}^n$. 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 $O(\ell + (n-m)^2 \log^2 sd)$ 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 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 this proposition in the non-uniform complexity model is implicitely contained in [Gi-He 91].

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

PROPOSITION 8 ([Ar 92]). *There exist random algorithms which determine the dimension $\dim V$ 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 $O(s^2 \log^2 nd + \ell)$.*

Let us remark that the duality principle expressed in Proposition 8 unifies in the context of algebraic geometry over algebraically closed fields basic results of the real case contained in [Gri-Vo 88], [Can 88a], [He-Ro-So 90], [Ren 92] and [Bar 91].

Proposition 8 is a straightforward consequence of Theorem 2. One has simply to observe that s is an upper bound for the codimension $n - r$ of V. The sequential complexities appearing in Proposition 8 are polynomial in d but singly exponential in n or in s. This observation may also be made with respect to Remark 5, Proposition 6 and Proposition 7 which can be restated in this way. We ask therefore whether the singly exponential dependency of our sequential complexity bounds on n or on s is intrinsic for problems (i)–(v). We shall consider this question in the next two sections.

In Proposition 4(i), Remark 5 and Proposition 6 we find sequential time bounds of order $s^{O(1)}d^{O(n)}$ and parallel time bounds of order $O(n^2 \log^2 sd)$. Here all arithmetical operations are considered. If one counts only the essential multiplications and divisions in the underlying algorithms (i.e. k–linear operations are free) one obtains a parallel time bound of $O(n \log sd)$, whereas the order of the sequential complexity remains unchanged. We call this complexity measure the nonscalar one. Thus the nonscalar parallel time of our algorithms

is in general of type $O(n \log sd)$. This observation applies mutatis mutandis also to Theorem 2 and Propositions 7 and 8.

An algorithm realized by a family of arithmetical networks over k is called well parallelizable if the parallel complexity is of order $\log^2$ of the sequential complexity of the algorithm and if the nonscalar parallel complexity is of order log of the same quantity.

2. Relative lower bound results.

In this and the next section we ask 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. (In the precedent two sections $F_1, \ldots, F_s$ were always supposed to be given in dense representation).

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 suppose that the polynomials $G_1, \ldots, G_s$ are given in dense representation. We consider them as input for the algorithmic result which we are going to explain now.

We denote by $(G_1, \ldots, G_s)$ the homogeneous ideal generated by $G_1, \ldots, G_s$ in $k[X_0, \ldots, X_n]$. We define the degree $\deg(G_1, \ldots, G_s)$ of the ideal $(G_1, \ldots, G_s)$ in the usual way by means of the Hilbert polynomial. In our case the Hilbert polynomial is constant, since W, the projective variety given by $G_1, \ldots, G_s$, is supposed to be zero dimensional. Moreover Bezout's Theorem implies $\deg(G_1, \ldots, G_s) \leq d^n$.

Let $(G_1, \ldots, G_s, U_0X_0 + \cdots + U_nX_n)$ be the homogeneous ideal of $k[U_0, \ldots, U_n, X_0, .$ generated by the forms $G_1, \ldots, G_s, U_0X_0 + \cdots + U_nX_n$. For $0 \leq i \leq n$ we denote by $((G_1, \ldots, G_s, U_0X_0 + \cdots + U_nX_n) : X_i^*)$ the homogeneous ideal of $k[U_0, \ldots, U_n, X_1, \ldots, X_n]$ defined by $((G_1 \ldots . G_s, U_0X_0 + \cdots + U_nX_n) : X_i^*) := \{G \in k[U_0, \ldots, U_n, X_0, \ldots, X_n];\ \exists N \in \mathbb{N}$ with $GX_i^N \in (G_1, \ldots, G_s, U_0X_0 + \cdots + U_nX_n)\}$. We consider the following homogeneous ideal of $k[U_0, \ldots, U_n]$:

$$k[U_0, \ldots, U_n] \cap \bigcap_{0 \leq i \leq n} ((G_1, \ldots, G_s, U_0X_0 + \cdots + U_nX_n) : X_i^*).$$

¿From [Ca 90], Proposition 1.3 one deduces immediately the well known fact that this ideal is principal. The (up to scaling by non–zero elements of k) unique generator of it is called the $\mathcal{U}$–resultant of $(G_1, \ldots, G_s)$.

The $\mathcal{U}$–resultant R of the zero dimensional homogeneous ideal $(G_1, \ldots, G_s)$ has the following properties:

- $\deg R = \deg(G_1, \ldots, G_s) \leq d^n$
- for any point $(u_0, \ldots, u_n) \in \mathbf{A}^{n+1}$ 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 [vd Wae 40], Kapitel 11, §79 and [Jou 90].

The improved complexity bounds in the last section are all based on the following fundamental result essentially due to D. Lazard:

PROPOSITION 9. *The $\mathcal{U}$–resultant of the homogeneous ideal generated by $G_1, \ldots, G_s$ in $k[X_0, \ldots, X_n]$ 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 $G_1, \ldots, G_s$.*

A proof os this proposition is implicitely contained in [La 81], [Ca 88b] and [Gi-He 91], 3.2.

Let us also observe that Proposition 9 entails a (partial) answer for the projective version of problem (iv). Let us call this version the projective zero-dimensional elimination problem.

The algorithm underlying Proposition 9 is well parallelizable. Moreover if k is the field of rational numbers $\mathbb{Q}$ the binary length of the parameters used during the procedure is of order log of its sequential complexity. We shall include this condition in our notion of a well parallelizable algorithm when the

base field is $\mathbb{Q}$. In this sense we have the following relative lower bound result :

PROPOSITION 10. *Let $G_1, \ldots, G_s$ be given by a well parallelizable straight line program of length L. If there exists an 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 U-resultant of the homogeneous ideal generated by $G_1, \ldots, G_s$, then $P = NP$ holds.*

Proof. Suppose that such an algorithm exists. Let $k := \mathbb{Q}$ and $s := n$. We consider the zero dimensional homogeneous ideal of $\mathbb{Q}[X_0, \ldots, X_n]$ generated by the forms $G_1 := X_1^2 - X_1X_0, \ldots, G_n := X_n^2 - X_nX_0$. Let $R_n \in \mathbb{Q}[U_0, \ldots, U_n]$ be the U-resultant of this ideal. Since $G_1, \ldots, G_n$ can be represented by a division free straight line program in $\mathbb{Q}[X_0, \ldots, X_n]$ of length $O(n)$ and depth $O(1)$ we conclude from our hypothesis that R_n can be evaluated by a division free and well parallelizable straight line program β_n in $\mathbb{Q}[X_0, \ldots, X_n]$ of length $n^{O(1)}$. Our (modified) notion of well parallelizability and the hypothesis of the uniformity of the algorithm which produces the straight line program β_n from the input $G_1, \ldots, G_n$ imply that there exists a polynomial time Turing machine which for any n and any $(n+1)$-tuple $u = (u_0, \ldots, u_n)$ of integers computes the value of $R_n(u)$. Hence this Turing machine decides whether the projective variety W_u defined by the forms $X_1^2 - X_1X_0, \ldots, X_n^2 - X_nX_0, u_0X_0 + \cdots + u_nX_n$ is empty. Let us observe that W_u is the projective closure of the affine variety

$$V_u := \{X_1^2 - X_1 = 0, \ldots, X_n^2 - X_n = 0, u_0 + u_1X_1 + \cdots + u_nX_n = 0\}.$$

Therefore we have $R(u) = 0$ if and only if $V_u \neq \emptyset$ holds.

Thus we obtain a deterministic polynomial time Turing Machine M which decides for arbitrary natural numbers $v, u_1, \ldots, u_n$ whether for $u := (-v, u_1, \ldots, u_n)$ the variety V_u obtained by intersecting $\{X_1^2 - X_1 = 0, \ldots, X_n^2 - X_n = 0\}$ with the equation $u_1X_1 + \cdots + u_nX_n = v$ is nonempty.

One sees immediately that for $u = (-v, u_1, \ldots, u_n)$ the variety V_u is nonempty if and only if there exists a set $I \subset \{1, \ldots, n\}$ such that $\sum_{i \in I} u_i = v$ is satisfied. This means that the Turing Machine M solves the knapsack problem in polynomial time, whence $P = NP$. □

The hypothesis of uniformity is unavoidable for the conclusion in the precedent proposition since the non-uniform knapsack problem over the reals is solvable in polynomial time ([Me 84]. See also [Mon-Par 92]).

REMARK 11. From Proposition 10 one deduces immediately that if $P \neq NP$ holds, there exists no uniform well parallelizable algorithm which for inputs $F_1, \ldots, F_s \in k[X_1, \ldots, X_n]$ given by a well parallelizable division free straight line program of length L solves the affine zero dimensional elimination problem (problem (iv)) in sequential time $(Ln)^{O(1)}$ and produces the following output: a polynomial $Q(Y)$ of degree $\deg V$ belonging to the ideal $(F_1, \ldots, F_s)$ which is given by a division free well parallelizable straight line program in $k[Y]$ of length $(Ln)^{O(1)}$.

Let $\beta = (Q_1, \ldots, Q_m)$ with $Q_1, \ldots, Q_m \in k[X_1, \ldots, X_n]$ be a straight line program in $k[X_1, \ldots, X_n]$. The polynomials $Q_1, \ldots, Q_m$ are the intermediate results of β and for $1 \leq \rho \leq m$ each Q_ρ satisfies one of the following conditions:

(i) $Q_\rho \in k \cup \{X_1, \ldots, X_n\}$

(ii) there exist $1 \leq \rho_1, \rho_2 < \rho$ such that $Q_\rho = Q_{\rho_1} * Q_{\rho_2}$ holds with $* \in \{+, -, \cdot, /\}$.

We call the straight line program β *monotone* if for each step of type (ii) in β with $* \in \{+, -\}$ the condition $\deg Q_\rho = \max\{\deg Q_{\rho_1}, \deg Q_{\rho_2}\}$ is satisfied.

Let X_0 be a new variable and let $Q \in k[X_1, \ldots, X_n]$ be a polynomial of degree δ. Then $\overline{Q} := X_0^\delta Q\left(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0}\right)$ is a form of degree δ of $k[X_0, \ldots, X_n]$. We call $\overline{Q}$ the homogeneization of Q by the variable X_0. Let us observe that $\overline{Q}(1, X_1, \ldots, X_n) = Q(X_1, \ldots, X_n)$ holds.

We need the following technical result:

LEMMA 12. *Let $Q \in k[X_1, \ldots, X_n]$ be a polynomial represented by a division free monotone straight line program β in $k[X_1, \ldots, X_n]$ of length L and depth ℓ. Then β can be transformed in sequential time $O(L^2)$ in a division free straight line program $\overline{\beta}$ in $k[X_0, \ldots, X_n]$ of length $O(L^2)$ and depth $O(\ell)$ which evaluates $\overline{Q}$.*

Proof. Let $\beta = (Q_1, \ldots, Q_m)$ with $Q_1, \ldots, Q_m \in k[X_1, \ldots, X_n]$. For $1 \leq$

$\rho \leq m$ let $d_\rho := \deg Q_\rho$ and observe that $d_\rho \leq 2^\ell \leq 2^L$ and $Q_m = Q$ holds. Without loss of generality we may suppose that every $Q_1, \ldots, Q_m$ is different from zero. Thus we have $d_\rho \geq 0$ for $1 \leq \rho \leq m$. In sequential time $O(L^2)$ and parallel time $O(\ell)$ we precompute for any pair of indices $1 \leq \rho_1, \rho_2 \leq m$ with $d_{\rho_1} \geq d_{\rho_2}$ the monomial $X_0^{d_{\rho_1} - d_{\rho_2}}$ using only multiplications in $k[X_0, \ldots, X_n]$. Observe that between this monomials appear all $X_0^{d_\rho}$, $1 \leq \rho \leq m$. Now we construct by recursion in $1 \leq \rho \leq m$ from $(X_0^{d_{\rho_1} - d_{\rho_2}};\ 1 \leq \rho_1, \rho_2 \leq m,\ d_{\rho_1} \geq d_{\rho_2})$ a division free straight line program $\beta' = (Q'_1, \ldots, Q'_m)$ as follows:

Let $1 \leq \rho \leq m$. If $Q_\rho \in k \cup \{X_1, \ldots, X_n\}$ we put $Q'_\rho := Q_\rho$. If Q_ρ is of the form $Q_\rho = Q_{\rho_1} * Q_{\rho_2}$ with $1 \leq \rho_1, \rho_2 < \rho$ we consider the following cases:

(a) $* \in \{+, -\}$ and $d_{\rho_1} = 0$ or $d_{\rho_2} = 0$.
If $d_{\rho_1} = 0$ we put $Q'_\rho := Q_{\rho_1} \cdot X_0^{d_{\rho_2}} + Q'_{\rho_2}$ and
if $d_{\rho_2} = 0$ we put $Q'_\rho := Q'_{\rho_1} + Q_{\rho_2} \cdot X_0^{d_{\rho_1}}$.

(b) $* \in \{+, -\}$ and $d_{\rho_1} > 0$, $d_{\rho_2} > 0$.
Without loss of generality we may suppose $d_{\rho_1} = \max\{d_{\rho_1}, d_{\rho_2}\}$. We put $Q'_\rho := Q'_{\rho_1} + X_0^{d_{\rho_1} - d_{\rho_2}} Q'_{\rho_2}$.

(c) $* \in \{\cdot\}$. We put $Q'_\rho := Q'_{\rho_1} * Q'_{\rho_2}$.
Since by hypothesis the straight line program β is monotone one verifies immediately by induction in $1 \leq \rho \leq m$ that $Q'_1 = \overline{Q}_1, \ldots, Q'_m = \overline{Q}_m = \overline{Q}$ holds. (The only subtle point is the verification of $Q_\rho = \overline{Q}_\rho$ in case (b). Here we use the hypothesis of monotony which implies $d_\rho = \max\{d_{\rho_1}, d_{\rho_2}\}$). Moreover β' is a division free straight line program in $k[X_0, \ldots, X_n]$ of length $O(L)$ and depth $O(\ell)$ which computes the polynomial $\overline{Q}$ from the inputs $X_1, \ldots, X_n$ and $X_0^{d_{\rho_1} - d_{\rho_2}}$ where $1 \leq \rho_1, \rho_2 \leq m$ and $d_{\rho_1} \geq d_{\rho_2}$. Joining at β' the precomputation of the monomials $X_0^{d_{\rho_1} - d_{\rho_2}}$ above we obtain a division free straight line program $\overline{\beta}$ in $k[X_0, \ldots, X_n]$ of length $O(L^2)$ and depth $O(\ell)$ which computes $\overline{Q}$, as desired. □

Let Z_{ij} with $1 \leq i, j \leq n$ be new indeterminates.

PROPOSITION 13. *Let $k := \mathbb{Q}(Z_{ij}; 1 \leq i, j \leq n)$ and let the polynomials $F_1, \ldots, F_s \in k[X_1, \ldots, X_n]$ 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* $\mathbf{Q}$ *and which solves the affine zero dimensional elimination problem (problem (iv)) 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* $\mathbf{Q}$ *can be evaluated by an arithmetic circuit of length* $n^{O(1)}$.

Proof. Let X_{ij} with $1 \leq i, j \leq n$ be new indeterminates over k. These indeterminates and Y will serve as the variables of the algorithmic problem we are going to consider. The input of this problem will be given by the following polynomials of $k[X_{ij}, Y; 1 \leq i, j \leq n]$:

$$X_{ij}^2 - X_{ij} \text{ for } 1 \leq i, j \leq n$$
$$-1 + \sum_{1 \leq j \leq n} X_{ij} \text{ for } 1 \leq i \leq n$$
$$-1 + \sum_{1 \leq i \leq n} X_{ij} \text{ for } 1 \leq j \leq n$$
$$Y - \prod_{1 \leq i \leq n} \sum_{1 \leq j \leq n} X_{ij} Z_{ij}$$

We consider the affine subvariety V of $\mathbf{A}^{n^2+1}$ defined by these polynomials and observe that V is reduced and zero-dimensional. Let $\pi : \mathbf{A}^{n^2+1} \to \mathbf{A}^1$ the projection map defined by $\pi((\xi_{ij})_{1 \leq i,j \leq n}, y) := y$ for $((\xi_{ij})_{1 \leq i,j \leq n}, y) \in \mathbf{A}^{n^2+1}$. Let $Q \in k[Y]$ be the monic polynomial of minimal degree which belongs to the ideal generated by our input polynomials in $k[X_{ij}, Y; 1 \leq i, j \leq n]$. Observe that Q is also the monic polynomial of minimal degree which defines the zero dimensional variety $\pi(V)$ (i.e. $Q(Y)$ is the minimal polynomial of $\pi(V)$). Therefore Q can be written as

$$(1) \qquad Q = \prod_{\sigma \in \mathrm{Sym}(n)} (Y - Z_{1\sigma(1)} \cdots Z_{n\sigma(n)}),$$

where $\mathrm{Sym}(n)$ denotes the symmetric group of permutations of n elements.

Let P be the permanent over $\mathbb{Q}$ of the $n \times n$ matrix $(Z_{ij})_{1 \leq i,j \leq n}$. Obviously P is a polynomial which belongs to $\mathbb{Q}[Z_{ij}; 1 \leq i, j \leq n]$ and therefore it is an element of k.

Developing the product (1) in Y we see that Q has the form

$$Q = Y^{n!} - PY^{n!-1} + \text{terms of lower degree in } Y \tag{2}$$

The input polynomials of our problem contain $n^2 + 1$ variables and can be represented by a division free straight line program in $k[X_{i,j}, Y; 1 \leq i, j \leq n]$ of length $O(n^2)$. Thus by hypothesis Q can be evaluated by a division free monotone arithmetic circuit β in $k[Y]$ of length $n^{O(1)}$. Let T be a new indeterminate and let $\overline{Q} \in k[T, Y]$ be the homogenization of Q by the variable T. By Lemma 12 $\overline{Q}$ can be represented by a division free straight line program $\overline{\beta}$ in $k[T, Y]$ of length $n^{O(1)}$. From (2) we deduce that $\overline{Q}$ has the following form:

$$\overline{Q} = Y^{n!} + PTY^{n!-1} + \text{terms of lower degree in } Y \tag{3}$$

¿From [Ba-Stra 82] (see also [Mo 84]) we deduce that we can evaluate the polynomial $\dfrac{\partial \overline{Q}}{\partial T}$ by a division free straight line program β' in $k[T, Y]$ of length $n^{O(1)}$. The representation (3) implies that $\dfrac{\partial \overline{Q}}{\partial T} - PY^{n!-1}$ is divisible by the indeterminate T. Therefore we have $\dfrac{\partial \overline{Q}}{\partial T}(0, 1) = P$. Since the straight line program β' is division free we can in β' specialize the variables T to 0 and Y to 1. Thus we obtain a circuit β'' in $k = Q(Z_{ij}; 1 \leq i, j \leq n)$ which uses possibly parameters from k and which computes the permanent P. We want to convert β'' into a straight line program in $\mathbb{Q}(Z_{ij}; 1 \leq i, j \leq n)$ which uses only parameters from $\mathbb{Q}$. The circuit β'' was obtained by transforming successively the initial straight line program β which evaluates Q of $k[Y]$. This transformation was done by means of an arithmetical network which uses only parameters from $\mathbb{Q}$. By hypothesis β itself is produced by an arithmetical network having the same property.

Both networks are of size $n^{O(1)}$. Therefore there exists an arithmetic network over k of size $n^{O(1)}$ which realizes the circuit β'' and which uses only

parameters from $\mathbb{Q}$. Thus the parameters of β'' which are elements of k but not of $\mathbb{Q}$ must be given by a straight line program in $\mathbb{Q}(Z_{ij}; 1 \leq i,j \leq n)$ of size $n^{O(1)}$. Hence joining this straight line program at β'' we obtain an arithmetical circuit β^* over $\mathbb{Q}$ of size $n^{O(1)}$ which computes all intermediate results of β'' in $\mathbb{Q}(Z_{ij}; 1 \leq i,j \leq n)$. Between these results one finds the $n \times n$ permanent $P = \dfrac{\partial \overline{Q}(0,1)}{\partial T}$. Thus P can be evaluated by a straight line program of size $n^{O(1)}$ in $\mathbb{Q}(Z_{ij}; 1 \leq i,j \leq n)$. □

3. An elimination polynomial which is difficult to evaluate.

In this section we consider the zero dimensional elimination problem in a semialgebraic context. We shall give an absolute lower bound of subexponential type for a particular instance of the counterpart of problem (iv) for real closed fields.

For this purpose we need some preparations concerning lower bound techniques for the evaluation complexity of polynomials. We first develop a method for showing lower bounds for the complexity of univariate polynomials which are given by their roots. This method is analogous to the technique used in [He-Sie 80].

3.1. A geometric model for straight line programs.

In this section let d and L be given natural numbers different from one. Let $k := \mathbf{C}$ and Y an indeterminante over $\mathbf{C}$. To any point $F = (f_1, \ldots, f_d)$ of $\mathbf{A}^d = \mathbf{A}^d(\mathbf{C})$ there corresponds a monic polynomial $Y^d + f_1 Y^d + \cdots + f_d \in \mathbf{C}[Y]$ of degree d which we denote also by F. In this way we identify the set of the monic polynomials of $\mathbf{C}[Y]$ of degree d with the affine space $\mathbf{A}^d$. Let $\mathcal{L}$ be the nonscalar (Ostrowski) complexity measure for division free circuits in $\mathbf{C}[Y]$. We say that a polynomial F of $\mathbf{C}[Y]$ has nonscalar complexity L if $L = \min\{\mathcal{L}(\beta); \beta$ is a division free circuit in $\mathbf{C}[Y]$ which computes $F\}$ is satisfied. We write $\mathcal{L}(F) := L$ if this is the case (see [Stra 72], [Sto 89] or [He 89] for details). We denote by $W(d, L)$ the Zariski closure in $\mathbf{A}^d$ of the set of monic polynomials of degree d of $\mathbf{C}[Y]$ which can be evaluated by division

free circuits in $\mathbf{C}[Y]$ of nonscalar length at most L. Let $m := (L+2)^2$ and let $T_1, \ldots, T_m$ be new indeterminates over $\mathbf{C}$.

LEMMA 14 ([Schn 78]). *There exist polynomials $Q_1, \ldots, Q_d \in \mathbf{Z}[T_1, \ldots, T_m]$ with the following properties:*

(i) $\deg Q_j \leq 2(d-j)L$ *for* $1 \leq j \leq d$

(ii) Let $\Phi_{d,L} : \mathbf{A}^m \to \mathbf{A}^d$ be the morphism of affine spaces given by $(Q_1, \ldots, Q_d)$. The morphism $\Phi_{d,L}$ satisfies the following condition: if a monic polynomial F of $\mathbf{C}[Y]$ of degree d has nonscalar complexity at most L, then the point F of $\mathbf{A}^d$ belongs to the image of $\Phi_{d,L}$.

(iii) The variety $W(d,L)$ is the Zariski closure of the image $\Phi_{d,L}$.

From Lemma 14 one deduces easily the following result.

LEMMA 15 ([He-Sie 80]). *$W(d,L)$ is a closed irreducible subvariety of $\mathbf{A}^d$ which is definable over $\mathbf{Q}$ and which satisfies the following conditions:*

(i) $\dim W(d,L) \leq (L+2)^2$

(ii) $\deg W(d,L) \leq (2dL)^{(L+2)^2}$

Let $P_1, \ldots, P_d$ and $Y_1, \ldots, Y_d$ be new indeterminates (corresponding to the coefficients and the roots of the monic polynomials in Y of degree d). Let $\sigma_1, \ldots, \sigma_d$ the polynomials of $\mathbf{Z}[Y_1, \ldots, Y_d]$ satisfying the equality

$$Y^d + \sigma_1 Y^{d-1} + \cdots + \sigma_d = \prod_{1 \leq j \leq d} (Y - Y_j) . \tag{4}$$

Up to sign the polynomials $\sigma_1, \ldots, \sigma_d$ are the elementary symmetric functions in $Y_1, \ldots, Y_d$. Let us identify the variables $P_1, \ldots, P_d, Y_1, \ldots, Y_d$ with the coordinate functions of the affine space $\mathbf{A}^{2d}$. We consider the closed subvariety $V(d,L)$ of $\mathbf{A}^{2d}$ given by

$$V(d,L) := (W(d,L) \times \mathbf{A}^d) \cap \{P_1 - \sigma_1 = 0, \ldots, P_d - \sigma_d = 0\} .$$

We denote by $\pi_1, \ldots, \pi_d$ and $\eta_1, \ldots, \eta_d$ the coordinate functions of $V(d,L)$ induced by $P_1, \ldots, P_d$ and $Y_1, \ldots, Y_d$. Let $\pi : V(d,L) \to W(d,L)$ be the morphism of affine varieties defined by $\pi = (\pi_1, \ldots, \pi_d)$.

With these notations we have the following technical result:

LEMMA 16. *Suppose that* $L \geq 2\log d$ *holds. Then* $V(d,L)$ *is a closed equidimensional subvariety of* $\mathbf{A}^{2d}$ *which is definable over* $\mathbf{Q}$. *The morphism* $\pi : V(d,L) \to W(d,L)$ *is finite and surjective. The* π*–fiber of any point* F *of* $W(d,L)$ *(which represents a monic polynomial of degree* d *of* $\mathbf{C}[Y]$*) has cardinality* $\dfrac{d!}{\alpha_1! \ldots \alpha_\ell!}$ *where* ℓ *is the number of distinct roots of the polynomial* F *and* $\alpha_1, \ldots, \alpha_\ell$ *are the multiplicities of these roots. The dimension and the degree of* $V(d,L)$ *satisfy*

(i) $\dim V(d,L) = \dim W(d,L)$

(ii) $\deg V(d,L) = d! \deg W(d,L)$.

Proof. One sees immediately from the definition that $V(d,L)$ is a closed subvariety of $\mathbf{A}^{2d}$. By Lemma 15 the variety $W(d,L)$ is definable over $\mathbf{Q}$. Hence this property is also shared by $V(d,L)$. From (4) and the definition of $V(d,L)$ one deduces that for any $1 \leq j \leq d$ the equality

$$\eta_j^d + \pi_1 \eta_j^{d-1} + \cdots + \pi_d = 0$$

holds in the coordinate ring of $V(d,L)$. This implies that π is finite.

Let $F = (p_1, \ldots, p_d)$ with $p_1, \ldots, p_d \in \mathbf{C}$ be an element of $W(d,L)$. The point F represents a monic polynomial of $\mathbf{C}[Y]$ of degree d which we denote also by F. In this sense we have $F = Y^d + p_1 Y^{d-1} + \ldots + p_d$. Let ℓ be the number of distinct roots of F. Denote these roots by $y_1, \ldots, y_\ell$ and let $\alpha_1, \ldots, \alpha_\ell \in \mathbb{N}$ be their multiplicities.

Thus we have $F = (Y - y_1)^{\alpha_1} \ldots (Y - y_\ell)^{\alpha_\ell}$ with $1 \leq \ell \leq d$. From the definition of $V(d,L)$ and π one deduces immediately that the π–fiber of F coincides with the $\mathrm{Sym}(d)$-orbit of the point $(F, (z_1, \ldots, z_d))$ where $z_1 := y_1, \ldots, z_{\alpha_1} := y_1$, $z_{\alpha_1+1} := y_2, \ldots, z_{\alpha_1+\alpha_2} := y_2, \ldots, z_{\alpha_1+\ldots+\alpha_{\ell-1}+1} := y_\ell, \ldots, z_{\alpha_1+\ldots+\alpha_\ell} := y_\ell$. (Here $\mathrm{Sym}(d)$ denotes the symmetric group of permutations of d elements.) Therefore the cardinality of the π–fiber of F is $\dfrac{d!}{\alpha_1! \ldots \alpha_\ell!}$. In particular the π–fiber of F is not empty. Therefore the finite morphism π is surjective. Thus the dimensions of $V(d,L)$ and $W(d,L)$ are equal, whence (i).

Let C be an irreducible component of $V(d,L)$. Since $V(d,L)$ is obtained by intersecting the irreducible variety $W(d,L) \times \mathbf{A}^d$ by d equations one concludes that $\dim C \geq \dim W(d,L)$ holds. On the other hand (i) implies $\dim C \leq \dim W(d,L)$. Thus we have $\dim C = \dim W(d,L) = \dim V(d,L)$, whence the equidimensionality of $V(d,L)$.

¿From the definition of $V(d,L)$ and the Bezout Inequality (see e.g. [He 83], Theorem 1) one deduces

$$\deg V(d,L) \leq d! \deg W(d,L) .$$

Let F be the polynomial $F := Y^d + 1$. F is separable and can be evaluated by a straight line program β in $\mathbf{C}[Y]$ which executes at most $2 \log d$ multiplications and one addition. Therefore β is division free and has nonscalar length bounded by L. This implies that the point $(0,\ldots,0,1)$ of $\mathbf{A}^d$ which represents the polynomial F belongs to $W(d,L)$. Therefore the constructible subset of $W(d,L)$ of points representing separable monic polynomials of degree d of $\mathbf{C}[Y]$ which can be evaluated by a division free straight line program of nonscalar length at most L is not empty. Since by Lemma 15 the variety $W(d,L)$ is irreducible this constructible set is Zariski dense in $W(d,L)$. We denote it by U and observe that U contains a non-empty open subset of $W(d,L)$.

Let $r := \dim W(d,L)$ and $D := \deg W(d,L)$. By [He 83], Remark 2, there exist r affine hyperplanes of $\mathbf{A}^d$ given by affine linear polynomials $H_1,\ldots,H_d \in \mathbf{C}[P_1,\ldots,P_d]$ which intersect $W(d,L)$ in exactly D points which belong all to the set U. Let $F_1,\ldots,F_D$ these points. They represent separable monic polynomials of degree d of $\mathbf{C}[Y]$ which we denote also by $F_1,\ldots,F_D$.

Let $1 \leq j \leq D$. Since the polynomial F_j is separable, all its zeroes are distinct and therefore the π-fiber of F_j has cardinality $d!$. This implies that the preimage $\widehat{V}$ of the set $\{F_1,\ldots,F_D\}$ by π is of cardinality $d!D = d! \deg W(d,L)$. On the other hand we have $\widehat{V} = V(d,L) \cap \{H_1 = 0,\ldots,H_d = 0\}$ (here we interprete $H_1,\ldots,H_d$ as affine linear polynomials of $\mathbf{C}[P_1,\ldots,P_d,Y_1,\ldots,Y_d]$). ¿From the Bezout Inequality we deduce now $\deg \widehat{V} \leq \deg V(d,L)$. Since $\widehat{V}$ is finite, this means that $\widehat{V}$ contains at most $\deg V(d,L)$ points. Thus we obtain $d! \deg W(d,L) \leq \deg V(d,L)$.

Since we have already shown the reverse inequality, we conclude that (ii) holds. □

Let $y = (y_1, \ldots, y_d)$ be a point of $\mathbf{A}^d$. We call $F_y := Y^d + \sigma_1(y)Y^{d-1} + \cdots + \sigma_d(y)$ its associated polynomial. Thus F_y belongs to $\mathbb{C}[Y]$ and is monic of degree d. We identify F_y with the point $(\sigma_1(y), \ldots, \sigma_d(y))$ of $\mathbf{A}^d$ which we denote also by F_y. We say that the point y is separable if F_y is, i.e. if all $y_1, \ldots, y_d$ are distinct.

Let G be the automorphism group of $\mathbb{C}$, i.e. the Galois group $G := \mathrm{Gal}(\mathbb{C} : \mathbb{Q})$ of $\mathbb{C}$ which has $\mathbb{Q}$ as fixed field. The action of G on $\mathbb{C}$ can be extended componentwise to $\mathbf{A}^d$. Let τ be an element of G. We write $\tau \cdot y := (\tau(y_1), \ldots, \tau(y_d))$. For a monic polynomial $F = Y^d + p_1 Y^{d-1} + \cdots + p_d$ of degree d which belongs to $\mathbb{C}[Y]$ we write $\tau \cdot F := Y^d + \tau(p_1)Y^{d-1} + \cdots + \tau(p_d)$. The same notation is used for the action of τ on the point of $\mathbf{A}^d$ representing this polynomial.

The symmetric group $\mathrm{Sym}(d)$ acts in a natural way on $\mathbf{A}^d$ and so does the product group $G^* := G \times \mathrm{Sym}(d)$. Let $\gamma = (\tau, w)$ with $\tau \in G$ and $w \in \mathrm{Sym}(d)$ an element of G^*. We denote by $\gamma \cdot y$ the action of γ on y, i.e. $\gamma \cdot y := (\tau(y_{w(1)}), \ldots, \tau(y_{w(d)}))$. Let us write $G^* \cdot y$ for the G^*-orbit of y, i.e. $G^* \cdot y := \{\gamma \cdot y; \gamma \in G^*\} = \{(\tau(y_{w(1)}), \ldots, \tau(y_{w(d)})) : \tau \in G,\ w \in \mathrm{Sym}(d)\}$.

The group G^* acts also on $\mathbf{A}^{2d} = \mathbf{A}^d \times \mathbf{A}^d$ in the following way: let $p = (p_1, \ldots, p_d) \in \mathbf{A}^d$, $y = (y_1, \ldots, y_d) \in \mathbf{A}^d$ and $\gamma = (\tau, w) \in G^*$ with $\tau \in G$, $w \in \mathrm{Sym}(d)$. Then $\gamma \cdot (p, y)$ is defined by

$$\gamma \cdot (p, y) := (\tau(p_1), \ldots, \tau(p_d), \tau(y_{w(1)}), \ldots, \tau(y_{w(d)})) .$$

Again we denote $G^* \cdot (p, y) := \{\gamma \cdot (p, y); \gamma \in G^*\}$ for the G^*-orbit of (p, y). If y is given as before and p is the point of $\mathbf{A}^d$ which represents the polynomial F_y the following is true:

- G^*y is finite iff the coordinates of y are algebraic and in this case we have $\#(G^* \cdot (p, y)) = \#(G^* \cdot y)$.
- for $\gamma = (\tau, w) \in G^*$ with $\tau \in G$ and $w \in \mathrm{Sym}(d)$ we have $\gamma \cdot (p, y) = (\tau \cdot p, \gamma \cdot y)$ and the point $\tau \cdot p$ represents the polynomial $F_{\gamma \cdot y} = F_{\tau \cdot y}$. From Lemma 16 we know that the algebraic variety $V(d, L)$ is definable over $\mathbb{Q}$. From this and the definition of $V(d, L)$ one see immediately that $V(d, L)$ remains invariant under the action of the group G^*.

With these notations and observations we have the following result which

is inspired in [He-Sie 80], Theorem 1.

PROPOSITION 17. *Let $y = (y_1, \ldots, y_d)$ be a separable point of $\mathbf{A}^d$ with (distinct) algebraic coordinates $y_1, \ldots, y_d$ and let $Q_1, \ldots, Q_N$ be symmetric polynomials of $\mathbb{Q}[Y_1, \ldots, Y_d]$ of degree at most q, where q is a given natural number different from one.*

We suppose that y is an isolated point of the algebraic variety $\{Q_1 = 0, \ldots, Q_N = 0\}$ contained in $\mathbf{A}^d$. Let $F := F_y = \prod_{1 \le j \le d} (Y - y_j)$. Then the nonscalar complexity of F satisfies

$$\mathcal{L}(F) \ge \left(\frac{\log \dfrac{\#(G^* \cdot y)}{d!}}{2 + \dfrac{3}{2} \log dq} \right)^{1/2} - 2 .$$

Proof. Let $L := \mathcal{L}(F)$ and $V := V(d, L)$. Observe that F is a separable monic polynomial of degree d of $\mathbb{C}[Y]$ satisfying $F = \prod_{1 \le j \le d} (Y - y_j)$. The polynomial F is represented by a point of $\mathbf{A}^d$ which we denote also by F. Since the nonscalar complexity of F is L the point (F, y) belongs to V.

Let $r := \dim V$. Observe that Lemma 15(i) and Lemma 16(i) imply $r \le (L+2)^2$. Let us choose a generic $r \times N$ matrix $M := (\mu_{j\ell})_{\substack{1 \le j \le r \\ 1 \le \ell \le N}}$ of rational numbers. We consider the polynomials $Q'_1, \ldots, Q'_r$ of $\mathbb{Q}[Y_1, \ldots, Y_d]$ defined by

$$Q'_j := \sum_{1 \le \ell \le N} \mu_{j\ell} Q_\ell ,$$

where $1 \le j \le r$. These polynomials are symmetric and their degree is bounded by q. Moreover the point (F, y) belongs to $V' := V \cap (\mathbf{A}^d \times \{Q'_1 = 0, \ldots, Q'_r = 0\})$.

Recall that y was assumed to be an isolated point of $\{Q_1 = 0, \ldots, Q_N = 0\}$. Thus from the generic choice of the matrix M we conclude that (F, y) is an isolated point of V'. Since the polynomials $Q'_1, \ldots, Q'_r$ are symmetric and belong to $\mathbb{Q}[Y_1, \ldots, Y_d]$ the variety $\mathbf{A}^d \times \{Q'_1 = 0, \ldots, Q'_r = 0\}$ is G^*-invariant.

As we have seen before the same is true for V. This implies the G^*–invariance of V'. Thus $(F,y) \in V'$ implies $G^* \cdot (F,y) \subset V'$. Since (F,y) is an isolated point of V' all elements of the (finite) orbit $G^* \cdot (F,y)$ have the same property. This implies

$$\#(G^* \cdot y) = \#(G^* \cdot (F,y)) \leq \deg V' \tag{5}$$

On the other hand the Bezout Inequality, Lemma 15(ii) and Lemma 16(ii) imply the following estimates:

$$\deg V' \leq q^r \deg V \leq d! q^{(L+2)^2} \deg W(d,L) \leq d! q^{(L+2)^2} (2dL)^{(L+2)^2} .$$

Thus we have

$$\deg V' \leq d! q^{(L+2)^2} (2dL)^{(L+2)^2} \tag{6}$$

¿From (5) and (6) we deduce

$$\frac{\#(G^* \cdot y)}{d!} \leq q^{(L+2)^2} (2dL)^{(L+2)^2} . \tag{7}$$

The algorithm [Pa-Stoc 73], 3.2 implies $L \leq 2\sqrt{d}$. Taking logarithms in (7) we obtain therefore

$$\log \frac{\#(G^* \cdot y)}{d!} \leq (L+2)^2 (1 + \log dqL) \leq (L+2)^2 \left(2 + \frac{3}{2} \log dq\right)$$

and finally

$$\mathcal{L}(F) = L \geq \left(\frac{\log \dfrac{\#(G^* \cdot y)}{d!}}{2 + \dfrac{3}{2} \log dq} \right)^{1/2} - 2 . \qquad \square$$

As an application of Proposition 17 we obtain the theorem below.

Let $j \in \mathbb{Z}$ with $j \geq 0$. If $j \geq 1$ we denote by $\sqrt{j}$ the positive square root of j. For $j = 0$ let $\sqrt{j} := 0$.

THEOREM 18. *Let $(F_d)_{d\in\mathbb{N}}$ be the family of monic polynomials $F_d \in \mathbb{R}[Y]$ of degree d defined as follows:*

$$F_d := \prod_{0\le j<d} (Y - \sqrt{j}) .$$

Then $\mathcal{L}(F_d) = \Omega\Big(\dfrac{\sqrt{d}}{\log d}\Big)$.

Thus the family $(F_d)_{d\in\mathbb{N}}$ is hard to compute in the sense of [He 89].

Proof. Let $(y^{(d)})_{d\in\mathbb{N}}$ be the family of points $y^{(d)} = (y_1^{(d)}, \ldots, y_d^{(d)})$ of $\mathbf{A}^n$ defined by $y_j^{(d)} := \sqrt{j-1}$ for $1 \le j \le d$. Thus we have $F_d = F_{y^{(d)}}$.

Fix for the moment $d \ge 2$ and let $y := y^{(d)}$, $y = (y_1, \ldots, y_d)$, $F := F_d = F_y$.

Let $P(Y) = \prod_{0\le j<d} (Y^2 - j)$ and observe that $P(Y) = (-1)^d F(Y)F(-Y)$ holds. Thus for $1 \le j \le d$ we have $P(y_j) = 0$. The polynomial P belongs to $\mathbb{Q}[Y]$ and is monic of degree $2d$.

Let $Q_1 := \sigma_1(P(Y_1), \ldots, P(Y_d)), \ldots, Q_d := \sigma_d(P(Y_1), \ldots, P(Y_d))$, where $\sigma_1, \ldots, \sigma_d$ are the symmetric polynomials defined by the equality (4) in the proof of Lemma 15. Observe that the polynomials $Q_1, \ldots, Q_d$ are symmetric in $Y_1, \ldots, Y_d$ and belong to $\mathbb{Q}[Y_1, \ldots, Y_d]$. Their degrees are bounded by $q := 2d^2$. Moreover $Q_1, \ldots, Q_d$ satisfy the identity

$$Y^d + Q_1 Y^{d-1} + \cdots + Q_d = \prod_{1\le j\le d} (Y - P(Y_j)) . \tag{8}$$

¿From (8) we infer immediately that a point $z = (z_1, \ldots, z_d)$ of $\mathbf{A}^d$ belongs to the variety $\{Q_1 = 0, \ldots, Q_d = 0\}$ if and only if $P(z_j) = 0$ holds for any $1 \le j \le d$. Therefore the algebraic variety $\{Q_1 = 0, \ldots, Q_d = 0\}$ is zero dimensional and contains the point y. Since $Q_1, \ldots, Q_d$ are symmetric polynomials of $\mathbb{Q}[Y_1, \ldots, Y_d]$ of degree at most $q = 2d^2$ we conclude from Proposition 17 that

$$\mathcal{L}(F) \ge \frac{\log \dfrac{\#(G^* \cdot y)}{d!}}{4 + 5\log d} - 2 \tag{9}$$

holds.

Now we are going to estimate the quantity $\frac{\#(G^* \cdot y)}{d!}$ from below.

Let $K' := \mathbb{Q}(y_1, \ldots, y_d) = \mathbb{Q}(\sqrt{j}; 0 \leq j < d)$ and observe that K' is a Galois extension of $\mathbb{Q}$. We denote by $G' := \mathrm{Gal}(K' : \mathbb{Q})$ the Galois group of K'. Let τ be an automorphism of K', i.e. an element of G'. Since for $1 \leq j \leq d$ the equality $y_j = \sqrt{j-1}$ holds we have $\tau(y_j) = \pm y_j$.

Thus τ can be described by its sign vector given by the d-tuple $(\tau_1, \ldots, \tau_d) \in \{0,1\}^d$ which satisfies the condition $\tau(y_j) = (-1)^{\tau_j} y_j$ for $1 \leq j \leq d$.

Let w be a permutation of $\mathrm{Sym}(d)$ and let $\gamma := (\tau, w)$.

We interprete γ as an element of G^*. Thus $\gamma \cdot y = (\tau(y_{w(1)}), \ldots, \tau(y_{w(d)})) = ((-1)^{\tau_1} y_{w(1)}, \ldots, (-1)^{\tau_d} y_{w(d)}) = ((-1)^{\tau_1} \sqrt{w(1)-1}, \ldots, (-1)^{\tau_d} \sqrt{w(d)-1})$. This implies that G' and $\mathrm{Sym}(d)$ act independently on y. Therefore we have

$$\#(G^* \cdot y) = d! \, \#G' \,. \tag{10}$$

Consider the primes $p_1, \ldots, p_m$ between 2 and $d-1$. Let $K'' := \mathbb{Q}(\sqrt{p_\ell}; 1 \leq \ell \leq m)$ and $G'' := \mathrm{Gal}(K'' : \mathbb{Q})$. Thus K'' is a subfield of K' and G'' is a homomorphic image of G'. From the proof of [vzGa-Stra 80], Application 2 we conclude that $\#G'' = 2^m$ holds. Therefore we have

$$\#G' \geq \#G'' = 2^m \tag{11}$$

¿From the Prime Number Theorem (or even from Chebyshev's Theorem, see [Cha 68]) we conclude that there exists a constant $c > 0$ such that for d sufficiently large the number m of primes between 2 and $d-1$ is at least $c \frac{d}{\log d}$.

Therefore (11) implies

$$\#G' \geq 2^{c(d/\log d)} \tag{12}$$

for d sufficiently large.

Thus from (9), (10) and (11) we infer that

$$\mathcal{L}(F) \geq \left(\frac{cd}{(4 + 5 \log d) \log d} \right)^{1/2} - 2$$

holds for d sufficiently large.

This implies $\mathcal{L}(F_d) = \Omega\left(\frac{\sqrt{d}}{\log d}\right)$. □

Open Problem.

For $d \in \mathbb{N}$ let $Y^{\underline{d}} := \prod_{0 \le j < d} (Y - j)$ and $\binom{Y}{d} := \frac{Y(Y-1)\ldots(Y-d+1)}{d!}$.

Obviously we have $d!\binom{Y}{d} = Y^{\underline{d}}$. The expression $\binom{Y}{d}$ is called the d-th Pochhammer polynomial in Y. We have $(Y^2)^{\underline{d}} = (-1)^d F_d(Y)F_d(-Y)$, where F_d is the polynomial of $\mathbb{R}[Y]$ considered in Proposition 17.

The question which we are still unable to answer is the following: are the families of polynomials $(Y^{\underline{d}})_{d\in\mathbb{N}}$ and $\left(\binom{Y}{d}\right)_{d\in\mathbb{N}}$ hard to compute?

3.2. A difficult zero dimensional elimination problem

For $n \in \mathbb{N}$ we consider the following semialgebraic subset of $\mathbb{R}^{n+1}$:

$$V_n := \left\{X_1^2 - X_1 = 0, \ldots, X_n^2 - X_n = 0,\ Y^2 - \sum_{1 \le i \le n} 2^{i-1} X_i = 0,\ Y \ge 0\right\}$$

Let $\pi_n : \mathbb{R}^{n+1} \to \mathbb{R}$ be the projection map defined by $\pi_n(x_1, \ldots, x_n, y) = y$ for $(x_1, \ldots, x_n, y) \in \mathbb{R}^{n+1}$.

Let $y^{(2^n)} = (y_1^{(2^n)}, \ldots, y_{2^n}^{(2^n)})$ be the point of $\mathbf{A}^{2^n}$ defined by $y_j^{(2^n)} := \sqrt{j-1}$ for $1 \le j \le 2^n$. Observe that $\#V_n = \#\pi(V_n) = 2^n$ and $\pi(V_n) = \{y_1^{(2^n)}, \ldots, y_{2^n}^{(2^n)}\} = \{\sqrt{j}; 0 \le j < 2^n\}$ holds.

Let $Q_n := F_{y^{(2^n)}} = \prod_{0 \le j < 2^n} (Y - \sqrt{j})$. Thus Q_n is a monic polynomial of degree 2^n of $\mathbb{R}[Y]$ which defines $\pi_n(V_n)$ as a subset of $\mathbf{A}^1 = \mathbf{A}^1(\mathbb{C})$:

$$\pi_n(V_n) = \{Q_n = 0\}\ .$$

V_n is a zero dimensional semialgebraic subset of $\mathbb{R}^{n+1}$ and Q_n is a possible solution of the semialgebraic counterpart of the zero-dimensional elimination problem (problem (iv)).

However one restriction has to be made: the coefficients of Q_n are not rational but real algebraic numbers. Thus Q_n would be never the output of a quantifier elimination procedure applied to the obvious elementary formula of ordered fields defining the semialgebraic set V_n. On the other hand Q_n is the (unique) monic polynomial of minimal degree of $\mathbb{R}[Y]$ which defines the set $\pi(V_n)$.

In this sense Q_n represents a natural output of an elimination procedure applied to the polynomials $X_1^2 - X_1, \ldots, X_n^2 - X_n, Y^2 - \sum_{1 \le i \le n} 2^{i-1} X_i, Y$ and involving computations with algebraic numbers.

Note that these polynomials may be represented by a division free straight line program in $\mathbb{Q}[X_1, \ldots, X_n, Y]$ of length $O(n)$ and depth $O(1)$. By Theorem 18 we know that the family of polynomials $(Q_n)_{n \in \mathbb{N}}$ is hard to compute. More precisely we have $\mathcal{L}(Q_n) = \Omega\left(\frac{2^{n/2}}{n}\right)$ for $n \in \mathbb{N}$. Since $\deg Q_n = 2^n$ holds the depth of any arithmetic circuit representing Q_n is $\Omega(n)$ (see [vzGa 86]). We state this conclusion in the following way:

THEOREM 19. *Let* $F_1 := X_1^2 - X_1, \ldots, F_n := X_n^2 - X_n$, $F_{n+1} := Y^2 - \sum_{1 \le i \le n} 2^{i-1} X_i$, $F_{n+2} := Y$ *and* $V_n := \{F_1 = 0, \ldots, F_n = 0, F_{n+1} = 0, F_{n+2} \ge 0\}$.

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* $\pi_n := \mathbb{R}^{n+1} \to \mathbb{R}$ *the projection map defined by* $\pi_n(x_1, \ldots, x_n, y) = y$, *where* $(x_1, \ldots, x_n, y) \in \mathbb{R}^{n+1}$.

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* $\Omega\left(\frac{2^{n/2}}{n}\right)$ *and parallel time* $\Omega(n)$ *for the representation of the output.*

It is insatisfactory that we have to insist in the formulation of the example

of Theorem 19 that the output is given exactly by the polynomial Q_n of minimal degree. The usual output of a quantifier elimination procedure applied to the obvious formula defining V_n would be the quantifier formula φ_n in the first order language of ordered fields given by

$$((Y^2)^{2^n} = 0 \wedge Y > 0) .$$

In view of this observation we make the following final remark:

Suppose that the family of polynomials $(Y^d)_{d \in \mathbb{N}}$ is hard to evaluate. Then either the zero-dimensional elimination problem (problem (iv)) is hard to solve for $k = \mathbb{Q}$ and $\overline{k} = \mathbb{C}$ 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.

Acknowledgment The first author (Joos Heintz) whishes to thank the Département de Mathématiques of the University of Nice for its hospitality during his stay in summer 1992, when the paper was written.

References

[Am 89] F. Amoroso: Test d'appartenance d'après un théorème de Kollár. C. R. Acad. Sci. Paris, Série I. **309** (1989) 691–694.

[Ar 92] I. Armendáriz: La complejidad del cálculo de la dimensión de una variedad algebraica. Master Thesis, Universidad de Buenos Aires (1992).

[Ba-Dí-Ga 90] J. Balcázar, J. Díaz and J. Gabarró: Structural Complexity II. EATCS Monographs on Theoretical Computer Science **22** Springer (1990).

[Bar 91] A.I. Barvinok: Feasibility testing for systems of real quadratic equations. Manuscript I.M. Sechenov Institute, Academy of Sciences, St. Petersburg (1991).

[Ba-Stra 82] W. Baur and V. Strassen: The complexity of partial derivatives. Theoret. Comput. Sci. **22** (1982) 317-330.

[Ber-Yg 90] C. Berenstein and A. Yger: Bounds for the degrees in the division problem. Michigan Math. Journal **37** (1990) 25–43.

[Ber-Yg 91] C. Berenstein and A. Yger: Effective Bezout identities in $\mathbf{C}[z_1, \ldots, z_n]$. Acta Math. **166** (1991) 69-120.

[Bro 87] W. D. Brownawell: Bounds for the degrees in the Nullstellensatz. Ann. Math. (Second Series) **126** (3) (1987) 577-591.

[Bu 85] B. Buchberger: Gröbner-Bases: An algorithmic method in polynomial ideal theory. Multidimensional System Theory, N.K. Bose ed., Reidel, Dordrecht (1985) 374-383.

[Ca-Ga-He 88] 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, Série I, **307** (1988) 255-258.

[Ca-Ga-He 89] L. Caniglia, A. Galligo, and J. Heintz: Some new effectivity bounds in computational geometry. Proc. 6th Int. Conf. Applied Algebra, Algebraic Algorithms and Error Correcting Codes AAECC–6, Rome 1988, T. Mora, ed., Springer LN Comput. Sci. **357** (1989) 131-151.

[Ca-Gu-Gu 91] L. Caniglia, J. A. Guccione and J. J. Guccione: Local membership problems for polynomial ideals. Effective Methods in Algebraic Geometry MEGA 90, T. Mora and C. Traverso, eds., Progress in Mathematics Vol. **94**, Birkhäuser (1991) 31–45.

[Can 88a] J. Canny: Some algebraic and geometric computations in PSPACE. Proc. 20-th Ann. ACM Symp. Theory of Computing (1988) 460-467.

[Can 88b] J. Canny: Generalized characteristic polynomials. Proc. Intern. Symp. on Symbolic and Algebraic Computation ISSAC'88 , Roma 1988, P. Gianni, ed., Springer LN Comput.

Sci. **358** (1989) 293-299.

[Cha 68] K. Chandrasekharan: Introduction to Analytic Number Theory. Grundlehren Band **148**, Springer (1968).

[Chi-Gri 83] A.L. Chistov and D.Yu. Grigor'ev: Subexponential time solving systems of algebraic equations. LOMI Preprints E-9-83, E-10-83, Leningrad (1983).

[Di-Fi-Gi-Se 91] A. Dickenstein, M. Giusti, N. Fitchas and C. Sessa: The membership problem for unmixed polynomial ideals is solvable in single exponential time. Discrete Appl. Math. **33** (1991) 73–94, Special Issue 7-th Intern. Conf. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes AAECC–7, Toulouse 1989.

[Du 90] T.W. Dubé: The structure of polynomial ideals and Gröbner bases. SIAM J. Comput. **19** (4) (1990) 750-773.

[Fi-Ga 90] 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.

[Fi-Ga-Mo 90a] N. Fitchas, A. Galligo and J. Morgenstern: Algorithmes rapides en séquentiel et parallèle pour l'élimination des quantificateurs en géométrie élémentaire. Sélection d'exposés 1986-1987, vol. I, F. Delon, M. Dickmann and D. Gondard, eds., Publ. Math. Univ. Paris 7, No. **32** (1990) 103-145.

[Fi-Ga-Mo 90b] 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.

[Fi-Gi-Smi 92] N. Fitchas, M. Giusti and F. Smietanski: Sur la complexité du théorème des zéros. Preprint Ecole Polytechnique Palaiseau (1992).

[vzGa 86] J. von zur Gathen: Parallel arithmetic computations: a survey.

Proc. 13-th. Conf. MFCS. Springer LN Comput. Sci. **233** (1986) 93-112.

[vzGa-Stra 80] J. von zur Gathen and V. Strassen: Some polynomials that are hard to compute. Theoret. Comput. Sci. **11** (3) (1980) 331-336.

[Gi 84] M. Giusti: Some effectivity problems in polynomial ideal theory. Eurosam 84, Springer LN Comput. Sci. **174** (1984) 159-171.

[Gi-He 91] M. Giusti and J. Heintz: La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. To appear in Proc. Int. Meeting on Commutative Algebra, Cortona 1991.

[Gi-He-Sa 91] M. Giusti, J. Heintz and J. Sabia: On the efficiency of effective Nullstellensatze. To appear in Computational Complexity.

[Gri 87] D. Yu. Grigor'ev: The complexity of the decision for the first order theory of algebraically closed fields. Math. USSR–Izv. 29(2) (1987) 459–475.

[Gri-Kar-Si 89] D. Yu. 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.

[Gri-Vo 88] D. Yu. Grigor'ev and N. N. Vorobjov (jr): Solving systems of polynomial inequalities in subexponential time. J. Symb. Comput. **5** (1988) 37-64

[He 83] J. Heintz: Definability and fast quantifier elimination in algebraically closed fields. Theoret. Comput. Sci. **24** (1983) 239-277. Also in: Kybernetičeskij Sbornik, Novaja Serija, Vyp. **22**, O.B. Lupanov, ed., Mir Moskva (1985) 113–138.

[He 89] J. Heintz: On the computational complexity of polynomials and bilinear mappings. A survey. Applied Algebra, Algebraic Algorithms and Error Correcting Codes. 5th Intern. Conf.

AAECC-5, Menorca 1987. L. Huguet and A. Poli, eds., Springer LN Comput. Sci. **356** (1989) 269–300.

[He-Ro-So 90] J. Heintz, M.-F. Roy and P. Solernó: Sur la complexité du principe de Tarski-Seidenberg. Bull. Soc. Math. France **118** (1990) 101–126.

[He-Schn 82] J. Heintz and C. P. Schnorr: Testing polynomials which are easy to compute. 12-th Ann. ACM Symp. Theory of Computing (1980) 262–280. Also in: Logic and Algorithmic. An International Symposium held in Honour of Ernst Specker, Monographie de l'Enseignement Mathématique No. **30**. Genève (1982) 237-254.

[He-Sie 80] J. Heintz and M. Sieveking: Lower bounds for polynomials with algebraic coefficients. Theoret. Comput. Sci. **11** (1980) 321–330.

[He-Sie 81] J. Heintz and M. Sieveking: Absolute primality of polynomials is decidable in random polynomial time in the number of variables. Proc. 8-th Colloquium on Automata, Languages and Programming ICALP 81, Akko 1981, S. Even and O. Kariv, eds., Springer LN Comput. Sci **115** (1981) 16–28.

[Her 26] G. Hermann: Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. Math. Ann. **95** (1926) 736–788.

[Ie 89] D. Ierardi: Quantifier elimination in the theory of an algebraically-closed field. Proc. 21-st Ann. ACM Symp. Theory of Computing (1989) 138–147.

[Jou 90] J.P. Jouanolou: Le formalisme du résultant. Preprint IRMA, Université de Strasbourg 1990.

[Ka 88] E. Kaltofen: Greatest common divisors of polynomials given by straight line programs. J. ACM **35** No. 1 (1988) 234–264.

[Ko 88] J. Kollár: Sharp effective Nullstellensatz. J. AMS **1** (1988) 963–975.

[Kri-Lo 91] T. Krick and A. Logar : Membership problems, representation problems and the computation of the radical for one-dimensional ideals. Effective Methods in Algebraic Geometry MEGA 90, T. Mora and C. Traverso, eds., Progress in Mathematics Vol. **94**, Birkhäuser (1991) 203-216.

[La 81] D. Lazard: Résolution des systèmes d'équations algébriques. Theoret. Comput. Sci. **15** (1981) 77-110.

[Me 84] F. Meyer auf der Heide: A polynomial linear search algorithm for the $n-$dimensional knapsack problem. J. Ass. Comp. Mach. **31** (3) (1984) 668-676.

[Mo 84] J. Morgenstern: How to compute fast a function and all its derivatives. Prépublication No. 49, Université de Nice 1984.

[Pa-Stoc 73] M. S. Paterson and L. J. Stockmeyer: On the number of non-scalar multiplications necessary to evaluate polynomials. SIAM J. Comput. **2** (1) (1973) 60-66.

[Phi 88] P. Philippon: Théorème des zéros effectif d'après J. Kollár. Problèmes diophantiens, Publ. Math. Univ. Paris, No. **88** (1988-89).

[Ren 92] J. Renegar: On the computational complexity and geometry of the first order theory of the reals I. J. Sym. Comp. **13** (1992) 255-300.

[Schn 78] C. P. Schnorr: Improved lower bounds on the number of multiplications/divisions which are necessary to evaluate polynomials. Theoret. Comput. Sci. **7** (1978) 251-261.

[Shi 89] B. Shiffman: Degree bounds for the division problem in polynomial ideals. Michigan Math. J. **36** (1989) 163-171.

[Sto 89] H.-J. Stoss: On the representation of rational functions of bounded complexity. Theoret. Comput. Sci. **64** (1989) 1-13.

[Stra 72] V. Strassen: Berechnung und Programm I. Acta Inform. **1**

(1972) 320–334.

[vdWae 40] B. L. van der Waerden: *Moderne Algebra*. Vol II, Springer Verlag 1940.

Unité de Recherche INRIA Sophia Antipolis
2004, route des Lucioles - B.P. 93 - 06902 SOPHIA ANTIPOLIS Cedex (France)

Unité de Recherche INRIA Lorraine Technopôle de Nancy-Brabois - Campus Scientifique
615, rue du Jardin Botanique - B.P. 101 - 54602 VILLERS LES NANCY Cedex (France)
Unité de Recherche INRIA Rennes IRISA, Campus Universitaire de Beaulieu 35042 RENNES Cedex (France)
Unité de Recherche INRIA Rhône-Alpes 46, avenue Félix Viallet - 38031 GRENOBLE Cedex (France)
Unité de Recherche INRIA Rocquencourt Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 LE CHESNAY Cedex (France)

EDITEUR
INRIA - Domaine de Voluceau - Rocquencourt - B.P. 105 - 78153 LE CHESNAY Cedex (France)

ISSN 0249 - 6399