LOWER BOUNDS FOR DIOPHANTINE APPROXIMATIONS

D.Y. Franck–Le Plateau [1] M. Giusti [2] K.Hägele [3] J.E. Morais [3] J.L. Montaña [4] L.M. Pardo [3] [5]

June 12, 1996

Abstract

We introduce a subexponential algorithm for geometric solving of multivariate polynomial equation systems whose bit complexity depends mainly on intrinsic geometric invariants of the solution set.

¿From this algorithm, we derive a new procedure for the decision of consistency of polynomial equation systems whose bit complexity is subexponential, too. As a byproduct, we analyze the division of a polynomial modulo a reduced complete intersection ideal and from this, we obtain an intrinsic lower bound for the logarithmic height of diophantine approximations to a given solution of a zero–dimensional polynomial equation system. This result represents a multivariate version of Liouville's classical theorem on approximation of algebraic numbers by rationals.

A special feature of our procedures is their *polynomial* character with respect to the mentioned geometric invariants when instead of bit operations only arithmetic operations are counted at unit cost.

Technically our paper relies on the use of straight–line programs as a data structure for the encoding of polynomials, on a new symbolic application of Newton's algorithm to the Implicit Function Theorem and on a special, basis independent trace formula for affine Gorenstein algebras.

1 Introduction

The present pages represent a continuation of [21], [22], [39]. These papers concern the design of algorithms of intrinsic type to solve systems of polynomial equations. Solving is then applied to decide consistency of systems of polynomial equations. By "intrinsic type" we mean algorithms which are able to distinguish between the semantical and the syntactical character of the input system in order to profit from both for the improvement of the complexity estimates.

[1] : *Département de Mathématiques, Université de Nice, Parc Valrose F-06108 Nice Cedex 2. France*

[2] : *GAGE, Centre de Mathématiques. École Polytechnique. F-91228 Palaiseau Cedex. France*

[3] : *Departamento de Matemáticas, Estadística y Computación. Facultad de Ciencias. Universidad de Cantabria. E-39071 Santander, Spain*

[4] : *Departamento de Matemática e Informática. Campus de Arrosadía. Universidad Pública de Navarra. E-31006 Pamplona, Spain*

[5] : *Research was partially supported by the following French and Spanish grants : GDR CNRS 1026 MEDICIS, DGCYT PB92–0498–C02–01 and PB93–0472–C02–02*

With respect to bit complexity we show how the time necessary to solve a given polynomial equation system is related to the affine degree and the (affine) logarithmic height of the corresponding diophantine variety. In this sense, the results of [21] and [22] show already that the (affine) degree of an input system is associated with the complexity when measured in terms of number of arithmetic operations. However, there are still some drawbacks in this approach.

The first one is that the algorithms developed in [22] require iterative calls to the procedure and that the algorithms in [21] rely on the use of algebraic numbers. Thus in the case of [21] the algorithms are not "rational" although their inputs and outputs are.

A second drawback concerns the modeling used to measure complexity. The quantity of arithmetic operations of an algorithm does not explain sufficiently what happens when we are using it on a "real life" computer. Years of experience show that models of bit complexity (Turing machines, random access machines or equivalent models) represent more realistic patterns for practical computing. In this sense a study of bit complexity of the intrinsic complexity of the algorithms of [21] and [22] becomes necessary.

In the present paper we deal with both disadvantages of the algorithms in [21] and [22], giving practicable solutions (cf. also Section 3 below). First, our new algorithm is completely rational. It does not require any constants other than those in the field of coefficients of the input system. Secondly, to improve the bit complexity estimates, we introduce a suitable notion of height of affine diophantine varieties which is inspired by the corresponding notion introduced for projective varieties in [5], [8], [18], [37], [38], [40], [41], [42], [43]. As shown in Section 2, our notion of height is strongly related to the bit complexity of geometric elimination procedures of any kind.

Our notion of height combined with a new algorithmic interpretation of duality theory for complete intersection ideals yields a new Liouville estimate (cf. Sections 2 and 4 below). Liouville estimates can be applied to get lower time bounds for the numerical analysis approach to solving systems of polynomial equations. In particular, we show the practical inefficiency of both floating point and binary encoding for rational approximation of zero–dimensional multivariate polynomial equation systems even in the algorithmically well suited cases.

To illustrate these introductory observations, let us first consider the following two problems:

Problem 1 *Let be given a sequence of n integer polynomials of degree at most 3, with coefficients in $\{0,1\}$, concerning three variables each:*

$$p_1(X_{1,1}, X_{1,2}, X_{1,3}), \ldots, p_n(X_{n,1}, X_{n,2}, X_{n,3})$$

Decide whether the following system of polynomial equations has a solution:

$$X_1^2 - X_1 = 0, \ldots, X_n^2 - X_n = 0, Y_1^2 - Y_1 = 0, \ldots, Y_{3n}^2 - Y_{3n} = 0$$

$$\prod_{i=1}^{n} p_i(X_{i,1}, X_{i,2}, X_{i,3}) - (1 + \sum_{i=1}^{3n} Y_j 2^j) = 0$$

Problem 2 *Let be given in binary representation an integer $k \in \mathbb{N}$ and the polynomials:*

$$X_1^2 - X_1 = 0, \ldots, X_n^2 - X_n = 0$$

$$k - (X_1 + 2X_2 + \cdots + 2^{n-1}X_n) = 0$$

Decide whether this system has a solution.

Both problems have a similar "syntactical form" (i.e. they look very similar, as a consistency question for "syntactically easy" polynomial equation systems). However, they possess completely different "semantical" characters : the first problem is a translation of a well–known **NP**–complete problem (3-satisfiability, for short 3SAT), while the second one just concerns the binary encoding of k with n bits (if there exists such an encoding). This means that the second system is consistent if and only if k may be encoded using at most n binary digits (cf. [27], [39]). Traditional symbolic procedures deal with both problems using in each case the same generalistic treatment. However these two problems demand for different algorithms that may profit from their different semantical features. The construction of algorithms which are able to distinguish between equation systems which are semantically well suited and such which are not is the main goal of our paper. We shall also consider the question of consistency of polynomial equation systems in the following terms:

Problem 3 (Effective Nullstellensatz) *Given a sequence of polynomials $f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_n]$, decide whether the affine algebraic variety*

$$V(f_1, \ldots, f_s) := \{x \in \mathbb{C}^n : f_1(x) = \cdots = f_s(x) = 0\}$$

is empty or not.

As both Problems 1 and 2 above can be written as a special case of this more general Problem 3, we have to find a way to distinguish (within the context of Problem 3) between the different levels of difficulty Problems 1 and 2 represent. To design algorithms which solve this problem, taking care of the special features of the particular instance of the input system, we need two major geometric invariants: the affine degree and the affine height of the system (cf. Section 2.2 below). Assuming these two notions we are going to show in this paper the following result:

Theorem 1 *There exists a bounded error probability Turing machine which solves the following task: given polynomials $f_1, \ldots, f_{n+1} \in \mathbb{Z}[X_1, \ldots, X_n]$ of degree at most 2 and of (logarithmic) height h, the Turing machine decides whether the variety $V(f_1, \ldots, f_{n+1})$ is empty or not. Moreover, if δ is the intrinsic (affine) degree of the system and η is the intrinsic (logarithmic) height of the system, the Turing machine answers in (bit) time*

$$(nh\delta\eta)^{O(log_2 n)}$$

using a total amount of arithmetic operations in $\mathbb{Q}$ of

$$(n\delta)^{O(1)}.$$

Our algorithm first solves a suitable polynomial equation system and then uses this information for the consistency test of the original system $f_1, \ldots, f_{n+1}$. Solving is done inductively. In order to explain the procedure let us assume that the polynomials $f_1, \ldots, f_n$ form a regular sequence, each ideal $(f_1, \ldots, f_i)$ $1 \leq i \leq n$, being radical. Then the algorithm proceeds in n steps, solving at each stage $1 \leq i \leq n$ the system $f_1 = 0, \ldots, f_i = 0$.

The corresponding intermediate algebraic varieties are obtained by a lifting process from special zero-dimensional varieties which we call the *lifting fibers*. The lifting process is based on a division-free symbolic version of the Newton-Hensel algorithm and represents a algorithmic version of the Implicit Function Theorem. In this way, the procedure constructs the lifting fiber of step $i+1$ from the lifting fiber of step i. Each inductive step includes two cleaning phases : one is performed to throw away extraneous projective components (mainly those at infinity) and a second one reduces the size of the representation of the integers which appear during the process. This second cleaning phase is included to avoid uncontrolled growth of integer coefficients of intermediate polynomials.

Finally we show how the following two computational problems are related: the division problem in the Nullstellensatz and the numerical analysis approach to solving systems of multivariate polynomial equations.

Problem 4 (Division Problem in the Effective Nullstellensatz) *Let be given polynomials $f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_n]$ without any common zeroes (i.e. the polynomials satisfy the condition $V(f_1, \ldots, f_s) = \emptyset$), compute a non-zero integer $a \in \mathbb{Z}$, and polynomials $g_1, \ldots, g_s \in \mathbb{Z}[X_1, \ldots, X_n]$ such that*

$$a = g_1 f_1 + \cdots + g_s f_s$$

holds.

Problem 5 (Numerical Analysis Approach to Solving) *Given a real number $\varepsilon > 0$ and a regular sequence of polynomials $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ of degree at most d defining a zero-dimensional affine variety $V := V(f_1, \ldots, f_n)$, compute for any point $\alpha \in V$ an approximation $a \in \mathbb{C}^n$ at level $\varepsilon > 0$, i.e. find by an effective procedure a point $a \in \mathbb{C}$ such that*

$$||a - \alpha|| < \varepsilon$$

holds.

At first glance Problems 4 and 5 seem to be unrelated. However we shall see how the solution of Problem 4 provides lower bounds for any solution of Problem 5. We shall state this observation in terms of Liouville estimates.

In order to understand the relation between Problems 4 and 5, let us observe that in the context of Problem 5 any approximation a computer may output is necessarily rational (i.e. such an approximation must be a point a belonging to $\mathbb{Q}\ [i]^n$). Such an output is assumed to be encoded in binary (i.e. by the binary expansion of denominators and numerators of the coordinates of a).

In the past the division problem in the Nullstellensatz was studied in both number theory and computer science simultaneously. The first results mainly established upper bounds for the degree ([9], [12], [11], [29]) and height ([3], [4]) of the polynomials $g_1, \ldots, g_s$ appearing in Problem 4. The complexity study in ([19], [30], [31]) yields optimal upper bounds for both invariants (see also [16], [32], [44]) and can be applied to derive Liouville estimates in the following sense (cf. also Subsection 2.5 below):

A Liouville estimate is a lower bound for the binary length (the height) of the numerators and denominators of the coordinates of a in terms of the variety V, the point α and the real number ε in the statement of Problem 5 above. The following Theorem 2 gives such a Liouville estimate.

Let us introduce the following notions and notations: let $V \subset \mathbb{C}^n$ be a zero-dimensional diophantine variety not intersecting $\mathbb{Q}[i]^n$ and let α be a point of V. Let $\varepsilon > 0$ be a real number. We call a point $a = (\frac{a_1}{q_1}, \ldots, \frac{a_n}{q_n}) \in \mathbb{Q}[i]^n$ a rational approximation of α at level $\varepsilon > 0$, if

$$||\alpha - a|| < \varepsilon$$

holds. (Here $||\cdot||$ denotes the norm associated with the usual hermitian product in $\mathbb{C}^n$). A regular sequence $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ is said to be smooth if for any $1 \leq i \leq n$ the Jacobian $J(f_1, \ldots, f_i)$ is not a zero-divisor modulo the ideal $(f_1, \ldots, f_i)$. Observe that for a smooth regular sequence the ideals $(f_1, \ldots, f_i)$ are always radical.

Theorem 2 *There exists a universal constant C with the following property: let be given a smooth regular sequence of polynomials $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ of degree at most d and of logarithmic height at most h. Furthermore let be given a point $a \in \mathbb{Q}[i]^n$ and a real number $0 < \varepsilon \leq 1$. Suppose that the variety $V := V(f_1, \ldots, f_n)$ verifies the following conditions :*

- $V \cap \mathbb{Q}[i]^n = \emptyset$.
- *there exists a point $\alpha \in V$ such that*

$$||a - \alpha|| < \varepsilon \leq 1$$

holds. Then we have for any denominator q of a the following inequality :

$$\frac{-log_2\varepsilon}{(nd\delta)^C} - (h + \eta) \leq log_2 q,$$

where δ denotes the degree and η the (affine) logarithmic height of V.

Proof.– According to Proposition 17 below we have:

$$\frac{\varepsilon^{-1}}{|g_{n+1}(\alpha)|(2||\alpha|| + 1)} \leq q^2.$$

Thus, we look for upper bounds for $||\alpha||$ and $|g_{n+1}(\alpha)|$. First, from Proposition 10 below we have:

$$(2||\alpha|| + 1) \leq \sqrt{n}\delta 2^{2\eta}.$$

On the other hand, combining Theorem 18 and Lemma 20 below we conclude:

$$log_2|g_{n+1}(\alpha)| \leq (nd\delta)^{O(1)}(h+\eta+log_2 q).$$

¿From these two upper bounds we easily deduce the bounds of the theorem. ■

We observe that for $n=1$ Theorem 2 represents just a restatement of Liouville's classical result with somewhat coarser bounds (compare e.g. [45] Kapitel I, Satz 1).

The height estimates in [3], [4], [16], [30] and [31], combined with the methods described in subsection 2.5 below (Proposition 17) produce Liouville bounds that relate the syntactical description of V as given by the input, the approximation ε and the height of the denominator of a. In fact, these estimates yield the inequality :

$$-\,log_2\varepsilon \leq d^{O(n)} h log_2 q \qquad (1)$$

On the other hand: degree and height of the solution set represent reasonable lower time bounds for the numerical analysis approach to polynomial equation solving by rational point approximation. Exponential degrees and exponential height produce exponential lower time bounds for numerical methods of polynomial equation solving (cf. [39]).

A lower bound such as inequality (1) above, i.e. a lower bound for $log_2 q$, represents a lower bound for the output length and therefore a lower time bound for numerical methods of polynomial system solving. The results of [2], [3], [4], [7], [8], [16], [30], [31], [41], [42], [43] imply that an approximation level of $\varepsilon := 2^{d^{O(n)}}$ is sufficient in order to characterize (and to distinguish adequately) the solutions of the variety V in Problem 4. On the other hand the examples of [34], Chapitre 4, Proposition 12, and [25], [26] show that even in case of semantically and syntactically "easy" systems such an approximation level may be necessary. Therefore it becomes reasonable to fix an approximation level for numerical solving of $\varepsilon := 2^{d^n}$, where d^n represents the Bézout number of the input system. Under this assumption, inequality (1) becomes meaningless and more precise lower bounds are required.

However an exponential lower time bound for numerical solving is implicitly contained in the following corollary to Theorem 2:

Corollary 3 *Given a smooth regular sequence $f_1,\ldots,f_n \in \mathbb{Z}[X_1,\ldots,X_n]$, and points $\alpha \in V$, $a \in \mathbb{Q}\,[i]^n$ verifying the conditions of Theorem 2 above, let $\varepsilon > 0$ be a level of approximation such that $-log_2\varepsilon = d^n$ (where d^n represents the Bézout number of the system). Then we have*

$$\frac{d^n}{(nd\delta)^C} - (h+\eta) \leq log_2 q,$$

where C is a suitable universal constant as in Theorem 2. In particular, for systems of "small" degree and height, the output length for numerical solving methods is necessarily exponential in the number of variables.

For instance, we may consider the following smooth regular sequence of quadratic polynomials:

$$X_1^2 + X_1 + 1, X_2 - X_1^2, \ldots, X_n - X_{n-1}^2$$

This sequence defines a zero-dimensional variety with just two points (the degree of the variety is 2) of small height (the height is 1). Thus, for a level of approximation $\varepsilon > 0$ with $-log_2\varepsilon = 2^n$, the lower bound obtained from inequality (1) says just:

$$2^n \leq 2^{O(n)} log_2 q,$$

whereas the lower bound from Corollary 3 states that every rational approximation of level ε of either solution of this system has exponential binary length. Thus, the main consequence of this corollary is that both binary and floating point encoding of numbers in $\mathbb{Q}[i]$ are not suitable to reach the appropriate level of approximation. An alternative encoding is therefore required.

Another way out of this dilemma may consist in the following approach initiated in [46] and further developed in [47], [48], [49], [50], [14], [15] instead of approximating rationally (or similarly by floating point arithmetic) the solutions of the zero–dimensional input system $f_1, \ldots, f_n$ up to the appropriate approximation level $\varepsilon = 2^{d^n}$, we just try to find approximate zeroes (in the sense of [50]) of the system, i.e. we try to find points $a \in \mathbb{Q}[i]^n$ from which a suitable version of Newton's algorithm converges quadratically to a true zero of the system.

2 Notions, notations and Results

We are going to study the consistency question of Problem 4 (i.e. the decisional problem in the effective Nullstellensatz) only when the input system of polynomial equations $f_1, \ldots, f_r \in \mathbb{Z}[X_1, \ldots, X_n]$ verifies the conditions:

- $r \leq n + 1$,
- the sequence $f_1, \ldots, f_{r-1}$ is a smooth regular sequence

These two additional conditions are not really restrictive. As shown in [19], [20], [23], [30], [31] an effective version of Bertini's Theorem allows to reduce a general input system $f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_n]$ to such a system. We just have to find generic $\mathbb{Z}$-linear combinations of the input polynomials such that these linear combinations contain only coefficients in $\mathbb{Z}$ of logarithmic height $O(n \cdot log_2 d)$, where n is the number of variables and d is an upper bound for the degrees of the input polynomials. Under the assumption of this preprocessing we may suppose without loss of generality that our input equations satisfy the following conditions:

- the ideals $(f_1, \ldots, f_i)$ are radical, $1 \leq i \leq r - 1$,
- for $1 \leq i \leq r - 1$ the varieties $V_i = V(f_1, \ldots, f_i)$ are complete intersection affine varieties of dimension $n - i$.

Notation 4 *Given $R \subset B$ a ring extension (which converts B into a R-algebra), and an element $b \in B$, we denote by $\eta_b : B \longrightarrow B$ the R-linear endomorphism induced by the multiplication of the elements of B by b (in the following we shall call such a linear map a homothety). If B is a free R-module of finite rank, we denote by M_b the matrix of the homothety η_b and by $\chi_b \in R[T]$ the characteristic polynomial of η_b. Moreover, if R is a unique factorization domain, we shall denote by m_b the primitive minimal polynomial of η_b. Observe that χ_b and m_b are monic polynomials of $R[T]$, which for short we will call characteristic and minimal polynomial of b, respectively.*

In order to decide whether $(f_1, \ldots, f_r)$ represents the trivial ideal we just need to compute the following items:

- A linear change of coordinates $(X_1, \ldots, X_n) \longrightarrow (Y_1, \ldots, Y_n)$ such that the following $\mathbb{Q}$ -algebra homomorphism represents a Noether normalization of the variety $V(f_1, \ldots, f_{r-1})$, with the variables $Y_1, \ldots, Y_{n-r+1}$ being free:

$$R := \mathbb{Q}[Y_1, \ldots, Y_{n-r+1}] \longrightarrow \mathbb{Q}[Y_1, \ldots, Y_n]/(f_1, \ldots, f_{r-1}) =: B$$

- the matrix M_{f_r} of the homothety η_{f_r} with respect to an appropriate R-module basis.

Suppose that such a Noether normalization is available. Then the $\mathbb{Q}$ -algebra homomorphism $R \to B$ is injective and B is a free R-module of rank at most *deg* V_{r-1} (cf. [23], [24]). Under this assumption the ideal $(f_1, \ldots, f_r)$ is trivial if and only if the matrix M_{f_r} is unimodular what means that the determinant of M_{f_r} is non zero and belongs to $\mathbb{Q}$.

This comment shows how the original Problem 3 of testing consistency of polynomial equation systems can be reduced to the problem of solving polynomial equation system in a very specific geometric sense. In the next subsection we are going to explain what exactly we mean by this, namely geometric solving.

2.1 Geometric Solving

The previous considerations reduce the search for a consistency test for the polynomial equation system $f_1 = 0, \ldots, f_n = 0$, namely Problem 3, to the problem of computing a Noether normalization of the variety $V(f_1, \ldots, f_{r-1})$ and the matrix M_{f_r} of the homothety η_{f_r} with respect to a suitable R-module basis. Assume that $X_1, \ldots, X_n$ are already in Noether position with respect to the variety $V(f_1, \ldots, f_{r-1})$, the variables $X_1, \ldots, X_{n-r+1}$ being free. Then we consider the following integral ring extension

$$R := \mathbb{Q}[X_1, \ldots, X_{n-r+1}] \longrightarrow \mathbb{Q}[X_1, \ldots, X_n]/(f_1, \ldots, f_{r-1}) =: B.$$

Our assumptions on $f_1, \ldots, f_{r-1}$ imply that B is a reduced algebra and a finite free R-module. We are now going to explain what we mean by "geometric solving" or "geometric solution". First we need the following notion of *primitive element* of B:

Definition 5 *Let R be a ring of polynomials over $\mathbb{Q}$ and $R \subseteq B$ an integral ring extension such that B is reduced and B is a free R-module of finite rank. An element*

$u \in B$ is called a primitive element of the ring extension $R \subseteq B$ if the degree of the minimal polynomial m_u of u equals the rank of B as free R-module, i.e. if

$$deg\ m_u = rank_R\ B$$

holds.

Let K be the quotient field of R and $B' = K \otimes_R B$ be the localization of B by the non-zero elements of R. An element $u \in B$ is a primitive element of B if and only if for $D := rank_r B = dim_k B'$ the set $\{1, u, \ldots, u^{D-1}\}$ represents a K-vectorspace basis of B'.

The computation of the matrix M_{f_r} is a consequence of the following "generic point" description of the K-algebra B': this algebra is characterized by the following items (which our algorithm will compute):

- a K-vectorspace basis of B'
- for $n-r+2 \leq i \leq n$ the matrices M_{X_i} of the homotheties $\eta_{X_i} : B \longrightarrow B$ with respect to the given basis (these matrices describe the multiplication tensor of the K-algebra B' and hence also of the R-algebra B)

We then obtain the matrix $M_{f_{r+1}}$ by substituting for the variables $X_{n-r+2}, \ldots, X_n$ appearing in the polynomial $f_{r+1}(X_1, \ldots, X_n)$ just the matrices $M_{X_{x-r+2}}, \ldots, M_{X_n}$. (In the sequel we shall write for short $M_{f_{r+1}} = f_{r+1}(M_{X_{n-r+2}}, \ldots, M_{X_n})$ for this substitution, interpreting f_{r+1} as an element of the polynomial ring $R[X_{n-r+2}, \ldots, X_n]$).

In this sense, geometric solving means just computing both a basis of the K-algebra B' and the matrices $M_{X_{n-r+1}}, \ldots, M_{X_n}$. This is done making use of a suitable primitive element of B.

In the context of this paper, the primitive element $u \in B$ will always be chosen as the image in B of a generic $\mathbb{Z}$-linear form of the variables $X_{n-r+2}, \ldots, X_n$. In particular, we may assume that u is the image of a linear form $U = \lambda_{n-r+2}X_{n-r+2} + \cdots + \lambda_n X_n$, with $\lambda_i \in \mathbb{Z}$ for $n-r+2 \leq i \leq n$. Let T be a new indeterminate. The minimal polynomial $m_u(T)$ of u as an element of the R-algebra B (or equivalently as an element of the K-algebra B') will be a monic polynomial in $\mathbb{Q}[X_1, \ldots, X_{n-r+1}, T] = \mathbb{Q} \otimes_{\mathbb{Z}} R[T]$.

We shall shall choose this minimal polynomial as an element of $\mathbb{Z}[X_1, \ldots, X_{n-r+1}, T] = R[T]$. In the sequel we shall pay special attention to the case $r = n+1$, where we have $R = \mathbb{Z}$, $K = \mathbb{Q}$ and where m_u is a polynomial of $\mathbb{Z}[T]$ of positive degree (the polynomial m_u is then trivially monic over $\mathbb{Q}[T]$ since we may divide it by its leading coefficient, which is a non-zero integer). Discarding the content (the maximum common divisor) of the coefficients of m_u, we may replace the minimal polynomial m_u by its primitive counterpart which we shall always denote by q_u. Similarly, for the case $r \leq n$, we shall replace the minimal polynomial $m_u \in \mathbb{Z}[X_1, \ldots, X_{n-r+1}, T] = R[T]$ by some "cleaner" (however not necessarily primitive) version q_u.

Finally, as $\{1, u, \ldots, u^{D-1}\}$ is a basis of the K-vector space B', for $n-r+2 \leq i \leq n$ there are polynomials $v_i^{(u)} \in R[T]$ and non-zero elements $\rho_i^{(u)} \in R$ such that $\rho_i^{(u)} X_i - v_i^{(u)}(U)$

belongs to the ideal $(f_1, \ldots, f_{r-1})$ in $K[X_{n-r+2}, \ldots, X_n]$. In particular, we have the following identity between ideals of $K[X_{n-r+2}, \ldots, X_n]$:

$$(f_1, \ldots, f_n) = (q_u(U), \rho_1^{(u)} X_1 - v_1^{(u)}(U), \ldots, \rho_n^{(u)} X_n - v_n^{(u)}(U)).$$

Moreover, if M denotes the companion matrix of the homothety η_u with respect to the basis $\{1, u, \ldots, u^{D-1}\}$, the matrices $M_{X_{n-r+2}}, \ldots, M_{X_n}$ characterizing the multiplication tensor of the R-algebra B (or equivalently of the K-algebra B') are given by the formula

$$M_{X_i} = \rho_i^{(u)\ -1} \cdot v_i^{(u)}(M)$$

for $n - r + 2 \leq i \leq n$. To simplify notations we shall often omit the superindex (u) when refering to these polynomials. After these explanations we shall assume without loss of generality that we have $r := n + 1$ in the statement of Problems 3 and 4. Consequently we restrict the meaning of "geometric solving" to the case where we have given as input polynomials $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ forming a regular sequence in $\mathbb{Q}[X_1, \ldots, X_n]$ (we shall say in the future for short that $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ is a regular sequence). With these conventions "geometric solving" means the following:

Definition 6 *An algorithm for geometric solving is a procedure which from a smooth regular sequence $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ as input produces:*

- *a primitive element u of the ring extension $\mathbb{Q} \longrightarrow \mathbb{Q}[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$ represented by a $\mathbb{Z}$-linear form $U = \lambda_1 X_1 + \cdots + \lambda_n X_n$*
- *the primitive minimal polynomial $q_u \in \mathbb{Z}[T]$*
- *the parametrizations of the variety $V(f_1, \ldots, f_n)$ by the zeroes of q_u, namely the (unique) primitive polynomials $\rho_1^{(u)} X_1 - v_1^{(u)}(T), \ldots, \rho_n^{(u)} X_n - v_n^{(u)}(T)$ with $\rho_1^{(u)}, \ldots, \rho_n^{(u)}$ non-zero integers and $v_1^{(u)}, \ldots, v_n^{(u)} \in \mathbb{Z}[T]$ which satisfy the conditions $max\{deg\ v_1^{(u)}, \ldots, deg\ v_n^{(u)}\} < deg\ q_u$ and $(f_1, \ldots, f_n) = (q_u, \rho_1^{(u)} X_1 - v_1^{(u)}(T), \ldots, \rho_n^{(u)} X_n - v_n^{(u)}(T))$ in $\mathbb{Q}[X_1, \ldots, X_n]$. Moreover, the non-zero integer $\rho := \prod_{i=1}^n \rho_i \in \mathbb{Z}$, called a discriminant of the input system, is a multiple of the discriminant of q_u.*

In the sequel we shall refer to the polynomials $U = \lambda_1 X_1 + \cdots + \lambda_n X_n \in \mathbb{Z}[X_1, \ldots, X_n]$ (with image u in $\mathbb{Q}[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$), $q_u(T), v_1^{(u)}(T), \ldots, v_n^{(u)}(T) \in \mathbb{Z}[T]$ and $\rho_1^{(u)}, \ldots, \rho_n^{(u)} \in \mathbb{Z}$ as "geometric solution" of the equation system $f_1 = 0, \ldots, f_n = 0$.

2.2 Intrinsic Parameters

We said in the introduction that we are interested in algorithms for geometric solving which are able to profit from "good" geometrical properties that an input system of polynomial equations might possess. This makes it necessary to precise what such "good" geometrical properties may be and how to find measures for them. Therefore, we are going to define two geometric invariants in this subsection that will arise as parameters of the complexity of our procedures: the (affine) degree and the (affine) logarithmic height of complete intersection varieties. The notion of degree has been taken directly from [24], while our notion of height is strongly inspired by the corresponding notion developed for projective varieties in [37], [38], [40], [41], [42], [43].

Let us first recall the notion of degree of an affine algebraic variety. We begin by defining the degree of a zero-dimensional variety and then we extend this notion to positive dimensional complete intersection algebraic varieties.

To fix notations, let $V \subseteq \mathbb{C}^n$ be an algebraic subset (variety) given as the set of common zeroes in $\mathbb{C}^n$ of a smooth regular sequence of polynomials $f_1, \ldots, f_i \in \mathbb{Z}[X_1, \ldots, X_n]$ of degree at most d. If V is zero-dimensional (i.e. if $i = n$) the degree of V is defined as the number of points of V (points at infinity are not counted in this definition). In the general case (when $dim\ V = n - i \geq 1$ holds) let us consider the class $\mathcal{D}$ of all affine linear subspaces of $\mathbb{C}^n$ of dimension i (defined as the set of solutions in $\mathbb{C}^n$ of a linear equation system $L_1 = 0, \ldots, L_{n-i} = 0$ where $L_k = a_{k1}X_1 + \cdots + a_{kn}X_n + a_{k0}$ is an affine linear polynomial with coefficients $a_{kj} \in \mathbb{Z}$ for $1 \leq k \leq n - i$ and $0 \leq j \leq n$). Let $\mathcal{D}_V$ be the subclass of $\mathcal{D}$ of all these affine linear spaces $H \in \mathcal{D}$ such that $H \cap V$ is a zero-dimensional variety.

Definition 7 *Let notations and assumptions be as before. The degree of V is defined as the maximum of the degrees of the intersections of V with affine linear spaces belonging to $\mathcal{D}_V$. We denote the degree of V by $deg\ V$.*

As observed in [24], this definition of the degree never yields infinity, but gives always a natural number. Our definition is equivalent to the following one: Consider all linear changes of coordinates in $\mathbb{C}^n$ defined by non-singular matrices with integer entries, i.e. linear changes of the type

$$(X_1, \ldots, X_n) \mapsto (Y_1, \ldots, Y_n),$$

where $Y_k = a_{k1}X_1 + \cdots + a_{kn}X_n$ is a linear form with integer coefficients for $1 \leq k \leq n$. Any generic linear change of coordinates induces an integral ring extension as follows:

$$\mathbb{Q}[Y_1, \ldots, Y_{n-i}] \longrightarrow \mathbb{Q}[Y_1, \ldots, Y_n]/(f_1, \ldots, f_i) = \mathbb{Q}[V].$$

It turns out that the ring $\mathbb{Q}[V]$ is a free $\mathbb{Q}[Y_1, \ldots, Y_{n-i}]$-module of finite rank (cf. [23] for instance). This rank is the same for any generic linear coordinate change and it equals the degree of the variety V.

In order to define the height of an affine diophantine variety, we also consider first the zero-dimensional case and then the case of positive dimension.

To start with let us first say what we mean by the (logarithmic) height of an integer, a vector of integers, a matrix over $\mathbb{Z}$ and a polynomial with integer coefficients. Let $a \in \mathbb{Z}$ be an integer, then the *height* of a is defined as $ht(a) := max\{log_2|a|, 1\}$. It is obvious that the height measures the bit length of a. On the other hand we shall see soon that this simple notion of height of an integer has a natural extension to algebraic varieties where it plays a rôle of "arithmetic degree" (see [8], [5], [18], [30], [31][41], [42], [43]). The main outcome of this paper will be the reinterpretation of the notion of height for algebraic varieties as a measure for the bit complexity of an elimination procedure. In this sense, our contribution justifies a posteriori Northcott's terminology of "complexity" for the height of an algebraic variety [52].

For a vector of integer numbers $\alpha := (a_1, \ldots, a_n) \in \mathbb{Z}^n$, we define the height $ht(\alpha)$ as the maximum of the heights of its coordinates. For a matrix $A \in \mathcal{M}_n(\mathbb{Z})$ with integer entries, its height $ht(A)$ is defined as the height of A as vector. Similarly, we define the height of a polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$ as the height of the vector of its coefficients.

Definition 8 *Given a zero-dimensional diophantine algebraic variety $V \subseteq \mathbb{C}^n$ and a linear form $U = \lambda_1 X_1 + \cdots + \lambda_n X_n$ with integer coefficients representing a primitive element u of the ring extension $\mathbb{Q} \longrightarrow \mathbb{Q}[V]$, we define the height of V with respect to U as the maximum of the heights of the polynomials $q_u(T), \rho_1^{(u)} X_1 - v_1^{(u)}(T), \ldots, \rho_n^{(u)} X_n - v_n^{(u)}(T)$ (as introduced in Definition 6) and denote this height by $ht(V;U)$.*

In our first approach to find a suitable notion of height for algebraic varieties we define the height of the given zero-dimensional variety V as the function $ht_V : \mathbb{N} \longrightarrow \mathbb{N}$ which associates to any natural number $c \in \mathbb{N}$ the value $ht_V(c) := max\{ht(V;u) : ht(u) \leq c\}$ if the ring extension $\mathbb{Q} \longrightarrow \mathbb{Q}[V]$ has a primitive element of height at most c and which associates to c the value 1 if no such primitive element exists.

This notion of height is related to the hermitian norm and the denominator of the points of the variety V. In order to explain this relation, let us introduce the following notations :

Taking into account that the zero-dimensional variety V is contained in $\mathbb{C}^n$, we define the norm $||V||$ as:

$$||V|| := max\{||\alpha|| : \alpha \in V\}.$$

Furthermore, a natural number $d \in \mathbb{N}$ is called a *denominator of* V if all elements in the set

$$d \cdot V := \{d \cdot \alpha : \alpha \in V\}$$

have algebraic integers as coordinates. The smallest denominator of V will be called *the* denominator of V and denoted by d_V.

With these notations we are able to state the following height estimation for zero-dimensional varieties:

Lemma 9 *There exists a universal constant $\kappa > 0$ such that for any zero-dimensional diophantine subvariety V of $\mathbb{C}^n$ and any $c \in \mathbb{N}$ the following inequality holds:*

$$ht_V(c) \leq \delta^{\kappa}(c + log_2(nd_V||V||)).$$

(This means the function ht_v is of order $ht_V(c) = \delta^{O(1)}(c + log_2(nd_V||V||))$).

Proof.– Let $V \subset \mathbb{C}^n$ be a zero-dimensional diophantine variety of degree $\delta \in \mathbb{N}$. The inequality is trivial for $ht_V(c) = 1$. Therefore we may suppose without loss of generality that the ring extension $\mathbb{Q} \longrightarrow \mathbb{Q}[V]$ has a primitive element u which is the image of a linear form $U = \lambda_1 X_1 + \cdots + \lambda_n X_n \in \mathbb{Z}[X_1, \ldots, X_n]$ of height at most c. We just show the inequality:

$$2^{ht(q_u(T))} \leq (2^{c+1} n d_V ||V||)^{\delta}$$

and leave the corresponding inequalities for $\rho_1^{(u)} X_1 - v_1^{(u)}(T), \dots, \rho_n^{(u)} X_n - v_n^{(u)}(T))$ to the reader. Since d_V is a denominator for V and u has integer coordinates, d_V is also a denominator for the set of algebraic numbers $u(V)$ contained in $\mathbb{C}$. Therefore, if $\alpha_1, \dots, \alpha_\delta \in \mathbb{C}^n$ are the points of V and if T is a new indeterminate, the polynomial

$$f(T) := \prod_{i=1}^{\delta} (T - d_V u(\alpha_i))$$

has integer coefficients, i.e. $f(T)$ belongs to $\mathbb{Z}[T]$. Moreover, the polynomial $f(d_V T)$ vanishes on the set $u(V)$. Since f and q_u have the same degree δ and since q_u is the primitive minimal polynomial of the image u of U in $\mathbb{Q}[V]$, the vanishing of $f(d_V T)$ on $u(V)$ implies that the existence of a non-zero integer $b \in \mathbb{Z}$ such that $f(T) = b q_u(T)$ holds. Taking into account $|b| \geq 1$ and that the coefficients of f are elementary symmetric functions in the points of the set $u(V) \subset \mathbb{C}$ we deduce the following inequalities:

$$2^{ht(q_u)} \leq 2^{ht(f)} \leq (2d_V ||u(V)||)^{\delta} \leq (2d_V)^{\delta} (n 2^c)^{\delta} ||V||^{\delta} \leq (2^{c+1} n d_V ||V||)^{\delta}.$$

■

Let V be again a zero-dimensional diophantine subvariety of $\mathbb{C}^n$ of degree δ. We estimate now the quantities d_V and $||V||$.

Proposition 10 *Let $c \in \mathbb{N}$ be a natural number such that the ring extension $\mathbb{Q} \longrightarrow \mathbb{Q}[V]$ has a primitive element $u := \lambda_1 X_1 + \cdots + \lambda_n X_n \in \mathbb{Z}[X_1, \dots, X_n]$ of height at most c. Then d_V and $||V||$ can be estimated as follows:*

i)

$$d_V \leq |a_\delta^{\delta-1} \prod_{i=1}^{n} \rho_i^{(u)}|,$$

where a_δ is the leading coefficient of $q_u(T)$ and $\prod_{i=1}^n \rho_i^{(u)}$ is the discriminant obtained from the polynomials in Definition 6. It follows that V has denominators of height $O((n+\delta) ht_V(c))$.

ii) the norm $||V||$ of V satisfies

$$||V|| \leq \sqrt{n} \delta 2^{\delta ht_V(c)}.$$

Proof.– The integer $|a_\delta|$ is a denominator of the set $u(V)$ because it is the leading coefficient of the polynomial $q_u(T)$ which defines $u(V)$. Since the polynomials $\rho_1^{(u)} X_1 - v_1^{(u)}(T), \dots,$ $\rho_n^{(u)} X_n - v_n^{(u)}(T)$ "parametrize" the variety V in function of the zeroes of $q_u(T)$, i.e. in function of the set $u(V)$, we deduce that $|a_\delta^{\delta-1} \prod_{i=1}^n \rho_i^{(u)}|$ is a denominator of V (notice that the degree of the polynomials $v_1^{(u)}(T), \dots, v_n^{(u)}(T)$ is bounded by $\delta - 1$).

¿From [34] Chapitre IV, Theoreme 2 (ii) one deduces :

$$||u(V)|| \leq 2^{ht_V(c)}.$$

Thus, for $\alpha = (\alpha_1, \ldots, \alpha_n) \in V$ and $1 \leq k \leq n$ we have:

$$|\alpha_k| = |\rho_k^{(u)}|^{-1} |v_k^{(u)}(u(\alpha))|.$$

Since $\rho_k^{(u)}$ is an integer and $v_k(T)$ is a polynomial of degree at most $\delta - 1$ and of height at most $2^{ht_V(c)}$, we conclude :

$$|\alpha_k| \leq \delta 2^{ht_V(c)} ||u(V)||^{\delta-1} \leq \delta 2^{\delta ht_V(c)}.$$

This implies

$$||V|| := max\{||\alpha|| : \alpha \in V\} \leq \sqrt{n}\delta 2^{\delta ht_V(c)}.$$

■

Remark 11 *The height is deeply related to complexity issues in polynomial equation solving. In fact, given a regular sequence of polynomials* $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ *defining a zero-dimensional diophantine variety* V *, we have an upper bound for the length of the output of any algorithm which solves the system* $f_1 = 0, \ldots, f_n = 0$ *geometrically, namely:*

$$(n+1) deg\ V\ \ ht_V(c).$$

Here we assume tacitly that the output is given by a linear form representing a primitive element of the ring extension $\mathbb{Q} \longrightarrow \mathbb{Q}[V]$ *and by polynomials as in Definition 6 and that these polynomials are given in dense and their coefficients in bit representation.*

It is also possible to give an upper bound for the height of zero-dimensional complete intersection varieties in terms of purely syntactical properties of its defining equations. This is the content of what follows, namely a weak form of the so-called arithmetical Bézout theorem ([3], [4], [7], [8], [16], [41], [42], [43], [30], [31]).

Proposition 12 *Let* $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ *be polynomials of degree at most* d *and of height at most* h *. Suppose they define a zero-dimensional variety* $V := V(f_1, \ldots, f_n)$ *. Then the function* ht_V *can be estimated as follows: for any* $c \in \mathbb{N}$ *we have*

$$ht_V(c) = d^{O(n)} \cdot h \cdot c.$$

Proposition 12 is an immediate consequence of [30]. Under the same assumptions as in Remark 11, namely that any algorithm which solves a given zero-dimensional complete intersection polynomial equation system returns a primitive element and polynomials as in Definition 6, we can state the following obvious *lower bound* for the bit length of the output (again we suppose that the output polynomials as in Definition 6 are given in dense and their coefficients in bit representation):

Proposition 13 *Let $f_1, \dots, f_n \in \mathbb{Z}[X_1, \dots, X_n]$ be a regular sequence defining a zero-dimensional diophantine variety $V = V(f_1, \dots, f_n)$. Let*

$$\eta := min\{ht(V; u) : u \text{ is a primitive element of the ring extension } \mathbb{Q} \longrightarrow \mathbb{Q}[V]\}.$$

Then, the bit time complexity of any algorithm which solves $f_1 = 0, \dots, f_n = 0$ geometrically, is at least:

$$max\{deg\ V, \eta\}.$$

Let us now consider the case of diophantine complete intersection variety V of positive dimension. Let $1 \leq i < n$ and let be given a smooth regular sequence of polynomials $f_1, \dots, f_i \in \mathbb{Z}[X_1, \dots, X_n]$ defining a $(n-i)$-dimensional diophantine complete intersection variety V. Let $\mathcal{N}_V$ be the class of all linear coordinate changes:

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} \times \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix},$$

such that the matrix $A = (a_{ij})_{1 \leq i,j \leq n}$ has integer entries (i.e. $A \in \mathcal{M}_n(\mathbb{Z})$, where $\mathcal{M}_n(\mathbb{Z})$ denotes the ring of $n \times n$ matrices of $\mathbb{Z}$), A is non-singular and such that the ring extension

$$\mathbb{Q}[Y_1, \dots, Y_{n-i}] \longrightarrow \mathbb{Q}[Y_1, \dots, Y_n]/(f_1, \dots, f_i) = \mathbb{Q}[V] \tag{2}$$

is integral. The linear coordinate change given by the matrix A induces a *finite* morphism of affine varieties $\pi : V \longrightarrow \mathbb{C}^{n-i}$. We consider for any linear form $U = \lambda_{n-i+1}X_{n-i+1} + \dots + \lambda_n X_n$ with integer coefficients such that its image u in $\mathbb{Q}[V]$ is a primitive element of the ring extension above, the class $\mathcal{F}_u$ of all those points $a \in \mathbb{Z}^{n-i}$ which have unramified π-fiber and for which the image of u in the coordinate ring $\mathbb{Q}[V_a]$ of the fiber $V_a := \pi^{-1}(\{a\})$ remains a primitive element of the ring extension $\mathbb{Q} \longrightarrow \mathbb{Q}[V_a]$.

In a more down-to-earth language this means that we ask all the elements of $V_a = \pi^{-1}(a)$ to be smooth points of V and the number $deg\ V_a$ of elements of V_a to be equal to the rank of the free $\mathbb{Q}[Y_1, \dots, Y_{n-i}]$-module $\mathbb{Q}[V]$. Furthermore we ask the linear form U to generate a primitive element of the ring extension $\mathbb{Q} \longrightarrow \mathbb{Q}[V_a]$. (Observe that everything comes together since the smoothness of the elements of V_a implies that the zero-dimensional $\mathbb{Q}$-algebra $\mathbb{Q}[V_a]$ is reduced.) Maintaining these notations we model our notion of height of algebraic varieties by means of the following function:

Definition 14 *Given V a complete intersection diophantine variety as before, a linear change of coordinates $A \in \mathcal{N}_V$, a linear form $U \in \mathbb{Z}[Y_{n-i+1}, \dots, Y_n]$ whose image u in $\mathbb{Q}[V]$ is a primitive element of the integral ring extension (2) and given a point $a \in \mathcal{F}_u$, we define the height of V with respect to the triple (A, U, a) as:*

$$ht(V; (A, U, a)) := ht(V_a; U).$$

Our first approximation to the notion of height of a diophantine complete intersection variety is given by the function $ht_V : \mathbb{N} \longrightarrow \mathbb{N}$ which associates to any natural number $c \in \mathbb{N}$ the value $ht_V(c) := max\{ht(V; (A, U, a)) \mid ht(A, U, a) \leq c\}$ if the triple (A, U, a) satisfies the assumptions of this definition, and which associates to c the value 1 if not.

2.3 Straight–line Programs

In the previous subsections we discussed the mathematical form and syntactical encoding of the output of an algorithm for geometric solving we are going to exhibit. However we also need a suitable encoding for input and intermediate results of our algorithm. As mathematical objects our inputs are polynomials with integer coefficients $f \in \mathbb{Z}[X_1, \ldots, X_n]$. These polynomials can be written as lists of monomials and this yields the first two possible encodings for input and intermediate results: dense and sparse encoding. Thus, if d is the degree of f and if h is an upper bound for its height, the length of f under dense encoding is

$$h \cdot \binom{d+n}{n} = h \cdot \binom{d+n}{d}.$$

Let us remark that the binomial coefficients appearing in this expression are polynomial in the number of variables in the case of “small” degree polynomials (e.g. the length of the dense encoding of f is $h \cdot \binom{n+2}{2} \simeq h \cdot n^2$ if the degree of f is at most 2). Analogously the length of the dense encoding of f is polynomial in d for $d >> n$.

Alternatively, our input polynomial f may be given by representing just all its non-zero coefficients: this is the sparse encoding of the polynomial f. Then, if h is a bound of the height, d the degree and N the number of monomials with non-zero coefficients of f, the length of the sparse encoding of f becomes

$$h \cdot N \cdot n \cdot log_2 d.$$

However, in many practical applications our input polynomials may be given as programs. This is for instance the approach in the encoding of the inputs of the version of the 3SAT problem (Problem 1) we stated in the introduction. In the sequel we shall mainly restrict ourselves to the straight–line program encoding of polynomials in the following sense:

Definition 15 *A generic straight–line program Γ' over $\mathbb{Z}$ is a pair $\Gamma' = (\mathcal{G}, Q)$, where $\mathcal{G}$ is a directed acyclic graph and Q is an assignment of instructions to the gates (i.e. vertices) of the graph. $\mathcal{G}$ contains $n+1$ gates of indegree 0 which are Q-labeled by the variables $X_1, \ldots, X_n$ and by the constant $1 \in \mathbb{Z}$. They are called the input gates of Γ'. We define the depth of a gate ν of the graph $\mathcal{G}$ as the length of the longest path joining ν and some input gate. Let us denote the gates of the directed acyclic graph $\mathcal{G}$ by pairs of integer numbers (i,j), where i represents the depth of the gate and j is the corresponding value of an arbitrary numbering imposed on the set of gates of depth i (this encoding can be seen in [22], [30], [35], [36], [39]). Associated to the gate (i,j) we have the following operation:*

$$Q_{i,j} := (\sum_{0 \leq r \leq i-1} A_{i,j}^{rs} Q_{rs}) \cdot (\sum_{0 \leq r' \leq i-1} B_{i,j}^{r's'} Q_{r's'}),$$

where $A^{rs}_{i,j}, B^{r's'}_{i,j}$ *are indeterminates called parameters of* Γ' *and* $Q_{rs}, Q_{r's'}$ *are precomputed values corresponding to the gates* (r,s) *and* (r',s').

We denote by $\bar{A} = (A^{rs}_{ij}), \bar{B} = (B^{r's'}_{ij})$ the list of all parameters in the straight–line program Γ'. The intermediate results Q_{ij} of Γ' are therefore polynomials belonging to $\mathbb{Z}[\bar{A}, \bar{B}, X_1, \ldots, X_n]$ and Γ' represents a procedure which evaluates them. A (finite) set of polynomials $f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_n]$ is said to be evaluated by a straight–line program of generic type Γ' with parameters in a set $\mathcal{F} \subseteq \mathbb{Z}$ if specializing the coordinates of the parameters $\bar{A}$ and $\bar{B}$ in Γ' to values in $\mathcal{F}$, there exist gates $(i_1, j_1), \ldots, (i_s, j_s)$ of Γ' such that

$$f_k = Q_{i_k j_k}(\bar{a}, \bar{b}, X_1, \ldots, X_n)$$

holds for $1 \leq k \leq s$. Specializing in the indicated way the parameters of Γ' into values of $\mathcal{F}$ we obtain a copy Γ of the directed acyclic graph $\mathcal{G}$ underlying the generic straight–line program Γ' and of its instruction assignment Q. We call this copy Γ a *straight–line program (of generic type* Γ' *) in* $\mathbb{Z}[X_1, \ldots, X_n]$ *with parameters in* $\mathcal{F}$. The gates of Γ correspond to polynomials belonging to $\mathbb{Z}[X_1, \ldots, X_n]$. These polynomials are obtained from the intermediate results Q_{ij} of Γ' by specializing adequately the parameters from which the depend. We shall call these polynomials the intermediate results of the straight–line program Γ. Furthermore the polynomials $f_1, \ldots, f_s$ are called (final) results or outputs of Γ. Alternatively, we shall say that $f_1, \ldots, f_s$ are represented, computed or evaluated by Γ.

The current complexity measures for the generic straight–line program Γ' are:

- the size of Γ' = the size of the graph $\mathcal{G}$
- the non-scalar depth (Γ') = the depth of the graph $\mathcal{G}$

The size and non-scalar depth of the specialized straight–line program Γ are analogously defined. Additionally, for any straight–line program Γ in $\mathbb{Z}[X_1, \ldots, X_n]$ with parameters in $\mathcal{F} \subseteq \mathbb{Z}$, we call the the maximum of the heights of the elements in $\mathcal{F}$ *the height of the parameters of* Γ or, for short, the *height of* Γ. The encoding of a polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$ by a straight–line program Γ in $\mathbb{Z}[X_1, \ldots, X_n]$ with parameters of height h has (bit) length

$$2(L^2 h + L log_2 L).$$

Note that the notion of straight–line program encoding covers as well both notions of dense and sparse encoding of polynomials. This can be seen as follows: a polynomial of degree at most d and height at most h, given in dense encoding, can be evaluated by a straight–line program of size $O(d\binom{d+n}{n})$ and non-scalar depth $O(log_2 d)$ with parameters of height at most h. Similarly, if a polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$ has degree at most d, height h and N non-zero coefficients, it can be evaluated by a straight–line program of size $O(d \cdot N)$ and non-scalar depth $O(log_2 d)$ with parameters of height at most h.

2.4 Complexity of geometric solving

Now that the notions of geometric solving, degree and height of polynomial equation systems and straight–line programs and its distinct complexity measures have been introduced, we are able to state our main result, namely the following Theorem 16. This theorem represents our principal contribution to the solution of Problem 3 in Section 1.

Theorem 16 *There exists a bounded error probabilistic Turing machine that from a smooth regular sequence $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ outputs a linear form $U \in \mathbb{Z}[X_1, \ldots, X_n]$ representing a primitive element u of the ring extension $\mathbb{Q} \longrightarrow \mathbb{Q}[V]$, where $V := V(f_1, \ldots, f_n)$ is the algebraic variety defined by $f_1, \ldots, f_n$, and polynomials of the form $q_u(T), \rho_1^{(u)} X_1 - v_1^{(u)}(T), \ldots, \rho_n^{(u)} X_n - v_n^{(u)}(T)$ with $\rho_1^{(u)}, \ldots, \rho_n^{(u)}$ non-zero integers and $q_u, v_1^{(u)}, \ldots, v_n^{(u)} \in \mathbb{Z}[T]$ such that these polynomials represent a geometric solution of the equation system $f_1 = 0, \ldots, f_n = 0$ (see Definition 6). The Turing machine finds this solution in time (counting the number of bit operations executed)*

$$(ndhL\delta\eta)^{O(log_2 n + \ell)}$$

using only

$$(ndL\delta)^{O(1)}$$

arithmetic operations in $\mathbb{Z}$ at unit cost. We assume that the polynomials $f_1, \ldots, f_n$ have degree at most d and that they are given by a straight–line program of size L and non-scalar depth ℓ with parameters of height at most h. The quantity δ defined by $\delta := max\{deg\ V(f_1, \ldots, f_i) : 1 \leq i \leq n\}$ is the degree of the system $f_1 = 0, \ldots, f_n = 0$. Finally the quantity η is the height of the system $f_1 = 0, \ldots, f_n = 0$ defined as $\eta := max\{ht_{V_i}(c_3((log_2 n + \ell) \cdot log_2 \delta)) : 1 \leq i \leq n\}$ where $c_3 > 0$ is a suitable universal constant independent of the specific input $f_1, \ldots, f_n$ (or even its size).

Theorem 16 follows from the description of the algorithm given in Section 3 below. Theorem 1 above follows immediately from Theorem 16 above by putting $d := 2$, $L := n$, $\ell := 2$. Let us remark here that Theorem 16 improves and extends the main result of [21] and [22] to the bit complexity model. It sheds also new light on the main complexity outcome of the papers [50], [17], [10].

2.5 A Division Step in the Nullstellensatz

In this subsection we show how Nullstellensatz bounds imply Liouville estimates. This establishes a close connection between Problems 4 and 5 in the Introduction. Let us recall the assumptions in the statement of Theorem 2.

There is given a smooth regular sequence of polynomials $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ of degree at most d and of height at most h, defining a zero-dimensional affine variety $V := V(f_1, \ldots, f_n) \subseteq \mathbb{C}^n$. Moreover there is given a point $\alpha = (\alpha_1, \ldots, \alpha_n) \in V$ and a real number $0 < \varepsilon \leq 1$. Finally, we assume that $V \cap \mathbb{Q}[i]^n = \emptyset$ holds. By a well-chosen linear change of coordinates we may assume without loss of generality $V \cap (\mathbb{Q}[i] \times \mathbb{C}^{n-1}) = \emptyset$. It is sufficient to show that the algebraic number α_1 is hard to approximate in the sense of the conclusion of Theorem 2. For this purpose consider integers $p \in \mathbb{Z}[i]$ and $q \in \mathbb{N}$ such that $\frac{p}{q}$ is an approximation at level ε to the algebraic number α_1.

We introduce the following polynomial :

$$f_{n+1} := (qX_1 - p)(qX_1 - \bar{p})$$

(here $\bar{p}$ stands for the complex conjugate of p). The assumption $V \cap (\mathbb{Q}[i] \times \mathbb{C}^{n-1}) = \emptyset$ implies that the sequence of polynomials $f_1, \ldots, f_{n+1}$ has no common zero in $\mathbb{C}^n$. Therefore there exists a non-zero integer $b \in \mathbb{Z}$ and polynomials $g_1, \ldots, g_{n+1} \in \mathbb{Z}[X_1, \ldots, X_n]$ such that the following Bézout identity holds :

$$b = g_1 f_1 + \cdots + g_{n+1} f_{n+1}.$$

Evaluating this identity at the point $\alpha \in V$ we obtain :

$$1 \leq |b| = |g_{n+1}(\alpha)| \cdot |q\alpha_1 - p| \cdot |q\alpha_1 - \bar{p}|.$$

This yields the following estimate:

Proposition 17 *With assumptions and notations as before, for any rational approximation $a := (p_1/q, \ldots, p_n/q) \in \mathbb{Q}[i]^n$ at level ε to the point $\alpha \in V$ we have the inequality :*

$$\frac{1}{|g_{n+1}(\alpha)|q^2} \leq ||a - \alpha||(|\alpha_1| + |\frac{p_1}{q}|).$$

In particular, for $||a - \alpha|| < \varepsilon \leq 1$, we obtain the estimation :

$$\frac{\varepsilon^{-1}}{|g_{n+1}(\alpha)|(2||\alpha|| + 1)} \leq q^2.$$

(Here $p_1, \ldots, p_n \in \mathbb{Z}[i]$ are Gaussian integers and $q \in \mathbb{N}$ is a natural number.)

¿From the second inequality we deduce that it is sufficient to bound the values of $||\alpha||$ and $|g_{n+1}(\alpha)|$ in order to obtain a Liouville estimate for the rational approximation a of the point α. Note that the bounds for $||\alpha||$ and $|g_{n+1}(\alpha)|$ which can be easily deduced from the known Nullstellensätze (as e.g. in [3], [4], [30]) would be insufficient for our purpose (proving Theorem 2) as they imply only a unspecific general estimate, namely

$$\frac{-log_2 \varepsilon}{d^{Cn} h} < log_2 |q|$$

for a suitable constant $C > 0$. A Liouville estimate of this type does not take into account the specific properties of the variety V expressed through its degree and height. The more specific bounds for $||\alpha||$ and $|g_{n+1}(\alpha)|$ as required for the proof of Theorem 2 by means of Proposition 17 are an immediate consequence of the following result:

Theorem 18 *Let $f_1, \ldots, f_n, f_{n+1} \in \mathbb{Z}[X_1, \ldots, X_n]$ polynomials having no common zero in $\mathbb{C}^n$ and verifying the following assumptions:*

- *there exists a straight–line program of size L and non-scalar depth ℓ with parameters of height h that evaluates the polynomials $f_1, \ldots, f_n, f_{n+1}$*

- *the degrees of the polynomials* $f_1, \ldots, f_{n+1}$ *are bounded by* d *and* h' *is an upper bound for their heights*

Let us furthermore assume that $f_1, \ldots, f_n$ *form a smooth regular sequence which defines a zero-dimensional affine algebraic variety* $V = V(f_1, \ldots, f_n)$. *We also consider the following quantities:*

- $\delta := deg(V)$
- $\eta :=$ *minimal height of* V *(i.e.* η *is the minimal value of* ht_V *distinct from* 1*)*

Then there exists a straight–line program of size $L(nd\delta)^{O(1)}$ *and non-scalar depth of order* $O(log_2 n + log_2 d + log_2 \delta + \ell)$ *with parameters of height at most* $O(max\{h, h', \eta, log_2 n, \ell\})$ *which evaluates a non-zero integer* $a \in \mathbb{Z}$ *and a polynomial* $g_{n+1} \in \mathbb{Z}[X_1, \ldots, X_n]$ *such that*

$$a - g_{n+1} \cdot f_{n+1}$$

belongs to the ideal $(f_1, \ldots, f_n)$ *generated by* $f_1, \ldots, f_n$ *in* $\mathbb{Z}[X_1, \ldots, X_n]$.

The proof of this theorem will follow from the description of the algorithm given in Section 4 below. Applying Theorem 18 and Lemma 20 below, we obtain a more precise upper bound for the value $|g_{n+1}(\alpha)|$. From this bound together with Proposition 10 and 17 we then deduce easily Theorem 2.

3 An algorithm for Geometric Solving

The aim of this section is to establish a proof for Theorem 16. We describe an algorithm which implies Theorem 16. This algorithm works inductively on the codimension of the varieties $V_i := V(f_1, \ldots, f_i)$, $1 \leq i \leq n$, and our main goal is to describe this recursion.

Recall that our input is a smooth regular sequence $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ of degree at most d. We assume that this input is encoded by a straight–line program Γ of size L and non–scalar depth ℓ with parameters of height at most h that evaluates the polynomials $f_1, \ldots, f_n$. Our algorithm computes a geometric solution of the zero-dimensional algebraic variety $V := V(f_1, \ldots, f_n) \subseteq \mathbb{C}^n$. In order to describe for $1 \leq i \leq n$ the i-th recursive step of our algorithm, we shall refer to the intermediate complete intersection algebraic varieties as $V_i := V(f_1, \ldots, f_i)$ and introduce the following parameters:

- $\delta_i := deg(V_i)$,
- $\delta := max\{\delta_i \ : \ 1 \leq i \leq n\}$,
- $\eta_i := ht_{V_i}(C)$, where C is a suitably chosen natural number of order $O((log_2 n + \ell) log_2 \delta)$, such that $\mathbb{Q}\,[V_i]$ has a primitive element of height C with respect to a suitable Noether position of V_i.
- $\eta := max\{\eta_i \ : \ 1 \leq i \leq n\}$.

As a byproduct of our algorithm, we shall obtain geometric solutions of the algebraic varieties V_i. In fact, our algorithm computes for every $1 \leq i \leq n$ a $\mathbb{Z}$-linear change of coordinates

$$(X_1, \ldots, X_n) \longrightarrow (Y_1^{(i)}, \ldots, Y_n^{(i)}),$$

such that the ring extension

$$R_i := \mathbb{Q}[Y_1^{(i)}, \ldots, Y_{n-i}^{(i)}] \longrightarrow B_i := \mathbb{Q}[Y_1^{(i)}, \ldots, Y_n^{(i)}]/(f_1, \ldots, f_i) = \mathbb{Q}[V_i]$$

is integral. The R_i-module B_i is a free module of rank say $D_i \leq \delta_i$. Let us denote by $\pi_i : V_i \longrightarrow \mathbb{C}^{n-i}$ the projection on the first $n-i$ coordinates of $(Y_1^{(i)}, \ldots, Y_n^{(i)})$. The morphism π_i of affine varieties is finite.

Definition 19 *Let assumptions and notations be as before. A lifting point for $W := V_i$ of the finite morphism π_i is a point $P = (p_1, \ldots, p_{n-i}) \in \mathbb{Z}^{n-i}$ with the following properties:*

- *the zero-dimensional fiber $W_P := \pi_i^{-1}(P)$ has degree (i.e. cardinality) equal to the rank of B_i as free R_i-module (this means $deg(W_P) = D_i$)*
- *the fiber W_P contains only smooth points. (This is equivalent to saying that the Jacobian matrix of the polynomials we obtain from $f_1(Y_1^{(i)}, \ldots, Y_n^{(i)}), \ldots, f_i(Y_1^{(i)}, \ldots, Y_n^{(i)})$ by substituting for $Y_1^{(i)}, \ldots, Y_{n-i}^{(i)}$ the coordinates $p_1, \ldots, p_{n-i}$ of P is regular at every point of the fiber W_P.)*

If $P \in \mathbb{Z}^{n-i}$ is a lifting point of the morphism π_i we will call its fiber W_P a lifting fiber of $W = V_i$. Observe that the elements of a lifting fiber of π_i are smooth points of W.

The lifting fibers W_P have the property that a geometric solution of the variety V_i can be reconstructed from the projection π_i and any geometric solution of the equations of such a fiber, (see Subsection 3.2 below). Our algorithm will choose for each $1 \leq i \leq n$ a suitable lifting point $P_i \in \mathbb{Z}^{n-i}$ of the morphism π_i. In the sequel we shall denote the lifting fiber of this point by V_{P_i}.

The following Section 3 is divided into two two well–distinguished parts, namely:

i) Subsection 3.2, treating "lifting by a symbolic Newton method", where we show how it is possible to reconstruct a geometric solution of the equations $f_1, \ldots, f_i$ from the lifting fiber V_{P_i}.

ii) Subsection 3.3, where we show how to find a linear coordinate change
$(X_1, \ldots, X_n) \longrightarrow (Y_1^{(i)}, \ldots, Y_n^{(i)})$, the lifting point P_i and a geometric solution of the equations of the lifting fiber V_{P_i}.

The i-th recursive step of our algorithm consists of the computation of the new variables $Y_1^{(i+1)}, \ldots, Y_n^{(i+1)}$, the point P_{i+1} and a geometric solution of its fiber $V_{P_{i+1}}$ from the data $Y_1^{(i)}, \ldots, Y_n^{(i)}$, P_i and V_{P_i}.

Let us conclude this subsection with the following remark: let $1 \leq i \leq n$ and consider the lifting fiber V_{P_i}. Since the degree of V_{P_i} equals $D_i = rank_{R_i}(B_i)$, any $\mathbb{Z}$-linear form $U_i := \lambda_{n-i+1}Y^{(i)}_{n-i+1} + \cdots + \lambda_n Y^{(i)}_n$ which separates the points of V_{P_i} represents not only a primitive element of the ring extension $\mathbb{Q} \longrightarrow \mathbb{Q}[V_{P_i}]$ but also a primitive element of the integral ring extension $R_i \subseteq B_i$ (which we will denote by u_i). Our algorithm will compute a geometric solution of both V_i and V_{P_i} using such a linear form U_i.

Let us observe that the bit length of our geometric solution of the equations of V_{P_i} will be bounded by the quantity

$$(i+1)(\delta_i + 2)\eta_i.$$

3.1 Elementary operations and bounds for straight–line programs

In this subsection we collect some elementary facts about straight–line programs. We start with an estimate for the degree and height of a polynomial given by a straight–line program. In order to state our result with sufficient generality, let us observe that the notion of height makes sense mutatis mutandi for polynomials over any domain equipped with an absolute value.

Lemma 20 ([30]) *Let R be a ring equipped with an absolute value $|\cdot| : R \longrightarrow \mathbb{R}$. Suppose $f \in R[X_1, \ldots, X_n]$ is a polynomial which can be evaluated by a straight–line program Γ in $R[X_1, \ldots, X_n]$ of size L and non-scalar depth ℓ with parameters of height h. Let $H > 0$ a real number and let $\alpha = (\alpha_1, \ldots, \alpha_n)$ be a point in R^n such that $log_2|\alpha_i| \leq H$ holds for $1 \leq i \leq n$. Then f and $f(\alpha)$ satisfy the following estimations:*

- $deg(f) \leq 2^\ell$
- $ht(f) \leq (2^{\ell+1} - 1) \cdot (h + log_2 L)$
- $log_2|f(\alpha)| \leq (2^{\ell+1} - 1) \cdot (max\{h, H\} + log_2 L)$

One of the main ingredients used in our procedure below is the efficient computation of the coefficients of the characteristic polynomial of a matrix. We shall use for this task Berkowitz' division-free and well parallelizable algorithm [6]. This is the content of the the next lemma.

Lemma 21 *[[6], [30]] Let R be a domain. There exists a straight–line program of size $N^{O(1)}$ and non-scalar depth $O(log_2 N)$ with parameters in $\{-1, 0, 1\}$ that from the entries of any $N \times N$ input matrix over R computes all coefficients of the characteristic polynomial of the given matrix.*

We use this algorithm not only for the computation of the characteristic polynomial of a given matrix but also for the computation of the greatest common divisor of two given univariate polynomials with coefficients in a unique factorization domain (this task can be reduced to solving a suitable linear equation system corresponding to the Bézout identity over the ground domain. See [30] for details).

The following result is an immediate consequence of the formal rules of derivation:

Lemma 22 *Let R be a domain. For a given a finite set of polynomials $f_1, \ldots, f_s$ of $R[X_1, \ldots, X_n]$ which can be evaluated by a straight–line program β in $R[X_1, \ldots, X_n]$ of size L and non-scalar depth ℓ, there exists a straight–line program in $R[X_1, \ldots, X_n]$ of size $(2n+1)L$ and non-scalar depth $\ell+1$ with the same parameters as β which evaluates $f_1, \ldots, f_s$ and all the first partial derivatives:*

$$\{\frac{\partial f_i}{\partial X_j} : 1 \leq i \leq s, 1 \leq j \leq n\}.$$

Combining this lemma with Lemma 21, one concludes: let $f_1, \ldots, f_n$ be a family of polynomials of $R[X_1, \ldots, X_n]$ which can be evaluated by a straight–line program β of size L and non-scalar depth ℓ. Then there exists a straight–line program in $R[X_1, \ldots, X_n]$ of size $n^{O(1)}L$ and non-scalar depth $O(\ell + log_2 n)$ with the same parameters as β which evaluates the Jacobian determinant.

$$J(f_1, \ldots, f_n) := det(\frac{\partial f_i}{\partial X_j})_{1 \leq i,j \leq n}.$$

In some exceptional cases the straight–line programs we are going to consider might contain divisions as operations. Since we are only interested in division-free straight–line programs, the following "Vermeidung von Divisionen" technique due to V. Strassen [53] becomes crucial:

Proposition 23 ([53]) *Let Γ be a (division-free) straight–line program in $\mathbb{Z}[X_1, \ldots, X_n]$ of size L and depth ℓ with parameters of height h that computes a finite set of polynomials $f_0, \ldots, f_m$ of $\mathbb{Z}[X_1, \ldots, X_n]$. Assume that $f_0 \neq 0$ holds and that f_0 divides f_i in $\mathbb{Z}[X_1, \ldots, X_n]$ for any $1 \leq i \leq m$. Then there exists a (again division-free) straight–line program Γ' in $\mathbb{Z}[X_1, \ldots, X_n]$ with the following properties:*

i) Γ' *computes polynomials $P_1, \ldots, P_m$ of $\mathbb{Z}[X_1, \ldots, X_n]$ and a non-zero integer θ such that*

$$P_i = \theta \frac{f_i}{f_0}$$

holds for any $1 \leq i \leq m$.

ii) Γ' *has size of order $O(2^{2\ell}(L+n+2^\ell+m))$, depth of order $O(\ell)$ and its parameters have height of order $\max\{h, O(\ell)\}$.*

Moreover, the height of θ is of order:

$$2^{O(\ell)}(max\{h, \ell\} + log_2 L).$$

The proof of this proposition is based on the computation of the homogeneous components of a polynomial given by a straight–line program. This proof also provides an algorithm computing the homogenization of a polynomial given by a straight–line program. This is the content of the next lemma.

Lemma 24 ([30]) *Suppose that we are given a polynomial* $P := \sum P^{\mu} X_1^{\mu_1} \dots X_n^{\mu_n}$ *in* $\mathbb{Z}[X_1, \dots, X_n]$ *which can be evaluated by a straight line program* Γ *of size* L *and depth* ℓ *with parameters in a given set* $\mathcal{F} \subset \mathbb{Z}$. *Let be given a natural number* D. *Then there exists a straight line program* Γ' *in* $\mathbb{Z}[X_1, \dots, X_n]$ *which computes all the homogeneous components of* P *having the following properties:* Γ' *uses parameters from* $\mathcal{F}$, *has size* $(D+1)^2$ *and non-scalar depth* 2ℓ.

In Section 4 we shall work with a specific polynomial which we call the pseudo-jacobian determinant of a given regular sequence. We introduce now this polynomial and say how it can be evaluated. Let R be a domain containing $\mathbb{Q}$. Let K be the field of fractions of R and let $f_1, \dots, f_n \in R[X_1, \dots, X_n]$ be a regular sequence in $K[X_1, \dots, X_n]$. Furthermore, let $Y_1, \dots, Y_n$ be new variables. We write $Y = (Y_1, \dots, Y_n)$. Fix $1 \leq j \leq n$. By $f_j^{(Y)} := f_j(Y_1, \dots, Y_n)$ we denote the polynomial from f_j substituting the variables $X_1, \dots, X_n$ by $Y_1, \dots, Y_n$. In the polynomial ring $R[Y_1, \dots, Y_n, X_1, \dots, X_n]$ we decompose the polynomial $f_j^{(Y)} - f_j$ in the following (non-unique) way:

$$f_j^{(Y)} - f_j = \sum_{k=1}^{n} l_{k,j}(Y_k - X_k),$$

with $l_{k,j} \in R[Y_1, \dots, Y_n, X_1, \dots, X_n]$. Let us consider the determinant Δ of the matrix $A = (l_{k,j})_{1 \leq k,j \leq n}$, namely:

$$\Delta := det(A).$$

This determinant is called the *pseudo-jacobian determinant* of the regular sequence of polynomials $f_1, \dots, f_n$. If d is a bound for the degrees of $f_1, \dots, f_n$ and these polynomials are given by a straight–line program β of size L and non-scalar depth ℓ, then there is a straight–line program β' of size $(nd)^{O(1)}L$ and non-scalar depth $O(log_2 n + \ell)$ which evaluates the pseudo-jacobian determinant Δ. The straight–line program β' uses apart from the same parameters as β only parameters of $\mathbb{Z}$ of height $O(log_2 d)$.

We shall also consider the execution of straight–line programs in matrix rings. The situations where we apply these considerations will be of the following type: Let R be a domain. Suppose that there is given a polynomial $g \in R[X_1, \dots, X_n]$ by a straight–line program β in $R[X_1, \dots, X_n]$ of size L and non-scalar depth ℓ. Suppose also that there are given n commuting $D \times D$ matrices $M_1, \dots, M_n$ over R. In such a situation the entries of the matrix $g(M_1, \dots, M_n)$ can be computed from the entries of of $M_1, \dots, M_n$ and the parameters of β by a straight–line program β' in R of size $D^{O(1)}L$ and non-scalar depth $O(\ell)$. The parameters of β' are just the values $0, 1$ (see [23] for details).

Another important aspect of our main algorithm is its probabilistic (or alternatively its non-uniform) character. This is the content of the next definition and proposition.

Definition 25 *Let be given a set of polynomials* $\mathcal{W} \subseteq \mathbb{Z}[X_1, \dots, X_n]$. *A finite set* $Q \subseteq \mathbb{Z}^n$ *is called a correct test sequence (or questor set) for* $\mathcal{W}$ *if for any polynomial* f *belonging to* $\mathcal{W}$ *the following implication holds:*

$$f(x) = 0 \textit{ for all } x \in Q \textit{ implies } f = 0.$$

Denote by $\mathcal{W}(n,L,\ell)$ the class of all polynomials of $\mathbb{Z}[X_1,\ldots,X_n]$ which can be evaluated by straight–line programs of size at most L and of non-scalar depth at most ℓ. The following result says that for the class $\mathcal{W}(n,L,\ell)$ exist many correct test sequences of moderate length.

Proposition 26 ([28], [30]) *Let be given natural numbers n,ℓ,L with $L \geq n+1$ and consider the following quantities:*

$$u := (2^{\ell+1}-2)\,(2^{\ell}+1)^2 \qquad \text{and} \qquad t := 6\,(\ell L)^2.$$

Then the finite set $\{1,\ldots,u\}^{nt} \subset \mathbb{Z}^{nt}$ contains at least $u^{nt}\,(1-u^{-\frac{t}{6}})$ correct test sequences of length t for $\mathcal{W}(n,L,\ell)$. In particular the set of correct test sequences for $\mathcal{W}(n,L,\ell)$ of length t containing only test points from $\{1,\ldots,u\}^n$ is not empty.

¿From Lemma 20 we deduce the following complexity estimate:

Let $f \in \mathbb{Z}[X_1,\ldots,X_n]$ be a polynomial given by a straight–line program of size L and non-scalar depth ℓ with parameters of height h. Let $\alpha =\in \mathbb{Z}^n$ be a point of height h' given in bit representation. Then there exists a (deterministic) ordinary Turing machine which computes the bit representation of the value $f(\alpha)$ in time $(2^{\ell}L max\{h,h'\})^{O(1)}$.

In the next subsection we shall make use of a problem adapted version of the Hensel-Newton iteration. We are now going to describe a suitable division-free symbolic form of this procedure.

Let R be a polynomial ring over $\mathbb{Q}$, let K be its field of fractions and let $f_1,\ldots,f_n \in R[X_1,\ldots,X_n]$ be polynomials of degree at most d. Suppose that $f_1,\ldots,f_n$ are given by a (division-free) straight–line program β of size L and non–scalar depth ℓ. Let us also assume that the Jacobian matrix $D(f) := D(f_1,\ldots,f_n) := \left(\frac{\partial f_i}{\partial X_j}\right)_{1\leq i,j\leq n}$ of the polynomials $f_1,\ldots,f_n$ is regular. We consider now the following Newton–Hensel operator:

$$N_f(X_1,\ldots,X_n) := \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} - D(f)^{-1} \begin{pmatrix} f_1(X_1,\ldots,X_n) \\ \vdots \\ f_n(X_1,\ldots,X_n) \end{pmatrix}. \qquad (3)$$

This operator is given as a vector of n rational functions of $K(X_1,\ldots,X_n)$. This is also true for the k-th iteration of this operator, which we denote by N_f^k. For any $k \in \mathbb{N}$ there exist numerators $(g_1^{(k)},\ldots,g_n^{(k)}) \in R[X_1,\ldots,X_n]$ and a non-zero denominator $h^{(k)} \in R[X_1,\ldots,X_n]$ such that N_f^k can be written as:

$$N_f^k = \left(\frac{g_1^{(k)}}{h^{(k)}},\ldots,\frac{g_n^{(k)}}{h^{(k)}}\right) \in K(X_1,\ldots,X_n)^n.$$

The next lemma gives a description of a division-free straight–line program in $R[X_1,\ldots,X_n]$ that evaluates numerators and denominators for N_f^k.

Lemma 27 *Let notations and assumptions be as before. Let k be a natural number. There exists a straight–line program in $R[X_1,\ldots,X_n]$ of size $O(kd^2n^7L)$ and non-scalar depth $O((log_2 n+\ell)k)$ with the same parameters as β which evaluates numerators $g_1^{(k)},\ldots,g_n^{(k)}$*

and a (non-zero) denominator $h^{(k)}$ *for the* k *-fold iteration* N_f^k *of the Newton-Hensel operator* N_f *.*

Proof.– Let $A(f) = (a_{ij})_{1\leq i,j\leq n}$ be the transposed matrix of the adjoint matrix of $D(f)$. Both $A(f)$ and the Jacobian determinant $J(f) := det(D(f))$ can be evaluated by a straight–line program of size $O(n^5 + nL)$ and non–scalar depth $O(log_2 n + \ell)$, as it can be seen just by combining Lemma 21 and 22. We can write the operator N_f as

$$N_f = \frac{J(f)\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} - A(f)\begin{pmatrix} f_1(X_1,\ldots,X_n) \\ \vdots \\ f_n(X_1,\ldots,X_n) \end{pmatrix}}{J(f)}. \tag{4}$$

The entries a_{ij} of the matrix $A(f)$ are polynomials of the ring $R[X_1,\ldots,X_n]$ having degree at most $(n-1)(d-1)$. Moreover, the Jacobian determinant $J(f)$ is a polynomial of $R[X_1,\ldots,X_n]$ having degree at most $n(d-1)$. For $1 \leq i \leq n$ we consider

$$g_i := J(f)X_i - \sum_{j=1}^{n} a_{i,j} f_j.$$

All polynomials appearing on the right hand side of the definition of g_i as summands have degree bounded by $\nu := nd + 1$. Thus the degree of any g_i is bounded by ν. Let ${}^h g_i(X_0, X_1, \ldots, X_n) \in R[X_0,\ldots,X_n]$ be the homogenization of g_i by a new variable X_0 and let ${}^h J(f)(X_0, X_1,\ldots,X_n) \in R[X_0,\ldots,X_n]$ be the homogenization of the Jacobian determinant $J(f)$ by X_0.

We introduce now the following homogeneous polynomials (forms):

- $G_i(X_0,\ldots,X_n) := X_0^{\nu - deg(g_i)}({}^h g_i)$,
- $H(X_0,\ldots,X_n) := X_0^{\nu - deg(J_f)}({}^h J(f))$.

According to Lemma 24, there exists a division-free straight–line program in $R[X_1,\ldots,X_n]$ of size $O(d^2(n^7 + n^3 L))$ and non–scalar depth $O(log_2 n + \ell)$ which evaluates the forms $G_1,\ldots,G_n,H$. We now define recursively the following polynomials:

- for $k = 1$ and $1 \leq i \leq n$ let $g_i^{(1)} := G_i(1, X_1,\ldots,X_n)$ and $q^{(1)} := H(1, X_1,\ldots,X_n)$,
- for $k \geq 2$ and $1 \leq i \leq n$ let $g_i^{(k)} := G_i(h^{(k-1)}, g_1^{(k-1)},\ldots,g_n^{(k-1)})$ and $h^{(k)} := H(h^{(k-1)}, g_1^{(k-1)},\ldots,g_n^{(k-1)})$.

It is easy to see that these polynomials $g_1^{(k)},\ldots,g_n^{(k)}$ are numerators and that the polynomial $h^{(k)}$ is a denominator of the iterated Newton-Hensel operator N_f^k. A straight–line program evaluating them is obtained by iterating k times the straight–line program which computes $G_1,\ldots,G_n$ and H. No new parameters are introduced by this procedure. Putting all this together we get the complexity bounds in the statement of Lemma 27. ∎

3.2 Lifting fibers by the symbolic Newton-Hensel algorithm

The idea of using a symbolic adaptation of Newton–Hensel iteration for lifting fibers was introduced in [21]. For technical reasons, in that paper it was necessary to use algebraic parameters for the lifting process. We present here a new version of this lifting algorithm in which the use of algebraic numbers is replaced by a certain matrix with integer entries. The whole procedure therefore becomes completely rational. The new lifting process is described in the statement of the next theorem and its proof.

Let notations and assumptions be as the same as at the beginning of this section. We fix $1 \leq i \leq n$ and assume for the sake of notational simplicity that the variables $X_1, \ldots, X_n$ are already in Noether position with respect to the variety V_i, the variables $X_1, \ldots, X_{n-i}$ being free. We suppose that the lifting point P_i, the coordinates of the $\mathbb{Z}$-linear form U_i and a geometric solution for the equations of the lifting fiber V_{P_i} are explicitly given. With these conventions we state the main result of this subsection as follows:

Theorem 28 *There exists a (division-free) straight–line program Γ_i in the polynomial ring $\mathbb{Z}[X_1, \ldots, X_{n-i}, U_i]$ of size $(id\delta_i L)^{O(1)}$ and non-scalar depth $O((log_2 i + \ell) log_2 \delta_i)$ using as parameters*

- *the coordinates of P_i*
- *the integers appearing in the geometric solution of the equations of the lifting fiber V_{P_i} and*
- *the parameters of the input program Γ*

such that the straight–line program Γ_i computes

- *the minimal polynomial $q_i \in \mathbb{Z}[X_1, \ldots, X_{n-i}, U_i]$ of the primitive element u_i of the ring extension $\mathbb{Q}[X_1, \ldots, X_{n-i}] \longrightarrow \mathbb{Q}[V_i] = \mathbb{Q}[X_1, \ldots, X_n]/(f_1, \ldots, f_i)$,*
- *polynomials $\rho_{n-i+1}^{(i)}, \ldots, \rho_n^{(i)} \in \mathbb{Z}[X_1, \ldots, X_{n-i}]$, $\rho := \prod_{k=n-i+1}^{n} \rho_k^{(i)}$ and polynomials $v_{r+1}^{(i)}, \ldots, v_n^{(i)} \in \mathbb{Z}[X_1, \ldots, X_{n-i}, U_i]$ with $max\{deg_u v_j^{(i)}\ ;\ r < j \leq n\} < \delta_i$ such that*

$$(f_1, \ldots, f_i)_\rho = (q_i(U_i), \rho_{r+1}^{(i)} X_{r+1} - v_{r+1}^{(i)}(U_i), \ldots, \rho_n^{(i)} X_n - v_n^{(i)}(U_i))_\rho$$

holds. Without loss of generality we may assume that Γ_i represents the coefficients of the polynomials q_i and $v_{r+1}^{(i)}, \ldots, v_n^{(i)}$ with respect to U_i.

Proof.– Under our hypotheses, namely that $X_1, \ldots, X_n$ are in Noether position with respect to the variety V_i, the variables $X_1, \ldots, X_{n-i}$ being free, we have the following integral ring extension of reduced rings:

$$R_i := \mathbb{Q}[X_1, \ldots, X_{n-i}] \longrightarrow B_i := \mathbb{Q}[X_1, \ldots, X_n]/(f_1, \ldots, f_i).$$

Let $P_i = (p_1, \ldots, p_{n-i}) \in \mathbb{Z}^{n-i}$ be a lifting point of the morphism π_i and let $V_{P_i} = \pi_i^{-1}(P_i)$ be its lifting fiber. We have $deg\ V_{P_i} = D_i = rank_{R_i} B_i \leq deg\ V_i = \delta_i$. Let $U_i =$

$\lambda_{n-i+1}X_{n-i+1}+\cdots+\lambda_n X_n \in \mathbb{Z}[X_{n-i+1},\ldots,X_n]$ generate a primitive element of the ring extension $\mathbb{Q} \longrightarrow \mathbb{Q}[V_{P_i}]$ (i.e. U_i separates the points of V_{P_i}). The minimal polynomial of the image of U_i in B_i has degree at least the cardinality of the set $U_i(V_{P_i})$. Since the linear form U_i seperates the points of V_{P_i}, this cardinality is $deg\ V_{P_i} = rank_{R_i} B_i$. We conclude that U_i generates also a primitive element of the ring extension $R_i \longrightarrow B_i$.

By hypothesis the following data are given explicitly (i.e. by the bit representaion of their coefficients):

- the primitive minimal equation, say $q \in \mathbb{Z}[T]$ of the primitive element u_i of $\mathbb{Q}[V_{P_i}]$,
- the parametrization of V_{P_i} by the zeroes of q, given by the equations

$$X_1 - p_1 = 0, \ldots, X_{n-i} - p_{n-i} = 0, q(T) = 0,$$
$$\rho_{n-i+1}X_{n-i+1} - v_{n-i+1}(T) = 0, \ldots, \rho_n X_n - v_n(T) = 0,$$

where $v_{n-i+1},\ldots,v_n$ are polynomials of $\mathbb{Z}[T]$ of degree strictly less $D_i = deg\ q$ and $\rho_{n-i+1},\ldots,\rho_n$ are non-zero integers. Check again Definition 6 to see that the polynomials $\rho_{n-i+1}X_{n-i+1} - v_{n-i+1}(T),\ldots,\rho_n X_n - v_n(T)$ are primitive.

Let $a \in \mathbb{Z}$ be the leading coefficient of q.

We consider now $f_1,\ldots,f_i$ as polynomials in the variables $X_{n-i+1},\ldots,X_n$, i.e. as elements of the polynomial ring $R_i[X_{n-i+1},\ldots,X_n]$. Let $f := (f_1,\ldots,f_i)$ and let

$$D(f) := \left(\frac{\partial f_k}{\partial X_j}\right)_{\substack{1\le k\le i \\ n-i+1\le j\le n}}$$

be the corresponding Jacobian matrix of f (with respect to the variables $X_{n-i+1},\ldots,X_n$). Recall that the Newton operator with respect to these variables is defined as

$$N_f = \begin{pmatrix} X_{n-i+1} \\ \vdots \\ X_n \end{pmatrix} - D(f)^{-1}\begin{pmatrix} f_1 \\ \vdots \\ f_i \end{pmatrix}.$$

Let k be a natural number. Using Lemma 27 we deduce the existence of numerators $g_{n-i+1},\ldots,g_n$ and a non-zero denominator q in the polynomial ring $R_i[X_{n-i+1},\ldots,X_n]$ such that the following k-fold iterated Newton operator has the form:

$$N_f^k = \begin{pmatrix} \frac{g_{n-i+1}}{h} \\ \vdots \\ \frac{g_n}{h} \end{pmatrix}.$$

Now, let $M_{X_{n-i+1}},\ldots,M_{X_n}$ be the matrices describing the multiplication tensor of the $\mathbb{Q}$-algebra $\mathbb{Q}[V_{P_i}]$ (recall that by assumption a geometric solution of the polynomial equation system defining V_{P_i} is given and that therefore the matrices $M_{X_{n-i+1}},\ldots,M_{X_n}$ are known).

Let M denote the companion matrix of the polynomial $a^{-1}q(T) \in \mathbb{Q}[T]$. Let $n-i+1 \le k \le n$. The following identity is immediate:

$$\rho_k M_{X_k} = v_k(M)$$

Moreover the matrices $\rho_k a^{D_i - 1} M_{X_i}$ have integer entries. Let $k := 1 + log_2 \delta_i$ and note that $k \geq 1 + log_2 D_i$ holds. Our straight–line program Γ_i will execute k Newton steps in a subroutine which we are going to explain now: Let us consider the following column vector of matrices $N_{n-i+1}, \ldots, N_n$ with entries in $\mathbb{Q}(X_1, \ldots, X_{n-i})$:

$$\begin{pmatrix} N_{n-i+1} \\ \vdots \\ N_n \end{pmatrix} := N_f^k(\underline{M}) = \begin{pmatrix} \frac{g_{n-i+1}(X_1,\ldots,X_{n-i},\underline{M})}{h(X_1,\ldots,X_{n-i},\underline{M})} \\ \vdots \\ \frac{g_n(X_1,\ldots,X_{n-i},\underline{M})}{h(X_1,\ldots,X_{n-i},\underline{M})} \end{pmatrix},$$

where $\underline{M} = (M_{X_{n-i+1}}, \ldots, M_{X_n})$ and $g_{n-i+1}, \ldots, g_n$ are the numerator and h the denominator polynomial of Lemma 27. Finally, let us consider the matrix

$$\mathcal{M} := U_i(N_{n-i+1}, \ldots, N_n) = \lambda_{n-i+1} N_{n-i+1} + \cdots + \lambda_n N_n.$$

This matrix is a matrix whose entries are rational functions of $\mathbb{Q}(X_1, \ldots, X_{n-i})$. More precisely, we can see that the entries of $\mathcal{M}$ belong to the local ring

$$R_{P_i} := (R_i)_{(X_1-p_1,\ldots,X_{n-i}-p_{n-i})} = \mathbb{Q}[X_1, \ldots, X_{n-i}]_{(X_1-p_1,\ldots,X_{n-i}-p_{n-i})}.$$

Let T be a new variable. With these notations and assumptions we have the following result:

Lemma 29 *Let $\chi \in \mathbb{Q}(X_1, \ldots, X_{n-i})[T]$ be the characteristic polynomial of $\mathcal{M}$ and $m_{u_i} \in R_i[T]$ the minimal integral equation of the primitive element u_i of B_i over R_i. Let $\chi(T) = T^{D_i} + \sum_{k=0}^{D_i-1} a_k T^k$ and $m_{u_i} = T^{D_i} + \sum_{k=0}^{D_i-1} b_k T^k$ with $a_k, b_k \in \mathbb{Q}(X_1, \ldots, X_{n-i})$ for $0 \leq k \leq D_i - 1$. Then all these coefficients satisfy the condition $ord_{p_i}(a_k - b_k) \geq \delta_i + 1$, where ord_{p_i} denotes the usual order function (additive valuation) of the local ring R_{P_i}.*

Proof.– Let $V_{P_i} = \{\xi_1, \ldots, \xi_{D_i}\}$ and let $\zeta_l := U_i(\xi_l)$ for $1 \leq l \leq D_i$. Because of the hypothesis made on the lifting fiber V_{P_i} and from Hensel's Lemma (which represents a symbolic version of the Implicit Function Theorem) we deduce that there exist formal power series $R_{n-i+1}^{(l)}, \ldots, R_n^{(l)} \in \mathbb{C}[[X_1 - p_1, \ldots, X_{n-i} - p_{n-i}]]$ with $R_{n-i+1}^{(l)}(P_i) = \xi_{n-i+1}^{(l)}, \ldots, R_n^{(l)}(P_i) = \xi_n^{(l)}$ such that for $R^{(l)} := (X_1 - p_1, \ldots, X_{n-i} - p_{n-i}, R_{n-i+1}^{(l)}, \ldots, R_n^{(l)})$ the identities

$$f_1(R^{(l)}) = 0, \ldots, f_i(R^{(l)}) = 0 \tag{5}$$

hold in $\mathbb{C}[[X_1 - p_1, \ldots, X_{n-i} - p_{n-i}]]$. Let us now consider $u^{(l)} := U_i(R^{(l)})$. As proved in [21] the minimal polynomial m_{u_i} verifies the following identity in $\mathbb{C}[[X_1 - p_1, \ldots, X_{n-i} - p_{n-i}]][T]$

$$m_{u_i} = \prod_{1 \leq l \leq \delta_i} (T - u^{(l)}). \tag{6}$$

Let us now consider the construction above which produces the matrix $\mathcal{M} \in (R_{P_i})^{D_i \times D_i}$ from the companion matrix $M \in \mathbb{Q}^{D_i \times D_i}$. The same construction transforms the eigenvalues of the matrix M, namely the values $\zeta_l := U_i(\xi_l)$, $1 \leq l \leq D_i$, into eigenvalues of $\mathcal{M}$. As shown in [21], this procedure produces D_i distinct rational functions $\tilde{u}^{(l)} \in \mathbb{C}(X_1, \ldots, X_{n-i})$, $1 \leq l \leq D_i$, which are defined in the point P_i. Therefore these rational functions can be interpreted as elements of the power series ring $\mathbb{C}[[X_1 - p_1, \ldots, X_{n-i} - p_{n_i}]]$ and they satisfy for $1 \leq l \leq D_i$ the condition

$$u^{(l)} - \tilde{u}^{(l)} \in (X_1 - P_1, \ldots, X_{n-i} - P_{n-i})^{\delta_i + 1}$$

in the power series ring $\mathbb{C}[[X_1 - P_1, \ldots, X_{n-i} - P_{n-i}]]$. (For a proof of these congruence relations see [21]).

Interpreting χ as a polynomial with coefficients in $\mathbb{Q}[[X_1 - p_1, \ldots, X_{n-i} - p_{n-i}]]$, we obtain the following representation:

$$\chi(T) = \prod_{k=0}^{D_i} (T - \tilde{u}^{(l)}). \tag{7}$$

Let σ_k denote the k–th elementary symmetric function in D_i arguments. Thus, we can write for $0 \leq k \leq D_i - 1$ the coefficient a_k of $\chi(T)$ as $a_k = (-1)^{D_i - k} \sigma_k(\tilde{u}^{(1)}, \ldots, \tilde{u}^{(D_i)})$. In the same way we deduce that $b_k = (-1)^{D_i - k} \sigma_k(u^{(1)}, \ldots, u^{(D_i)})$ holds for $0 \leq k \leq D_i$. Taking into account equations (6) and (7) we conclude now that for $0 \leq k \leq D_i$ the congruence relation

$$a_k - b_k \in (X_1 - P_1, \ldots, X_{n-i} - P_{n-i})^{\delta_i + 1}$$

holds in $\mathbb{Q}[[X_1 - P_1, \ldots, X_{n-i} - P_{n-i}]]$. This proves the lemma. ∎

In order to see how to evaluate the coefficients of χ, let us consider $\theta := det(h(\underline{M})) \in R_i$ and the matrix

$$\mathcal{M}_1 := \theta \mathcal{M}.$$

This matrix $\mathcal{M}_1$ has entries in R_i. Now we have:

$$det(T \cdot Id_{D_i} - \mathcal{M}) = det(T \cdot Id_{D_i} - \theta^{-1} \mathcal{M}_1) = \theta^{-D_i} det((\theta T) Id_{D_i} - \mathcal{M}_1).$$

Thus, we apply Lemma 21 to compute the coefficients of the characteristic polynomial of $\mathcal{M}_i$. We can write this characteristic polynomial as $f(T) = T^{D_i} + f_{D_i - 1} T^{D_i - 1} + \cdots + f_0 \in R_i[T]$. Therefore we have

$$a_k = \frac{\theta^k f_k}{\theta^{D_i}}.$$

There is a straight–line program Γ' of non-scalar size $O(log_2 \delta_i d^3 i^6 L)$ and non-scalar depth $O((log_2 i + \ell) log_2 \delta_i)$ using as parameters those described in the statement of the theorem which evaluates the family of polynomials $\{1, \theta, \ldots, \theta^{D_i}, f_0, \ldots, f_{D_i - 1}\} \subseteq R_i$.

Now, applying Strassen's Vermeidung von Divisionen technique (Proposition 23) we can obtain a division-free straight–line program of size $(id\delta_i L)^{O(1)}$, non-scalar depth $O((log_2 i +$

$\ell)log_2\delta_i)$ using as parameters the coordinates $p_1, \ldots, p_{n-i}$ of P_i, the coefficients of the linear change of coordinates for the Noether normalization for V_i, the numbers appearing in the geometric solving for the lifting fiber V_{P_i} and the parameters of Γ which evaluates the expansion of a_k in $\mathbb{Q}[[X_1 - p_1, \ldots, X_{n-i} - p_{n-i}]]$ up to terms of degree of order $\delta_i + 1$, i.e. it evaluates polynomials $g_o, \ldots, g_{D_i-1} \in \mathbb{Q}[X_1, \ldots, X_{n-i}]$ such that

$$b_k - g_k \in (X_1 - p_1, \ldots, X_{n-i} - p_{n-i})^{\delta_i+1}.$$

¿From [21] we deduce that the degree of the coefficients of the minimal polynomial $m_{u_i} \in R_i[T]$ is at most δ_i. Putting all this together, we conclude that

$$m_{u_i} = T^{D_i} + g_{D_i-1}T^{D_i-1} + \cdots + g_0$$

holds.

In order to compute the parametrizations $v_{n-i+1}^{(i)}, \ldots, v_n^{(i)} \in \mathbb{Q}[X_1, \ldots, X_{n-i}, T]$ we have to use the same kind of techniques (Newton–Hensel iteration) combined with other techniques which have been developed in [30] and used in [21] and [22]. Let us be more precise:

Let for $n-i+1 \leq k \leq n$ m_{X_k} be the minimal polynomial of the endomorphism determined by X_k over the $\mathbb{Q}$–algebra $\mathbb{Q}[V_{P_i}] = \mathbb{Q}[X_1, \ldots, X_n]/(X_1 - p1, \ldots, X_{n-i} - p_{n-i}, f_1, \ldots, f_i)$ Since Γ_i is a lifting point m_{X_t} is squarefree. The same argument as above provides a squarefree polynomial $r_k \in R_i[T]$ such that $r_k(X_k)$ vanishes on the variety V_i. So, we have two squarefree polynomials $r_k \in R_i[X_k]$ and $q_i \in R_i[u_i]$. Taking into account that U_i separates the associated primes of (r_k, q_i), we can apply directly Lemma 26 in [30] in order to obtain the parametrization associated to the variable X_k. Doing the same for each of the variables involved (namely $\{X_{n-i+1}, \ldots, X_n\}$) and putting together the corresponding straight–line programs, we obtain a procedure of the desired complexity. ■

3.3 Inductive Step

Proposition 30 *There exists a division-free arithmetic network of non-scalar size of order* $(id\delta_i L)^{O(1)}$ *and non-scalar depth* $O((log_2 i + \ell)log_2\delta_i)$ *using parameters of logarithmic height bounded by* $max\{h, \eta_i, O((log_2 i + \ell)log_2\delta_i)\}$ *which takes as input*

- *the Noether normalization for the variety* V_i,
- *the lifting point* P_i *and*
- *the geometric solution of the lifting fiber* V_{P_i}

and produces as output

- *a linear change of variables* $\{X_1, \ldots, X_n\} \longrightarrow \{Y_1^{(i+1)}, \ldots, Y_n^{(i+1)}\}$ *such that the new ones* $\{Y_1^{(i+1)}, \ldots, Y_n^{(i+1)}\}$ *are in Noether position with respect to* V_{i+1},
- *a lifting point* P_{i+1} *for* V_{i+1} *and*
- *the geometric solution for the corresponding lifting fiber* $V_{P_{i+1}}$.

Proof.– The first step is the application of the algorithm underlying Theorem 28. The second step is an elimination step, that is, the generation of a Noether normalization with respect to V_{i+1}, a primitive element u_{i+1} and a straight–line program representing similar polynomials for V_{i+1} as those obtained as output for the variety V_i in Theorem 28 above. This step is nearly the same as in the proof of Proposition 14 in [21] just by considering that in our case K is $\mathbb{Q}$ and taking into account the height of the parameters we introduce. We remark that this straight–line program has non-scalar size $(id\delta_i L)^{O(1)}$ and non-scalar depth $O(log_2(d\delta_i)+\ell)$ with parameters of logarithmic height bounded by $O(log_2(d\delta_i)+\ell)$. Now, let us consider

$$J(f_1\ldots,f_{i+1}) := det\left(\frac{\partial f_k}{\partial X_j}\right)_{\substack{1\le k\le i+1\\ n-i\le j\le n}},$$

which is a nonzero divisor modulo $I_{i+1}=(f_1,\ldots,f_{i+1})$. Let us observe that the polynomial $J(f_1\ldots,f_{i+1})$ can be evaluated by a division-free straight–line program of length $O((i+1)^5+L)$ and depth $O(log_2(i+1)+\ell)$.

Let $\mu\in K[X_1,\ldots,X_{n-i-1}]$ be the constant term of the characteristic polynomial of the homothety given by $J(f_1\ldots,f_{i+1})$ modulo I_{i+1}. Since J represents a nonzero divisor modulo I_{i+1} we conclude that μ is not 0. Furthermore we observe that μ can be evaluated by a division-free straight–line program in $k[X_1,\ldots,X_{n-i-1}]$ of length $(i\delta_i L)^{O(1)}$ and depth $O(log_2 d\delta_i+(log_2 i+\ell)log_2\delta_i)=O((log_2 i+\ell)log_2\delta_i)$, and so does the product $\rho\cdot\mu$, where $\rho:=\prod\limits_{n-i+1}^{n}\rho_j^{(i)}$.

Using a correct test sequence (see [28]) we are able to find in sequential time $(i\delta L)^{O(1)}$ and parallel time $O((log_2 i+\ell)log_2\delta_i)$ a rational point $P_{i+1}\in\mathbb{Z}^{n-i-1}$ of logarithmic height bounded by $O((log_2 i+\ell)log_2\delta_i)$ which satisfies $(\rho\cdot\mu)(P_{i+1})\neq 0$. Clearly, P_{i+1} is a lifting point for the variety V_{i+1}. In order to obtain the geometric solving for $V_{P_{i+1}}$ with primitive element u_{i+1} we must specialize the polynomials obtained as output for the elimination step in P_{i+1} (see [21], Section 3). After this specialization we obtained the binary representation of some polynomials which verifies all the hypothesis of the geometric solving. Nevertheless it can happen that the height of these coefficients is excessive. In order to make these polynomials primitive and hence with admissible height, we have to make some integer gcd calculations which do not modify the asymptotic time complexity estimations made for the algorithm. ■

4 Lifting Residues and Division Steps

This section is dedicated to the proof of Theorem 18. Our new outcome is a new version of the Trace Formula in Gorenstein algebras that profits from the good features of the algebra. Our new version requires no monomial basis: the Trace Formula is an "easy-to-evaluate" expression.

4.1 Trace and Duality

The Trace Formula appears in several recent works in elimination theory. Some of these works use the Trace Formula to compute quotients of divisions modulo complete intersections (cf. [19], [30]). Other works design algorithms for computing basis (and solving) of Gorenstein algebras ([1], [2], [13]). Some other works simply use the Trace Formula to get upper bounds for the degrees in the Nullstellensatz ([44]).

However, all of these applications of the Trace Formula require the use of some generating family of monomials of bounded degree. In this sense, it just provides syntactical bounds and no intrinsic upper complexity bound can be obtained (as in Theorem 18). In this subsection we introduce an alternative version in order to get a maximum benefit from the good features of the Gorenstein algebra. Let us start with a sketch of the trace theory. Readers interested in details might want to consult Appendices E and F of [33].

Let R be a ring of polynomials with coefficients in a field (for our discussion the field may be assumed to be $\mathbb{Q}$). Now, $R[X_1,\ldots,X_n]$ is the ring on n-variate polynomials with coefficients in R and K should be the quotient field of R. Let $f_1,\ldots,f_n \in R[X_1,\ldots,X_n]$ a smooth regular sequence of polynomials of degree at most d generating the radical ideal $(f_1,\ldots,f_n)$.

Now we have the R-algebra B given as the quotient of $R[X_1,\ldots,X_n]$ by this ideal:

$$B := R[X_1,\ldots,X_n]/(f_1,\ldots,f_n).$$

We also assume that the morphism $R \to B$ is an integral ring extension such that R will be a Noether normalization of B. Thus, B is a free R-module of rank bounded by the degree of the variety $V(f_1,\ldots,f_n)$. Moreover, B is a typical Gorenstein R-algebra and we have good properties coming from this fact.

First of all, let $B^* := Hom_R(B,R)$ be the B-module with the natural operation:

$$B \times B^* \longrightarrow B^*$$

which associates to (b,τ) in $B \times B^*$ the homomorphism $x \mapsto \tau(bx)$.

By hypothesis B^* is a free B-module of rank one. Every element σ of B^* such that $\{\sigma\}$ is a basis of B^* as free B-module is called a *trace*. There are two relevant morphisms in B^* that we denote by Tr and σ. The first one, Tr, is called the usual trace and it is defined in the following form: given $b \in B$, let $\eta_b : B \longrightarrow B$ the endomorphism defined by multiplying by b. Then, $Tr(b)$ is the trace of this endomorphism. To introduce the second one, we need some additional notations. For every element $b \in R[X_1,\ldots,X_n]$ we denote by $\bar{b}$ the class defined by b modulo $(f_1,\ldots,f_n)$. Let $f_j^{(Y)} := f_j(Y_1,\ldots,Y_n) \in R[Y_1,\ldots,Y_n]$ and for $1 \leq j \leq n$ let us consider the polynomials:

$$f_j^{(Y)} - f_j = \sum_{k=1}^{n} l_{j,k}(Y_k - X_k) \in R[X_1,\ldots,X_n] \otimes_R R[Y_1,\ldots,Y_n],$$

where the polynomials $l_{j,k} \in R[X_1,\ldots,X_n,Y_1,\ldots,Y_n]$ have total degree at most $(d-1)$. Then, let us consider the determinant of the matrix $(l_{k,j})$, $1 \leq k,j \leq n$, given by:

$$\Delta := \sum_m a_m(X) \otimes_R b_m(Y) \in R[Y_1, \ldots, Y_n] \otimes R[X_1, \ldots, X_n].$$

This element Δ is called the pseudo-jacobian determinant of the sequence $(f_1, \ldots, f_n)$. Observe that the polynomials $a_m(X)$ and $b_m(Y)$ have respectively degrees at most $n(d-1)$ in the variables $\{X_1, \ldots, X_n\}$ and $\{Y_1, \ldots, Y_n\}$. If $\bar{J}$ is the class of the Jacobian determinant $J(f_1, \ldots, f_n)$, we have:

$$\bar{J} = \sum_m \bar{a}_m \cdot \bar{b}_m.$$

This justifies the name of pseudo-jacobian for Δ. These notations stated, there is a unique trace $\sigma_\Delta \in B^*$ such that the following identity holds in B:

$$\bar{1} = \sum_m \sigma_\Delta(\bar{a}_m) \cdot \bar{b}_m.$$

This identity is known as the Trace Formula and is used through the following lifting property

$$\forall \bar{q} \in B, \bar{q} = \sum_m \sigma_\Delta(\bar{q} \cdot \bar{a}_m) \cdot \bar{b}_m$$

which we explicit below:

Problem 6 (Lifting a residual class) *Suppose you are given a residual class $\bar{q} \in B$ and you want to compute a polynomial $q_1 \in R[X_1, \ldots, X_n]$ of degree at most $n(d-1)$ in the variables $\{X_1, \ldots, X_n\}$ such that $\bar{q}_1 = \bar{q}$.*

As already seen before, the Trace Formula solves this problem by computing the following polynomial:

$$\bar{q}_1 = \sum_m \sigma_\Delta(\bar{q} \cdot \bar{a}_m) \cdot b_m \in R[X_1, \ldots, X_n].$$

However, using this expression for q_1, one can not take advantage of any possibly good semantical features of the R-algebra B: one “a priori” needs all monomials of degree at most $n(d-1)$ to obtain the b_m. Therefore, we introduce the following alternative:

Proposition 31 (Trace Formula) *With the same notations as before, let us consider the free $R[X_1, \ldots, X_n]$-module $B[X_1, \ldots, X_n]$ given by extending scalars in B (this means $B[X_1, \ldots, X_n] := B \otimes_R R[X_1, \ldots, X_n]$) and let us also consider the polynomial given by:*

$$\Delta_1 := \sum_m \bar{a}_m \cdot b_m \in B[X_1, \ldots, X_n].$$

Given $\bar{q}$ in B, we have the following identity

$$\sum_m \sigma_\Delta(\bar{b} \cdot \bar{a}_m) \cdot b_m = \widetilde{Tr}(\bar{J}^{-1}\bar{b} \cdot \Delta_1) \in R[X_1, \ldots, X_n],$$

where $\widetilde{Tr} := Tr \otimes Id : B[X_1, \ldots, X_n] \longrightarrow R[X_1, \ldots, X_n]$ is obtained from the usual trace by extending scalars.

Proof.– First of all, let us recall ([33], [44]) that for all $\bar{q} \in B$ we have:

$$Tr(\bar{J}^{-1}\bar{q}) = \sigma_\Delta(\bar{q}),$$

where $Tr : B \longrightarrow R$ is the usual trace of the free R-module B. Then, since $\widetilde{Tr}$ is $R[X_1, \ldots, X_n]$-linear, we have:

$$\widetilde{Tr}(\bar{J}^{-1}\bar{q}\Delta_1) = \sum_m \widetilde{Tr}(\bar{J}^{-1}\bar{q}\bar{a}_m \otimes b_m) = \sum_m \widetilde{Tr}(\bar{J}^{-1}\bar{q}\bar{a}_m) \otimes b_m.$$

In other words

$$\widetilde{Tr}(\bar{J}^{-1}\bar{q}\Delta_1) = \sum_m \sigma_\Delta(\bar{q} \cdot \bar{a}_m) \cdot b_m.$$

Finally, an elementary exercise of linear algebra would show that for all $f \in B[X_1, \ldots, X_n]$, $\widetilde{Tr}(f)$ is simply the usual trace of the $R[X_1, \ldots, X_n]$-module $B[X_1, \ldots, X_n]$. We leave this to the reader. ■

Now we observe that the lifting process can be described just in terms of the tensor matrices. This means that we can consider the K-algebra $B' = K \otimes_R B$ obtained by localization and a basis β' be a basis of B' considered as a finite dimensional vector space. Let $M_{X_1}, \ldots, M_{X_n}$ be the matrices of the homotheties $\eta_{X_i} : B \longrightarrow B'$ in this basis and Tr the usual trace of a matrix. Then we have:

$$q_1 = Tr(J(f_1, \ldots, f_n)^{-1}_{(M_{X_1}, \ldots, M_{X_n})} \cdot q(M_{X_1}, \ldots, M_{X_n}) \cdot \Delta(M_{X_1}, \ldots, M_{X_n}, X_1, \ldots, X_n)).$$

4.2 A Division Step

This lifting process is applied to compute the quotient of two polynomials modulo a reduced complete intersection ideal. More precisely, let us consider $f \in R[X_1, \ldots, X_n]$ a polynomial which is not a zero-divisor in B and another polynomial $g \in R[X_1, \ldots, X_n]$ such that the residual classes verify $\bar{f} \mid \bar{g}$ in B. The following proposition shows how to compute a lifting quotient $q \in R[X_1, \ldots, X_n]$.

Proposition 32 (Division Step) *With the notations of the previous subsection, let us call D the rank of B as free R-module. Given the following items as input:*

- *two straight–line programs Γ_i of size L_i, depth ℓ_i and parameters of height h_i representing $\{f, g\}$ and $\{f_1, \ldots, f_n\}$ respectively,*
- *the matrices of the tensors $M_{X_1}, \ldots, M_{X_n}$,*

there exists a straight–line program Γ over R of size $(L_1 + L_2)(ndD)^{O(1)}$ and non-scalar depth $O(max\{\ell_1, \ell_2\} + log_2 D + log_2 n)$ with parameters of height $max\{h_1, h_2\}$ computing a non-zero θ in R, and q in $R[X_1, \ldots, X_n]$ such that θ divides q in $R[X_1, \ldots, X_n]$.

Proof.– In order to prove this result, let us observe that if β is a basis of B as free R-module, the set $\beta' = \{b \otimes 1 : b \in B\}$ is a basis of $B[X_1, \ldots, X_n]$ as free $R[X_1, \ldots, X_n]$-module. Moreover if M_{X_i} is the matrix of the tensor of the multiplication by $\bar{X}_i$ in B, the same holds for the extended multiplication

$$\eta_{\bar{X}_i} : B[X_1, \ldots, X_n] \longrightarrow B[X_1, \ldots, X_n].$$

(Remember to distinguish well between $\bar{X}_i$ as an element of the ring of coefficients B of $B[X_1, \ldots, X_n]$ and X_i as variable.) Next, since the polynomials f and $J(f_1, \ldots, f_n)$ are not zero-divisors modulo $(f_1, \ldots, f_n)$, the following matrices are non-singular:

$$F_1 := f(M_{X_1}, \ldots, M_{X_n}),$$

$$J_1 := det(\frac{\partial f_i}{\partial X_j}(M_{X_1}, \ldots, M_{X_n}))_{1 \le i,j \le n}.$$

Finally, let us denote by G_1 and Δ_1 the following two matrices:

$$G_1 := g(M_{X_1}, \ldots, M_{X_n}),$$

$$\Delta_1 := \Delta(M_{X_1}, \ldots, M_{X_n}, X_1, \ldots, X_n).$$

Let us remark that the matrices F_1, J_1 and G_1 have entries in R while Δ_1 has entries in $R[X_1, \ldots, X_n]$. Now, the results of the previous subsection say that the following polynomial

$$q_1 := Tr(J_1^{-1} \cdot F_1^{-1} \cdot G_1 \cdot \Delta_1) \in R[X_1, \ldots, X_n]$$

(where Tr is the usual trace of a matrix), verifies that $\bar{q}_1 \bar{f} - \bar{g}$ is 0 in B.
Finally, let us transpose the adjoint matrices of F_1 and J_1:

$$F_2 := {}^tAdj(F_1), \text{ and } J_2 := {}^tAdj(J_1).$$

The wanted quotient $q \in R[X_1, \ldots, X_n]$ and the constant $\theta \in R$, $\theta \neq 0$ are given by the following rules:

- $q := Tr(F_2 \cdot J_2 \cdot G_1 \cdot \Delta_1)$
- $\theta := det(F_2) \cdot det(J_2)$

Clearly, the polynomial q_1 is the quotient of $\frac{q}{\theta}$, while $\bar{q}\bar{f} - \bar{\theta}\bar{g}$ is 0 in B. The bounds stated in the Proposition follow by reconstructing the straight–line programs that evaluate $f, g, J(f_1, \ldots, f_n), \Delta$ and the determinants described above (cf. Subsection 3.1 above).

Proof of Theorem 18

In order to prove Theorem 18 we just follow the previous proposition. We have to add just some comments concerning the tensor matrices in this case. Let us consider a primitive element $u = \lambda_1 X_1 + \cdots + \lambda_n X_n$ (with $\lambda_i \in \mathbb{Z}$) of the zero-dimensional $\mathbb{Q}$-algebra $\mathbb{Q}[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$. In this case R will be the field $\mathbb{Q}$. Let $q_u \in \mathbb{Z}[T]$ be the minimal polynomial of u and $\rho_1 X_1 - v_1(T), \ldots, \rho_n X_n - v_n(T)$ the parametrizations of the variety with respect to this primitive element. Let α be the leading coefficient of q_u and $\rho = \prod_{i=1}^n \rho_i$ the discriminant. Then the companion matrix of q_u has the form

$$\alpha^{-1} M,$$

where M is a matrix with rational entries. Now, the matrices of the tensors have the form

$$M_{X_i} = \rho_i^{-1} \cdot v_i(\alpha^{-1} M).$$

Taking $g = 1$ and $f = f_{n+1}$ in the Proposition above we obtain $\theta \in \mathbb{Q}$, $\theta \neq 0$ and $q \in \mathbb{Q}[X_1, \ldots, X_n]$ such that

$$\theta \cdot 1 - q \cdot f_{n+1} \in (f_1, \ldots, f_n).$$

Finally, multiplying by appropriate powers of α and ρ we get

$$a := \alpha^N \rho^M \cdot \theta \in \mathbb{Z} \quad g_{n+1} := \alpha^N \rho^M q \in \mathbb{Z}[X_1, \ldots, X_n],$$

such that $a - g_{n+1} f_{n+1} \in (f_1, \ldots, f_n)$. The bounds of the theorem are obtained from the bounds of the Proposition above. The bounds for the height of the parameters are obtained simply by choosing an appropriate primitive element u such that q_u and the parametrizations have height equal to the minimal height of the diophantine variety $V := V(f_1, \ldots, f_n)$. ■

References

[1] M. E. Alonso, E. Becker, M.-F. Roy, T. Wörmann: Zeroes, multiplicities and idempotents for zerodimensional systems, to appear in *Proc. MEGA'94*, Birkhäuser Progress in Mathematics.

[2] E. Becker, J.P. Cardinal, M.-F. Roy, Z. Szafraniec: Multivariate Bezoutians, Kronecker symbol and Eisenbud–Levine formula, to appear in *Proc. MEGA'94, Birkhäuser Progress in Math.*

[3] C. Berenstein, A. Yger: Effective Bézout identities in $\mathbb{Q}[X_1, \ldots, X_n]$, *Acta Math.*, **166** (1991) 69-120.

[4] C. Berenstein, A. Yger: Une formule de Jacobi et ses conséquences, *Ann Sci. E.N.S.*, *4^{ieme} série*, **24** (1991) 363-377.

[5] C. Berenstein, A. Yger: Green currents and analytic continuation, *preprint, Univ. of Maryland*, (1995)

[6] S.J. Berkowitz: On computing the determinant in small parallel time using a small number of processors, *Inf. Proc. Letters* **18** (1984) 147–150.

[7] J.-B. Bost, H. Gillet, C. Soulé: Un analogue arithmétique du théorème de Bézout, *C.R. Acad. Sci. Paris, Série I, Math.* **312**, (1991) 845-848.

[8] J.-B. Bost, H. Gillet, C. Soulé: Heights of projective varieties and positive Green forms, *Manuscript IHES*, (1993).

[9] D. W. Brownawell: Bounds for the degree in the Nullstellensatz, *Annals of Math.* **126** (1987) 577-591.

[10] J. F. Canny, I.Z. Emiris: Efficient Incremental Algorithms for the Sparse Resultant and the Mixed Volume, *Preprint* (1995)

[11] L. Caniglia, A. Galligo, J. Heintz: Borne simplement exponentielle pour les degrés dans le théorème des zéros sur un corps de caractéristique quelconque, *C.R. Acad. Sci. Paris, Série I, Math.* **307** (1988) 255-258.

[12] L. Caniglia, A. Galligo, J. Heintz: Some new effectivity bounds in computational geometry, *Proc. AAECC–6, T. Mora, ed., Springer LNCS* **357**(1989) 131–152.

[13] J.P. Cardinal: *Dualité et algorithmes itératives pour la solution des systèmes polynomiaux*, Thèse, U. de Rennes I (1993).

[14] J.-P. Dedieu, Estimations for the Separation Number of a Polynomial System, *Preprint, Univ. Paul Sabatier, Toulouse* (1995)

[15] J.-P. Dedieu, Approximate Solutions of Numerical Problems, Condition Number Analysis and Condition Number Theorems, *Preprint, Univ. Paul Sabatier, Toulouse* (1995)

[16] M. Elkadi. "Bornes pour le degré et les hauteurs dans le problème de division", in *Michigan Math. J.* **40** (1993) 609-618

[17] I. Z. Emiris: On the Complexity of Sparse Elimination, *ReportNo. UCB/CSD-94/840, Univ. of California* (1994)

[18] G. Faltings, Diophantine approximation on Abelian varieties, *Ann. of Math.*, **133** (1991), 549-576

[19] N. Fitchas, M. Giusti, F. Smietanski: Sur la complexité du théorème des zéros, in *Approximation and Optimization in the Caribbean II, Proceedings of the Second International Conference on Approximation and Optimization*, La Habana, 1993, M. Florenzano et al., eds., Approximation and Optimization, Peter Lang Verlag, Frankfurt (1995) 274–329.

[20] M. Giusti, J. Heintz: La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial, In *Computational Algebraic Geometry and Commutative Algebra*, Proceedings of the Cortona Conference on Computational Algebraic Geometry and Commutative Algebra, D. Eisenbud and L. Robbiano, eds., Symposia Matematica, vol. XXXIV, Istituto Nazionale di Alta Matematica, Cambridge University Press (1993).

[21] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, L.M. Pardo: Straight–line programs in Geometric Elimination Theory, to appear in *Journal of Pure and Applied Algebra*

[22] M. Giusti, J. Heintz, J.E. Morais, L.M. Pardo: When polynomial equation systems can be "solved" fast? in *Proc. 11th International Symposium Applied Algebra, Algebraic Algorithms and Error–Correcting Codes, AAECC–11*, Paris 1995, G. Cohen, M.Giusti and T. Mora, eds., Springer LNCS **948** (1995) 205–231.

[23] M. Giusti, J. Heintz, J. Sabia: On the efficiency of effective Nullstellensätze, *Computational Complexity* **3** (1993) 56–95.

[24] J. Heintz: Fast quantifier elimination over algebraically closed fields, *Theoret. Comp. Sci.* **24** (1983) 239-277.

[25] J. Heintz, T. Krick, A. Slissenko, P. Solernó: "Searching for a shortest path surrounding semi–algebraic obstacles in the plane" (in russian): *Teorija složnosti vyčislenij*, **5**, Zapiski naučnyh seminarov LOMI (Leningrad branch of the Mathematical Institute Steklov), Nauka, Leningrad, vol. **192**, (1991), 163-173

[26] J. Heintz, T. Krick, A. Slissenko, P. Solernó. "Une borne inférieure pour la construction des chemins polygonaux dans $\mathbb{R}^n$, *Preprint, Univ. de Limoges*, (1992)

[27] J. Heintz, J. Morgenstern: On the intrinsic complexity of elimination theory, *J. of Complexity* **9** (1993) 471–498.

[28] J. Heintz, C.P. Schnorr: Testing polynomials which are easy to compute, *Proc. 12th Ann. ACM Symp. on Computing* (1980) 262–268; also in *Logic and Algorithmic. An International Symposium held in Honour of Ernst Specker*, Monographie No. **30** de l'Enseignement de Mathématiques, Genève (1982) 237–254.

[29] J. Kollár: Sharp Effective Nullstellensatz, *J. of A.M.S.* **1** (1988) 963-975.

[30] T. Krick, L.M. Pardo: A Computational Method for Diophantine Approximation, to appear in *Proc. MEGA'94, Birkhäuser Progress in Mathematics.*

[31] T. Krick, L.M. Pardo: Une approche informatique pour l'approximation diophantienne, *C. R. Acad. Sci. Paris, t.* **318**, Série I, no. 5 , (1994) 407–412.

[32] T. Krick, J. Sabia, P. Solernó: On Intrinsic Bounds in the Nullstellensatz, *Preprint* (1996), to appear in: AAECC

[33] E. Kunz: *Kähler Differentials*, Advanced Lectures in Mathematics, Vieweg Verlag, Braunschweig/Wiesbaden (1986).

[34] M. Mignotte: *Mathématiques pour le Calcul Formel*, Presses Universitaires de France (1989).

[35] J.L. Montaña, J.E. Morais, L.M. Pardo: Lower Bounds for Arithmetic Networks II: Sum of Betti numbers, *Applicable Algebra in Engineering Communications and Computing (AAECC)*, vol. **7**, No. 1 (1996) 41-51.

[36] J.L. Montaña, L.M. Pardo: Lower Bounds for Arithmetic Networks, *Applicable Algebra in Engineering Communications and Computing (AAECC)*, vol. **4** (1993), 1–24.

[37] Yu. V. Nesterenko: Estimates for the order of zero o functions of a certain class and applications in the theory of transcendental numbers *Math. USSR Izvestija*, vol.**11**, No. 2 (1977) 239–270.

[38] Yu. V. Nesterenko: On a measure of the algebraic independence of the values of certain functions, *Math. USSR Sbornik* **56** (1987) 545– 567.

[39] L.M. Pardo: How lower and upper complexity bounds meet in elimination theory, in *Proc. 11th International Symposium Applied Algebra, Algebraic Algorithms and Error–Correcting Codes, AAECC–11*, Paris 1995, G. Cohen, M.Giusti and T. Mora, eds., Springer LNCS **948** (1995) 33–69.

[40] P. Philippon: Critères pour l'indépendence algébrique, *Pub. Math. de l'IHFS* **64** (1987) 5–52.

[41] P. Philippon: Sur des hauteurs alternatives, I, *Math. Ann.* **289** (1991) 255–283.

[42] P. Philippon: Sur des hauteurs alternatives, II, *Ann. Inst. Fourier, Grenoble*, vol. **44** No. 2 (1994) 1043–1065.

[43] P. Philippon: Sur des hauteurs alternatives, III, to appear in *J. Math. Pures Appl.*

[44] J. Sabia, P. Solernó: Bounds for traces in complete intersections and degrees in the Nullstellensatz, *Applicable Algebra in Engineering Communications and Computing (AAECC)*, vol. **6** (1996) 353–376.

[45] T. Schneider, Einführung in die Theorie der transzendenten Funktionen, *Springer Verlag, Berlin* (1957)

[46] M. Shub, S. Smale: Complexity of Bezout's theorem I: Geometric aspects, *J. Amer. Math. Soc.* **6** (1993), 459-501

[47] M. Shub, S. Smale: Complexity of Bezout's theorem II: Volumes and probabilities, in *Proceedings Effective Methods in Algebraic Geometry, MEGA'92* Nice, 1992, F. Eyssette and A. Galligo, eds. Progress in Mathematics, Vol. 109, Birkhäuser, Basel, (1993) 267-285

[48] M. Shub, S. Smale: Complexity of Bezout's theorem III: Condition number and packing, *J. of Complexity* **9** (1993) 4-14

[49] M. Shub, S. Smale: Complexity of Bezout's theorem IV: Probability of Success, Extensions, *SIAM J. Numer. Anal.* to appear

[50] M. Shub, S. Smale: Complexity of Bezout's theorem V: Polynomial time, *Theoretical Comp. Sci.* **133** (1994)

[51] M. Shub, S. Smale: On the intractability of Hilbert's Nullstellensatz and an algebraic version of $NP \neq P$?, *IBM Research Report*, Yorktown Heights (1994)

[52] C. Soulé: oral communication (1994)

[53] V. Strassen: Vermeidung von Divisionen, *Crelle J. Reine Angew. Math.* **264** (1973) 184-202.