On the Intrinsic Complexity of the Arithmetic Nullstellensatz[1]

K. Hägele[2], J. E. Morais[3], L. M. Pardo[2] and M. Sombra[4]

Keywords. Polynomial system solving, elimination, geometric degree, arithmetic networks, straight–line programs, complexity.
1991 Math. Subj. Class.: 68Q25, 14Q25, 11J99

Abstract

We show several arithmetic estimates for Hilbert's Nullstellensatz. This includes an algorithmic procedure computing the polynomials and constants occuring in a Bézout identity, whose complexity is polynomial in the geometric degree of the system. Moreover, we show for the first time height estimates of intrinsic type for the polynomials and constants appearing, again polynomial in the geometric degree and linear in the height of the system. These results are based on a suitable representation of polynomials by straight–line programs and duality techniques using the Trace Formula for Gorenstein algebras.

As an application we show more precise upper bounds for the function $\pi_S(x)$ counting the number of primes yielding an inconsistent modular polynomial equation system. We also give a computationally interesting lower bound for the density of small prime numbers of controlled bit length for the reduction to positive characteristic of inconsistent systems. Again, this bound is given in terms of intrinsic parameters.

1 Introduction and statement of results

In the sequel we discuss several arithmetic aspects of Hilbert's Nullstellensatz whose origin is closely connected with the classical consistency question for systems of multivariate polynomial equations. Let us assume that a system $S = \{f_1, \ldots, f_s\} \subseteq \mathbb{Z}[X_1, \ldots, X_n]$ of multivariate polynomials with integer coefficients is given. *The consistency problem over* $\mathbb{C}$ *on input* S can be stated as deciding whether the following formula is true or not :

$$\exists x_1 \in \mathbb{C}, \ldots, \exists x_n \in \mathbb{C}, f_i(x_1, \ldots, x_n) = 0 \text{ for } 1 \leq i \leq s. \tag{1}$$

Hilbert's Nullstellensatz (which was probably already considered by Kronecker) states that this formula is false if and only if an *arithmetic Bézout identity* holds, i.e. if and only there exist a non–negative integer $a \in \mathbb{Z} \setminus \{0\}$ and polynomials $g_1, \ldots, g_s \in \mathbb{Z}[X_1, \ldots, X_n]$ such that the following identity holds :

$$a = g_1 f_1 + \cdots + g_s f_s. \tag{2}$$

This arithmetic presentation of the Hilbert Nullstellensatz is more suitable than the standard one for the study of the *consistency problem over prime fields of positive characteristic*. More precisely,

[1]: Research was partially supported by the following French and Spanish grants :
CNRS 1026 MEDICIS and PB96–0671–C02–02.
[2]: Departamento de Matemáticas, Estadística y Computación.
Facultad de Ciencias, Universidad de Cantabria, E-39071 Santander, Spain
[3]: Departamento de Matemática e Informática, Campus de Arrosadía.
Universidad Pública de Navarra, E-31006 Pamplona, Spain
[4]: Departamento de Matemática, Facultad de Ciencias Exactas.
Calle 50 y 115, Universidad Nacional de la Plata, (1900) La Plata, Argentina

let us consider a prime number $p \in \mathbb{N}$, $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ the prime field of *positive* characteristic p, and let K_p be an algebraic closure of $\mathbb{F}_p$. For every polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$ we denote by $\bar{f} \in \mathbb{Z}/p\mathbb{Z}[X_1, \ldots, X_n]$ the polynomial obtained by taking residues $\pmod p$ in the coefficients of f. The consistency problem over K_p on input system S can now be stated as deciding whether the following formula is true or not :

$$\exists x_1 \in K_p, \ldots, \exists x_n \in K_p, \bar{f}_i(x_1, \ldots, x_n) = 0 \text{ for } 1 \leq i \leq s. \tag{3}$$

One of the main topics of this thesis will be the estimation of the number of primes p for a given system S such that the formula (3) is false. In order to formalize this problem, we introduce the following function (which depends on S) :

$$\pi_S : \mathbb{Z}_{\geq 0} \longrightarrow \mathbb{Z}_{\geq 0}$$

defined by $\pi_S(x) :=$ the number of primes p such that $p \leq x$ and the formula (3) is true. A precise description of this function π_S is not known up to now. For the moment, only upper and lower bounds are available, which will be improved here.

One of the motivations for this study is the interest in reductions of bounded complexity from the consistency problem in characteristic 0 with the consistency problem in positive characteristic.

This kind of reductions have been used recently by P. Koiran in [41]. Let us observe that the consistency problem has (up to now) worst case upper time bounds which are exponential in the input length, whereas the upper space bounds are known to be polynomial by [13]. In fact, Koiran's work is stronger, since it reduces consistency problems in characteristic 0 to another relevant question concerning polynomial equation systems : the *satisfiability* problem.

The satisfiability problem for a system $S \subseteq \mathbb{F}_p[X_1, \ldots, X_n]$ is to decide whether there exists a solution in $\mathbb{F}_p^n$ for the system S or not. For fixed prime number p, the satisfiability problem is known to be NP–complete due to a result of [19]. In [41] a reduction from the consistency problem in characteristic zero to the satisfiability problem in positive characteristic is shown. This yields more precise space bounds for the characteristic zero case than those shown in [13]. This reduction is based on estimates for upper bounds for π_S using the results of [44], also yielding a lower bound for π_S assuming the Generalized Riemann Hypothesis. Corollary 5 on the arithmetic Nullstellensatz improves the known upper bounds for π_S. In the sequel we also show a lower bound for π_S improving on the one presented in [60], assuming the Generalized Riemann Hypothesis. This lower bound is a consequence of the studies done in [29], [28], [25], [30].

Let us observe that if the system S is inconsistent over $\mathbb{C}$, the arithmetic Bézout identity (2) holds. In that case, π_S is a bounded function. The obvious reason is that if (2) holds, then (3) is false for all those prime numbers p such that $a \not\equiv 0 \pmod p$. In particular, if we know the value of a from the arithmetic Nullstellensatz, we immediately obtain the following bound :

$$\pi_S(x) \leq \log_2 |\, a \,| \text{ for all } x \in \mathbb{N}$$

where $|\, a \,|$ denotes the usual absolute value of a. Conversely, if (1) is a valid formula, π_S is unbounded but co–finite, i.e. $\pi - \pi_S$ is a bounded function. Thus, studies around the arithmetic Bézout identity (2) with estimates for the absolute value of a (and consequently of the coefficients of the polynomials $g_1, \ldots, g_s$) are of central relevance for estimating π_S.

A discussion of the historical achievements around (arithmetic) Bézout identities follows. Let us assume now that d is an upper bound for the degrees of the polynomials in the input system $S = \{f_1, \ldots, f_s\}$ and that h is an upper bound for the absolute values of the coefficients of the polynomials in S. First estimates for $\log_2 |\, a \,|$ were obtained by the systematic use of upper bounds for the degrees of the polynomials $g_1, \ldots, g_s$ that may occur in a Bézout identity like (2).

Let us assume from now on that the system S is inconsistent and denote by $D(d, n)$ the minimum of the degrees of the polynomials $g_1 f_1, \ldots, g_s f_s$ in the Bézout identity (2).

The first remarkable achievement was G. Hermann's upper bound that stated $D(d,n) \leq d^{2^n}$, cf. [37]. We have to wait until the late eighties to see major improvements of Hermann's bound. In [12], [13], [14], [42] the bound was improved to $D(d,n) \leq \max\{3,d\}^n$, cf. also [22] and [65]. For the case of $d = 2$, which seemed to escape these techniques, the following bound was obtained in the nineties, cf. [21], [70] :

$$D(d,n) \leq 4nd^n$$

which also holds for $d = 2$. Recently, [78] showed $D(d,n) \leq 2^{n+1}$ for $d = 2$. The lower bound $D(d,n) \geq d^n - d^{n-1}$ is a consequence of the following example due to Mora-Lazard-Masser-Philippon, see [12] :

$$S := \{X_1^d, X_1 - X_2^d, \ldots, X_{n-2} - X_{n-1}^d, 1 - X_{n-1}X_n^{d-1}\}. \tag{4}$$

One can interpret Equation (2) as a big system of linear equations in the unknowns a and the coefficients of the polynomials $g_1, \ldots, g_s$. Making appropriate use of Cramer's rule, we obtain a as the determinant of a square submatrix M with approximately $\binom{D(d,n)+n}{n}$ rows and columns. We then conclude :

$$\log_2 |\, a \,| \leq D(d,n)^n \log_2 h.$$

The previous bounds imply the estimation $\pi_S(x) \leq \log_2 |\, a \,| \leq d^{n^2} s \log_2 h$, which is still far from being satisfactory.

P. Philippon establishes in his paper [65] the bound

$$\log |\, a \,| \leq (n+2)^2 \cdot (8n+1)^{n+2} \cdot (\log h + d) \cdot d^n,$$

where h is a bound on the absolute values of the coefficients of the input polynomials. The contributions of [7], [6] provide the following more precise upper bounds :

$$\pi_S(x) \leq \log_2 |\, a \,| \leq k(n) d^{8n+3} (\log_2 h + d \log_2 d) \tag{5}$$

where $k(n)$ is an effective (but super-exponential) bound depending only on n. In [43], [44] the following, even more precise upper bound was obtained :

$$\pi_S(x) \leq \log_2 |\, a \,| \leq (nd)^{cn} (\log_2 h + \log_2 s)$$

for a universal constant $0 < c < 32$. These bounds seemed to be a final achievement because of the following example adapted from the above example (4) for $a \in \mathbb{Z} \setminus \{0\}$, cf. [44], [56] :

$$S := \{X_1 - 2, X_2 - X_1^d, \ldots, X_n - X_{n-1}^d, X_n\}.$$

Here we observe that for the constant a obtained from the Bézout equality (2) for this inconsistent system S holds $\log_2 |\, a \,| \geq d^{n-1}$.

However, all these approaches had some inconvenience. First of all, their estimates depend strongly on the syntactical representation of the polynomials (degree, number of variables, absolute value of the coefficients). In particular, for systems of degree 2 the previous bounds in [6], [7] and [43], [44] yield a bound of order :

$$\pi_S(x) \leq \log_2 |\, a \,| \leq n^{cn+3} (\log_2 h + 2).$$

Secondly, this dependence from the syntactical representation of the input system S hides any special features of the system with respect to arithmetic Bézout identities. For instance, these features will not be perceivable when we are facing systems as the following one :

$$S := \{X_1 - 1, X_2 - X_1^d, \ldots, X_n - X_{n-1}^d, X_n\}.$$

In this example, the integer $a \in \mathbb{Z} \setminus \{0\}$ in identity (2) can be chosen to be exactly 1, whereas all the approaches cited above yield bounds exponential in n.

In the sequel we also show that the Nullstellensatz depends on the special features of some geometric objects associated to the input system S. We show that we can profit from these special features to improve the estimates for upper bounds of $\log_2 |a|$. In this sense, the works [23], [43] and [44] were fundamental. These contributions essentially proved that the polynomials $g_1, \ldots, g_s$ and the integer $a \in \mathbb{Z} \setminus \{0\}$, occurring in a Bézout identity can be chosen with very special features with respect to their representation.

In fact, the authors showed in [44] that $g_1, \ldots, g_s$ and a can be expressed in terms of the input system in a way far better than expected : For the case $d \geq n$ the polynomials $g_1, \ldots, g_s$ and the integer a can be evaluated by a (certain kind of) program of polynomial size $d^{O(n)}$. This particular property yields bounds of order equivalent to those in (5). Moreover, it was shown that the circuits (*straight–line programs*) which evaluate the polynomials can be computed by a Turing machine running in time essentially polynomial in $d^n \log_2 h$.

However, the complexity estimates for the elimination procedures underlying [43], [44] were also of syntactic nature (they were strongly inspired by [27]). The resulting bounds are of syntactic nature too (depending on the bound d^n) and thus can not profit from the special features of the input system (as in the example before).

Statement of results Several intrinsic complexity elimination procedures were developed since then in [29], [43], [28], [25], [30], [60]. These elimination procedures have the following properties :

- they can be adapted to the syntactic representation chosen to encode the polynomials in the input system S.
- two intrinsic invariants (called the degree and height of the system S) appear in the complexity estimates.

These methods have been discussed in detail in [60] and are fundamental to the forthcoming Theorem 1 and 2. Let us also mention that these intrinsic elimination methods inspired a new type of effective Nullstellensätze with intrinsic degree bounds of order $3n^2 d\delta_S$ in [45] and for the sparse monomial representation of order $\min\{n, s\}^2(d + 3n)\delta_S$ in [76], [77], where δ_S is the *geometric degree of the system* S as in Definition 50 on page 40.

An estimate in terms of intrinsic invariants for the representation of the constant $a \in \mathbb{Z} \setminus \{0\}$ and the polynomials $g_1, \ldots, g_s \in \mathbb{Z}[X_1, \ldots, X_n]$ by straight–line programs (see Section 2.2 for a definition) can be obtained as a consequence of the following Theorem :

Theorem 1 *There exists a universal constant $c_1 > 0$ with the following property : Let R be the ring of algebraic integers of a given number field K and $f_1, \ldots, f_t, f \in R[X_1, \ldots, X_n], t \leq n+1$ polynomials of degree at most d. Suppose that the following properties are verified :*

i) All the ideals $(f_1, \ldots, f_i)$ in $K[X_1, \ldots, X_n]$ are radical ideals defining a variety of co-dimension i for $1 \leq i \leq t-1$.

ii) The polynomial f_t is not a zero divisor in the residue ring $K[X_1, \ldots, X_n]/(f_1, \ldots, f_{t-1})$.

iii) The polynomial f belongs to the ideal $(f_1, \ldots, f_t)$ in $K[X_1, \ldots, X_n]$.

iv) There is given a straight–line program Γ of size L, non–scalar depth ℓ and parameters in a finite set $\mathcal{F} \subset R$, such that Γ evaluates the polynomials $f_1, \ldots, f_t, f$.

Let us define δ as the maximum of the geometric degrees (see Section 3) of the intermediate varieties, $\delta := \max\{\deg V(f_1, \ldots, f_i) : 1 \leq i \leq t-1\}$.

1) Then, there exists a division-free straight–line program Γ_1 *of size* $(tdL\delta)^{c_1}$*, non–scalar depth* $O((n+\ell)^2 \log_2 \delta)$ *and parameters in* $\mathcal{F} \cup \{z \in \mathbb{Z} : |z| \leq (tdL\delta)^{c_1}\} \subseteq R$*, such that* Γ_1 *evaluates polynomials* $g_1, \ldots, g_t \in R[X_1, \ldots, X_n]$ *and a non–zero constant* $a \in R \setminus \{0\}$ *such that the following holds :*

$$af = g_1 f_1 + \cdots + g_t f_t.$$

2) Moreover, the polynomials $g_1, \ldots, g_t$ *verify the degree bound* $\deg(g_i) \leq 3t^2 d\delta$*.*

Our proof of Theorem 1 (see Section 6) exhibits explicitly such a straight–line program Γ_1 evaluating the polynomials $g_1, \ldots, g_t$. However, the non–scalar depth of the straight–line program describing the polynomials obtained in this way is too big (of order $O(n \log_2 \delta)$) to yield good bounds for the height of the constant $a \in R$ and the polynomials $g_1, \ldots, g_t \in R[X_1, \ldots, X_n]$ in the Bézout identity.

By an alternative approach, analyzing the parallel complexity of the polynomials $a^{-1}g_i \in K[X_1, \ldots, X_n]$ and starting from the so-called *geometric solution* (see Section 3 for a definition) produced by the algorithm underlying Theorem 1, we yield the following result :

Theorem 2 *There exists a universal constant* $c_2 > 0$ *with the following property : Let* R *be the ring of algebraic integers of a given number field* K *and* $f_1, \ldots, f_t, f \in R[X_1, \ldots, X_n], t \leq n+1$ *polynomials of degree at most* d *satisfying conditions* $i), ii)$ *and* $iii)$ *of Theorem 1 above. Suppose we are given a division-free straight–line program* Γ *of size* L*, non–scalar depth* $\ell = O(\log L)$ *and parameters in a finite set* $\mathcal{F} \subset R$ *such that* Γ *evaluates the polynomials* $f_1, \ldots, f_t, f$*. Then there exists a division-free straight–line program* Γ_2 *of size* $((td)^t L\delta)^{c_2}$*, non–scalar depth* $O(\log_2 t + \log_2 d + \log_2 L + \log_2 \delta)$*, and parameters in* $\mathcal{F} \cup \{z \in \mathbb{Z} : |z| \leq ((td)^t L\delta)^{c_2}\} \subseteq R$*, such that from the geometric solutions of the varieties* $V(f_1, \ldots, f_i), 1 \leq i \leq t-1$*, the straight–line program* Γ_2 *evaluates polynomials* $h_1, \ldots, h_t \in R[X_1, \ldots, X_n]$ *and a non–zero element* $b \in R$ *such that holds :*

$$bf = h_1 f_1 + \cdots + h_t f_t.$$

Moreover, the polynomials $h_1, \ldots, h_t$ *verify the degree bound* $\deg(h_i) \leq 3t^2 d\delta$*.*

The proof of the above Theorem 2 as established in Section 7 shows that the straight–line program evaluating the polynomials $g_1, \ldots, g_t$ for the representation found by the algorithms underlying Theorem 1 and 2 are, up to constants, the same, i.e. $a^{-1}g_i = b^{-1}h_i$ holds in the above Theorems.

The total complexity of the algorithm underlying Theorem 2 is obviously worse than the result obtained in the first Theorem. This is due to the iterated interpolation technique used, which causes an increasal of the straight–line program size. Nevertheless, at the same time we obtain an improved bound on the non–scalar depth of the straight–line program evaluating the polynomials, and as these are up to constants identical, this yields an improved overall bound for the constant a in the Bézout identity.

The two Theorems above have meaningful consequences in terms of complexity and arithmetic estimates for the membership problem in complete intersection ideals. As a first consequence of Theorem 1, the method described in Section 6, and the results obtained in the series of papers [29], [43], [28], [25], [30], [60] we have :

Corollary 3 (Bounds on the complexity) *With the same notations and hypotheses as in Theorem 1, let* $R = \mathbb{Z}$ *be the ring of integers. Then there exists a bounded error probability Turing machine* M *which takes as input polynomials* $f_1, \ldots, f_t, f$ *in* $\mathbb{Z}[X_1, \ldots, X_n]$ *and produces a straight–line program computing a constant* $a \in \mathbb{Z} \setminus \{0\}$ *and polynomials* $g_1, \ldots, g_t \in \mathbb{Z}[X_1, \ldots, X_n]$ *verifying :*

$$af = g_1 f_1 + \cdots + g_t f_t.$$

Moreover, the running time of M *is polynomial in* $ndL\delta$*.*

On the other hand, Theorem 2 is helpful to obtain arithmetic estimates for the polynomials occuring as quotients in a division modulo a complete intersection ideal. We have chosen two different height measures for polynomials. The first one takes only archimedean absolute values into account for polynomials $g \in R[X_1, \ldots, X_n]$. The second one is the invariant (logarithmic) height as introduced by P. Philippon in the series of papers [66], [67], [68] to give a notion of height for unmixed homogeneous ideals (here invariance means invariance under scalar multiplication). In particular, using the notation of Theorem 1 and 2, the invariant heights of $a^{-1}g_i$ and $b^{-1}h_i$ agree. For a finite subset $\mathcal{F} = \{a_1, \ldots, a_m\} \subseteq R$ we define the height $ht(\mathcal{F})$ as the logarithmic height (following [50]) of the projective point $(1 : a_1 : \ldots : a_m)$.

We have the following Corollary to Theorem 2 :

Corollary 4 (Bounds on the height) *There exists a universal constant $c_3 > 0$ with the following property : With the same notations and assumptions as in Theorem 2, let $\eta, \tilde{\eta}$ be respectively the quantities defined by :*

$$\eta := \max\{ht(V(f_1, \ldots, f_i)) : 1 \leq i \leq t-1\}, \qquad \tilde{\eta} := \max\{\widetilde{ht}(V(f_1, \ldots, f_i)) : 1 \leq i \leq t-1\}$$

where $ht(V(f_1, \ldots, f_i))$ is the normalized logarithmic height of the variety $V(f_1, \ldots, f_i)$ which takes into account only the archimedean absolute values, whereas $\widetilde{ht}(V(f_1, \ldots, f_i))$ is the invariant logarithmic height of the elimination polynomials of $V(f_1, \ldots, f_i)$ (see Def. 38 on page 30).

For the constant b and the polynomials $h_1, \ldots, h_t$ as evaluated by the straight–line program of Theorem 2 the following estimates hold :

$$\max\{ht(b), ht(h_1), \ldots, ht(h_t)\} \leq (ndL\delta)^{c_3}(\eta + ht(\mathcal{F})), \text{ and}$$

$$\max\{\widetilde{ht}(b), \widetilde{ht}(h_1), \ldots, \widetilde{ht}(h_t)\} \leq (ndL\delta)^{c_3}(\tilde{\eta} + ht(\mathcal{F})) \text{ holds.}$$

Let us remark that $\widetilde{ht}(a) = \widetilde{ht}(b) = 1$ holds and the polynomials $g_1, \ldots, g_t$ evaluated by the straight–line program of Theorem 1 also verify that :

$$\widetilde{ht}(g_i) = \widetilde{ht}(h_i) \leq (nd\delta)^{c_3}(\eta + ht(\mathcal{F})).$$

The conditions *i)* and *ii)* imposed on the polynomials $f_1, \ldots, f_t, f$ in Theorem 1 and also in Theorem 2 may seem very restrictive, but this is not the case as will be shown in Section 5.

In a purely existential form, combining Theorems 1 and 2 above, we may also show estimates for the Arithmetic Nullstellensatz of the following minimal nature.
Let $S = \{f_1, \ldots, f_s\} \subseteq R[X_1, \ldots, X_n]$ be a sequence of polynomials of degree at most d generating the trivial ideal in $K[X_1, \ldots, X_n]$. For every positive integer $H \in \mathbb{N}$, we define the class S_H of sequences of polynomials $F := (F_1, \ldots, F_r)$ with $1 \leq r \leq n+1$ with the following properties :

i) for every $i, 1 \leq i \leq r$, F_i is not a zero divisor in $K[X_1, \ldots, X_n]/(F_1, \ldots, F_{i-1})$

ii) for every $i, 1 \leq i \leq r-1$ the ideal $(F_1, \ldots, F_i)$ is a radical ideal of codimension i in $K[X_1, \ldots, X_n]$.

iii) $(F_1, \ldots, F_r) = (f_1, \ldots, f_s)$ in $K[X_1, \ldots, X_n]$

iv) there exist integer numbers $\lambda_{ij} \in \mathbb{Z}$ with $1 \leq i \leq r$ and $1 \leq j \leq s$ such that $|\lambda_{ij}| \leq H$ and $F_i = \lambda_{i1}f_i + \cdots + \lambda_{is}f_s$

Estimates for H such that $S_H \neq \emptyset$ are shown in Section 5 below. In fact, there exists a universal constant $c_1 > 0$ such that for every given system S and every $H \geq d^{c_1 n}$ the set S_H is non–empty.
Now, let $S \subset R[X_1, \ldots, X_n]$ be a finite system defining the trivial ideal in $K[X_1, \ldots, X_n]$ and $H \in \mathbb{N}$ such that $\widetilde{S}_H \neq \emptyset$. For every sequence $F = (F_1, \ldots, F_r) \in S_H$ we define :

- $\delta(F) := \max\{\deg V(F_1,\ldots,F_i) : 1 \leq i \leq r-1\}$ where $\deg V(F_1,\ldots,F_i)$ is the geometric degree of the unmixed algebraic variety $V(F_1,\ldots,F_i) := \{x \in \mathbb{C}^n : F_1(x) = 0,\ldots,F_i(x) = 0\}$ of codimension i. Here geometric degree is used as introduced in [34] without counting multiplicities or points ar infinity.
- $\widetilde{\eta}(\widetilde{F}) := \max\{\widetilde{\eta}(V(F_1,\ldots,F_i)) : 1 \leq i \leq r-1\}$ where $\widetilde{\eta}(V(F_1,\ldots,F_i))$ is the logarithmic invariant height of the variety $V(F_1,\ldots,F_i) \in \mathbb{C}^n$ as introduced in [66], [67], [68].
- $\eta(\widetilde{F}) := \max\{\eta(V(F_1,\ldots,F_i)) : 1 \leq i \leq r-1\}$ where $\eta(V(F_1,\ldots,F_i))$ is the logarithmic height of the variety taking into account only archimedean absolute values.

From these estimates we can define the minimal tradeoff between degree and height of a system S. With the previous notions and notations, given $S \subseteq R[X_1,\ldots,X_n]$ and $H \in \mathbb{N}$ such that $S_H \neq \emptyset$, we define :

$$\delta \times \widetilde{\eta}_{\min}(S,H) := \min\{\delta(F)\cdot\widetilde{\eta}(F) : F \in S_H\},$$

where $\delta_{\min}(S,H) := \min\{\ \delta(F) : F \in S_H\}, \qquad \widetilde{\eta}_{\min}(S,H) := \dfrac{\delta \times \widetilde{\eta}_{\min}(S,H)}{\delta_{\min}(S,H)}.$

Corollary 5 (Existential estimates for the Arithmetic Nullstellensatz) *With the previous notations, let $S = \{f_1,\ldots,f_s\} \in \mathbb{Z}[X_1,\ldots,X_n]$ be a sequence of polynomials of degree at most d generating the trivial ideal in $K[X_1,\ldots,X_n]$. Let us assume that the polynomials in S can be evaluated by a non–scalar straight–line program of size L, non–scalar depth $\ell = O(\log_2 L)$ and parameters in a finite set $\mathcal{F} \subseteq \{z \in \mathbb{Z} : |\,z\,| \leq h\}$. Let $H \in \mathbb{N}$ be such that $\widetilde{S}_H \neq \emptyset$. Then, there exists a universal constant $c > 0$ and a non–zero $a \in Rwzero$ such that the following holds :*

i) $a = g_1 f_1 + \cdots + g_s f_s$,

ii) $\deg(g_i) \leq 3n^2 d\delta_{\min}(S,H)$ *holds for* $1 \leq i \leq s$,

iii) The invariant (logarithmic) height of $g_1,\ldots,g_t$ verifies the following upper bound :

$$\widetilde{ht}(g_i) \leq (ndL\delta_{\min}(S,H))^c(ht(\mathcal{F}) + \widetilde{\eta}_{\min}(S,H) + \log_2 H + \log_2 s).$$

iv) The polynomials $g_1,\ldots,g_s \in R[X_1,\ldots,X_n]$ and the constant $a \in \mathbb{R}\setminus\{0\}$ can be evaluated by a straight–line program over K of size $(ndL\delta_{\min}(S,H))^c$ and parameters in

$$\mathcal{F} \cup \{z \in \mathbb{Z} : |\,z\,| \leq \max\{(ndL\delta_{\min}(S,H))^c, H\}\}.$$

Here, $\widetilde{ht}(g_i)$ is the above mentioned notion of height for multivariate polynomials introduced by P. Philippon in [64]. However, these estimates will equally hold for any reasonable notion of logarithmic invariant height. As observed in Section 5 below, there exists a universal constant $c > 0$ such that for $H \geq O(d^{cn})$, we have $\widetilde{S}_H \neq \emptyset$.

These existential estimates are complementary of some others of a more computational nature we are going to introduce. Let us observe that for approriate bounds H a procedure to find some sequence $\widetilde{F} \in \widetilde{S}_H$ is given in Section 5 below. However, the computable sequence $\widetilde{F}$ is not necessarily the best one in the sense of minimizing the product of $\delta_{\min}$ and $\eta_{\min}$.
Thus, we have also developped a notion of degree and height of a system S according to the computational feasablity of this $\widetilde{S} \in \widetilde{S}_H$. These notions are essentially the geometric degree of the system δ_S, and the logarithmic archimedean height of the system η_S and the logarithmic invariant height of the system $\widetilde{\eta}_S$ as defined in Section 5 below.

Let us remark that these notions depend on the geometric and arithmetic features of the input system, independently from the syntactic representation of the polynomials in S. Let us also remark that δ_S

is in any case at most d^{n-1} and that applying for instance the results of [44], $\widetilde{\eta}_S$ and η_S can be shown to be of order $d^{O(n)}$.
Actually, the procedure followed in Section 6 to show Theorem 1, Corollary 3, Theorem 2, Corollary 4 and Corollary 5 (which are existential statements) is the description of an algorithmic procedure based on previous statements and geometric elimination methods (see for example [29], [43], [28], [25], [30], [60]). We also obtain the following statements :

Corollary 6 (Membership problem for complete intersection varieties) *Let R be the ring of algebraic integers of a number field K and for $t \leq n$ $f_1, \ldots, f_t, f \in K[X_1, \ldots, X_n]$ polynomials of degree at most d verifying the following hypotheses :*

i) the ideal $f_1, \ldots, f_t$ in $K[X_1, \ldots, X_n]$ is a complete intersection ideal of codimension t,

ii) the polynomial f belongs to the ideal $(f_1, \ldots, f_t)$ of $K[X_1, \ldots, X_n]$, and

iii) there exists a non–scalar straight–line program Γ of size L, non–scalar depth $\ell = O(\log_2 L)$ and parameters in a finite set $\mathcal{F} \subset R$.

Then, there exist a non–zero constant $a \in R \setminus \{0\}$ and polynomials $g_1, \ldots, g_t \in R[X_1, \ldots, X_n]$ such that the following properties hold :

i) $af = g_1 f_1 + \cdots + g_t f_t$,

ii) $\max\{\deg(g_i) : 1 \leq i \leq t\} \leq 3t^2 d\delta$, where δ is the degree of the system $f_1, \ldots, f_t$,

iii) the polynomials $a^{-1}g_1, \ldots, a^{-1}g_t$ can be evaluated by a non–scalar straight–line program over K of size $(tdL\delta)^{O(1)}$ using parameters in $\mathcal{F} \cup \{a \in \mathbb{Z} : |\, a \,| \leq (tdL\delta)^{O(1)}\}$,

iv) the logarithmic height of $a, g_1, \ldots, g_t$ verify the following bounds :

$$ht(a) \leq (tdL\delta)^{O(1)}(ht(\mathcal{F}) + \eta), \qquad ht(g_i) \leq (tdL\delta)^{O(1)}(ht(\mathcal{F}) + \eta)$$

where η is the (logarithmic) height of the system $f_1, \ldots, f_t$, as defined in Section 3.

v) the invariant (logarithmic) height of the polynomials $g_1, \ldots, g_t$ verifies the following upper bound :

$$\widetilde{ht}(a^{-1}g_i) = \widetilde{ht}(g_i) \leq (tdL\delta)^{O(1)}(ht(\mathcal{F}) + \widetilde{\eta}).$$

As in Corollary 5, a straight–line program evaluating the integer a and the polynomials $g_1, \ldots, g_t \in \mathbb{Z}[X_1, \ldots, X_n]$ can be computed by a bounded error probability Turing machine running in time

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

We are now in conditions to give upper bounds for the function π_S. In particular, we obtain directly from claim *iv*) of Corollary 5 the following upper bound :

Corollary 7 (Upper bounds for π_S) *There exists a universal constant $c_1 > 0$ (in particular, independent of x) such that for every given system $S = \{f_1, \ldots, f_s\} \subseteq \mathbb{Z}[X_1, \ldots, X_n]$ of polynomials verifying the hypotheses of Corollary 5, the function $\pi_S : \mathbb{N} \to \mathbb{N}$ verifies the bound :*

$$\pi_S(x) \leq (ndL\delta_S)^{c_1}(ht(\mathcal{F}) + \eta_S + \log_2 s).$$

The reduction of the consistency problem in characteristic zero to positive characteristic is not satisfactorily characterized by the upper and lower bounds obtained for π_S. Another outstanding estimate concerns density questions in the following sense :

Supposing that S is inconsistent, π_S is a bounded function. We are also interested in the following density question :

Given a system of multivariate polynomial equations $S \subset \mathbb{Z}[X_1, \ldots, X_n]$, inconsistent over $\mathbb{C}$. Let $\mathbb{P}$ denote the set of all primes and let $I \subseteq \mathbb{P}$ be a given finite set of prime numbers. We are interested in estimates of the ratio of prime numbers $p \in I$ such that the system S remains inconsistent when reduced mod p and the cardinality of I. We define a density function depending only on the system S and the set of chosen primes I :

$$P_S(I) := \frac{\#\{p \in I : S \pmod p \text{ is inconsistent}\}}{\#(I)}.$$

Estimates for density functions depending on the representation of a in terms of arithmetic operations were initiated in the late seventies and early eighties (as in [71], [38], cf. also [63]). Here, we give the following lower bound for $P_S(I)$:

Corollary 8 *There exist universal constants $c_2, c_3 > 0$ such that the following holds : For every given system of multivariate polynomials $S = \{f_1, \ldots, f_s\} \subseteq \mathbb{Z}[X_1, \ldots, X_n]$ verifying the hypotheses of Corollary 5, and for every finite subset $I \subseteq \mathbb{P}$ we have :*

i) $P_S(I) \geq 1 - \frac{(ht(\mathcal{F})+\log_2 L)(\delta_S n 2^\ell)^{c_2 n}}{\#(I)}$

ii) $P_S(I) \geq 1 - \frac{2^{\mathcal{C}(S)}}{\#(I)}$

where $\mathcal{C}(S) := \max\{c_3 \log_2(ndL\delta_S), (\eta_S + ht(\mathcal{F}) + \log_2 s)\}$.

Let us observe that the first bound does not take into account the height of the intermediate varieties whereas the second one is polynomial in all the parameters involved. These lower bounds can be applied to estimate densities for small prime numbers as done in the following Corollary :

Corollary 9 *There exist universal constants $c_2', c_3' > 0$ such that the following holds :*
For every given system of polynomials $S = \{f_1, \ldots, f_s\} \subseteq \mathbb{Z}[X_1, \ldots, X_n]$ verifying the hypotheses of Corollary 5, we have :

i) The probability that, choosing at random a prime number $p \in \mathbb{Z}$ of bit length bounded by $(ht(\mathcal{F}) + \log_2 L)(\delta_S n 2^\ell)^{c_2' n}$ such that the modular system

$$\bar{f}_1, \ldots, \bar{f}_s \in \mathbb{F}_p[X_1, \ldots, X_n] \tag{6}$$

is inconsistent, is at least $\frac{1}{2}$.

ii) The probability that choosing at random a prime number $p \in \mathbb{Z}$ in the set $\{2, \ldots, (ndL\delta_S)^{c_3'}(ht(\mathcal{F}) + \eta_S + \log_2 s)\}$ such that the modular system (6) is inconsistent, is at least $\frac{1}{2}$.

Observe that the first bound does not take into account the height of the system. The second bound yields together with the bounds obtained in [43] and [44] a reduction from inconsistent systems in characteristic 0 to inconsistent systems in characteristic p, where the bit length of p is polynomial in the input size.

As for the lower bounds for π_S, we make use of the Generalized Riemann Hypothesis and Chebotarev's Density Theorem to obtain the following lower bound in terms of intrinsic parameters :

Theorem 10 (Lower bounds for π_S [60]) *For consistent systems S the following lower bound holds :*

$$\pi_S(x) \geq \frac{1}{\delta_S}\left(\pi(x) - \delta_S^{c_1}(n - r + \eta_s)(1 + c_2\sqrt{x}) - \delta \log x\right).$$

2 Fixing notations and notions

For the correct and precise elaboration of the results announced in the introduction ingredients from different fields are required. Most of the material is common knowledge, well spread over the mathematical literature. Nevertheless, as the topics range from theoretical computer science to algebraic and diophantine geometry, commutative algebra and back, it is very unlikely that all of the literature covered is available to all of the readers. Therefore we settle in this Section the necessary definitions and properties in a succinct form. In this way, the reader will hopefully be able to follow even the less familiar notions and relations up to a level allowing him to proceed to the forthcoming Sections. Also included are several references giving a more complete view on the subjects.

In Section 2.1, the notation used for multivariate polynomials, absolute values over number fields and the Mahler measure of a polynomial are introduced. Then we briefly discuss in Section 2.2 the theoretical background of the complexity model chosen in this work for the metric measures introduced in Subsection 2.1.4.

2.1 Basic ingredients

2.1.1 Multivariate polynomials

A multivariate polynomial over a field K is a syntactic mathematical object whose existence is due to the systematic study of a certain class of semantical objects : the polynomial functions

$$f : K^n \longrightarrow K.$$

Thus in a polynomial we may observe two aspects : the syntactical and the semantical. Years of tradition in the systematic study of polynomial functions have established a convention of representing them by their monomial expansions. Therefore a relevant part of the mathematical studies has tried to relate both aspects. Several different estimates have been used just to connect the syntactical representation and the semantical geometric object, for instance, relating the degree of a polynomial and the degrees of the hypersurfaces given as the fibers $f^{-1}(\{0\})$.

In what follows we give the notation for the dense monomial encoding : Let $\langle \cdot, \cdot \rangle$ denote the standard hermitian product on the field of complex numbers $\mathbb{C}$. For every complex number $a \in \mathbb{C}$ we denote by $|\, a \,| := \sqrt{\langle a, a \rangle}$ its absolute value. Each multivariate complex polynomial $P \in \mathbb{C}[X_1, \ldots, X_n]$ has a *dense representation* of the form :

$$P(X_1 \ldots, X_n) = \sum_{|\, \mu \,| \leq d} P_\mu \, X_1^{\mu_1} \cdots X_n^{\mu_n}$$

where $d := \deg(P)$ denotes the total degree of P, $\mu := (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n$ is a multi–index, $|\, \mu \,| := \mu_1 + \cdots + \mu_n$ is its length and P_μ are coefficients in $\mathbb{C}$. Whereas the degree is an outstanding syntactical invariant for the geometry of the hypersurface defined by a polynomial, other metric measures are required when diophantine properties are studied. We define the (standard) weight of a complex polynomial $P \in \mathbb{C}[X_1, \ldots, X_n]$ as :

$$wt(P) := \sum_{|\, \mu \,| \leq d} |\, P_\mu \,|.$$

The number of monomials of a multivariate polynomial P of total degree d is given by the length of the vector of coefficients of P in the dense monomial encoding, which is $\binom{d+n}{n}$.

2.1.2 Absolute values over number fields

We resume here in a very concise form the language and notation used for absolute values over number fields. For an introduction refer to e.g. [50, Chapter 1] whereas a more complete exposition of the

theory of absolute values can found in Artin's *Algebraic Numbers and Algebraic Functions* or [55]. Let R be the ring of algebraic integers of a number field K and let $\mathbb{K}$ be an algebraic closure of K.

By K_ν we denote the completion of K with respect to the absolute value $|\cdot|_\nu$ and by $\mathbb{K}_\nu$ we shall denote the algebraic closure of K_ν. For sake of simplicity we assume that for archimedean ν its algebraic closure $\mathbb{K}_\nu$ is included in $\mathbb{C}$.

Finally, according to whether $|\cdot|_\nu$ is archimedean or not, we shall denote by n_ν the degree of K_ν over the completion of $\mathbb{Q}$ with respect to the absolute value $|\cdot|_\nu : \mathbb{Q} \longrightarrow \mathbb{R}$. Following [50], let M_K be a proper set of absolute values of K. We assume that M_K has been chosen such that it satisfies Weil's *product formula* with multiplicities n_ν : For all $x \in K \setminus \{0\}$ holds

$$\frac{1}{[K:\mathbb{Q}]} \sum_{\nu \in M_K} n_\nu \log |x|_\nu = 0 \tag{7}$$

where log stands for the natural logarithm, cf. [50, Chapter 2]. Let us recall that by [50, Proposition 4.3] for any given absolute value w on $\mathbb{Q}$ and all absolute values ν extending w to K, the following holds :

$$\sum_{\nu|w} n_\nu = [K:\mathbb{Q}]. \tag{8}$$

Observe that the proper set of absolute values M_K has only a finite number of archimedean absolute values (precisely the independent extensions of the ordinary archimedean value on $\mathbb{Q}$ to K induced by the non–isomorphic embeddings of K into $\mathbb{C}$, see below).

Let us recall that for archimedean valuations, i.e. $\nu \in S$, the absolute value $|\cdot|_\nu$ is defined in the following terms : for every $\nu \in S$ there exists an associated embedding $\sigma_\nu : K \longrightarrow \mathbb{C}$ such that for all $a \in K$,

$$|a|_\nu := |\sigma_\nu(a)|,$$

where $|\cdot|$ stands for the usual absolute value in $\mathbb{C}$. For archimedean valuations $\nu \in S$, given P a polynomial in $R[X_1, \ldots, X_n]$, we denote by $\sigma_\nu(P)$ the polynomial in $\mathbb{C}[X_1, \ldots, X_n]$ given by

$$\sigma_\nu(P) := \sum_{|\mu| \le d} \sigma_\nu(P_\mu) X_1^{\mu_1} \cdots X_n^{\mu_n}.$$

Now, for all valuations $\nu \in M_K$ we define the *height of P with respect to the absolute value* $|\cdot|_\nu$ as the maximum of the absolute values of the coefficients of P with respect to $|\cdot|_\nu$, i.e. $H_\nu(P) := \max_{|\mu| \le d}\{|P_\mu|_\nu\}$. We define in the same way for a finite set $\mathcal{F} \subseteq R$ the *height of $\mathcal{F}$ with respect to the absolute value* $|\cdot|_\nu$ as $H_\nu(\mathcal{F}) := \max\{|a|_\nu : a \in \mathcal{F}\}$. We define for archimedean absolute values the *weight of P with respect to the absolute value* $|\cdot|_\nu$ as the sum of the absolute values of the coefficients of P, i.e. for a polynomial $P \in R[X_1, \ldots, X_n]$ as $wt_\nu(P) := \sum_{|\mu| \le d} |P_\mu|_\nu$. Let us remark that $wt_\nu(P) = wt(\sigma_\nu(P))$ holds. Finally, for all absolute values $\nu \in M_K$, we define the *logarithmic height with respect to the absolute value* $|\cdot|_\nu$ as $ht_\nu(\mathcal{F}) := \log H_\nu(\mathcal{F})$ and $ht_\nu(P) := \log H_\nu(P)$.

2.1.3 Mahler measure of multivariate polynomials

In the context of transcendental number theory, P. Philippon used the Mahler measure to derive a notion of height for projective varieties in [64], which in the simplest case coincides with the logarithmic absolute height of the point described. Later on, the author observed "*le parallélisme qui existe entre cette hauteur et le degré des variétés projectives*" and showed this by establishing an arithmetic Bézout inequality in [66].

This remark, together with the discussion of possible alternative definitions for the height of a projective variety (which were shown to be equivalent in a precise sense, see [66, Par.1]) gave rise to our

hope, that a similar behaviour would certainly hold for a (suitably defined) version of height for affine algebraic varieties and the geometric degree as defined in [34] (see Section 3.3 on page 25).

The Mahler measure of multivariate polynomials was used in [64] and more recently in [66], [67], [68]. We begin in this Subsection with the introduction of the Mahler measure for multivariate polynomials to discuss different possible notions of height in the following Subsection 2.1.4.

When dealing with complex polynomials, i.e. when P is seen as element of $\mathbb{C}[X_1, \ldots, X_n]$, an interesting metric measure is available : the Mahler measure $M(P)$ of the polynomial P. $M(P)$ is defined as zero for the zero polynomial $P = 0$ and for non–zero polynomials as :

$$M(P) := exp\left(\int_0^1 \cdots \int_0^1 \log \mid P(e^{2\pi i t_1}, \ldots, e^{2\pi i t_n}) \mid dt_1 \cdots dt_n\right).$$

Sometimes we prefer to use the logarithmic Mahler measure which is obviously given as $m(P) := \log M(P)$, where log is the natural logarithm. In [51], the author used precisely this notion for univariate polynomials under the form :

$$M(P) := \mid a_0 \mid \prod_{i=1}^{d} \max\{1, \mid \alpha_i \mid\},$$

where P is a univariate complex polynomial verifying $P = a_0 \prod_{i=1}^{d}(X_1 - \alpha_i)$. Let us recall that the link between these two versions of the same invariant is Jensen's Formula [50, p.60]. The Mahler measure is closely related to the standard weight wt of the corresponding complex polynomial. In [64] it was observed that for every complex polynomial $P \in \mathbb{C}[X_1, \ldots, X_n]$ the following inequalities hold :

$$m(P) \leq \log wt(P) \leq m(P) + d \log(n+1). \tag{9}$$

A short resumé of the main relations between Mahler measure and degree / number of variables of the polynomial can be found in [50, pp. 59–62]. We will make use of a particular feature of the Mahler measure M, the fact that it is a multiplicative function. This means that $M(PQ) = M(P) \cdot M(Q)$ holds. This multiplicative character is quite relevant for arithmetic Bézout inequalities (as in [66], [67] and [68]) and we shall use this in Subsection 2.3 to estimate the height of polynomials given by straight–line programs.

However, the behaviour of the Mahler measure with respect to additions of polynomials is not as comfortable (cf. [64]) :

$$m(P+Q) \leq m(P) + m(Q) + (\deg(P) + \deg(Q)) \log(n+1).$$

On the other hand, the standard weight is very well suited when dealing with the addition of polynomials : it verifies the triangular inequality $wt(P+Q) \leq wt(P) + wt(Q)$, but it is not as comfortable for products of polynomials. In the sequel we shall profit from the features of each measure (and their relation).

With the same notations as before, we define for archimedean absolute values $|\cdot|_\nu$ and polynomials $P \in R[X_1, \ldots, X_n]$ the *Mahler measure of P with respect to ν* as :

$$M_\nu(P) := M(\sigma_\nu(P)) \text{ and } m_\nu(P) := m(\sigma_\nu(P)).$$

Of course, this Mahler measure inherits all properties of the usual Mahler measure $m(P)$ for complex polynomials through the embedding σ_ν.

2.1.4 Different notions of height

The measures we have chosen for the estimation of degrees and heights in our complexity study have a double aspect : geometric and diophantine. The geometric aspect refers to properties coming from

algebraic geometry. Typically we may consider degrees of polynomials, number of monomials or the cardinality of zero–dimensional solution sets given by systems of multivariate polynomial equations. The diophantine aspect is more concerned with metric properties of the polynomials and the solution sets.

Our idea here for obtaining improved bounds for the arithmetic Nullstellensatz is based on estimations of the metric properties of the straight–line programs appearing in the concepts developed in [29], [43], [44], [28], [25], [30] and [60].

Both Nesterenko and Philippon considered in their works the Chow form or elimination polynomial for the introduction of a notion of height for equi-dimensional varieties. Furthermore, Philippon used the Mahler measure for the definition of an invariant height for projective varieties over the algebraic closure of $\mathbb{Q}$ by considering local height functions on the Chow form of the variety.

For the estimations of π_S or P_S it is sufficient to work with a rather simple notion of height, but this is not the case for the arithmetic Nullstellensatz. We will compare the pairs of (suitably defined) *invariant height*, *archimedean height* and *elimination polynomial* and *geometric solution*.

To give precise definitions of what we are going to use, we start with the standard definition for the height of a projective point (cf. [50]).

Given a projective point $\underline{a} := (a_0 : a_1 : \ldots : a_N) \in \mathbb{P}^N(K)$ with coordinates in the number field K, we define the *height of a projective point* $\underline{a}$ as :

$$H(\underline{a}) := (\prod_{\nu \in M_K} \max\{\mid a_i \mid_\nu : 0 \leq i \leq N\}^{n_\nu})^{\frac{1}{[K:\mathbb{Q}]}},$$

which does not depend on the number field K under consideration. Given a finite set $\mathcal{F} := \{b_i : 0 \leq i \leq N\} \subseteq K$, we can associate a projective point in $\mathbb{P}^{N+1}(K)$ at a finite distance :

$$\mathcal{F}_1 := (1 : b_0 : b_1 : \ldots : b_N) \in \mathbb{P}^{N+1}(K).$$

Looking at the height of this projective point yields a notion of height of the finite set $\mathcal{F}$, namely H_1.

$$H_1(\mathcal{F}) := H(\mathcal{F}_1) = (\prod_{\nu \in M_K} \max\{1, \mid b_i \mid_\nu : 0 \leq i \leq N\}^{n_\nu})^{\frac{1}{[K:\mathbb{Q}]}}.$$

Let us observe that if the finite set $\mathcal{F}$ consists of just one point $\mathcal{F} = \{\alpha\} \in K$, the height $H_1(\mathcal{F})$ gives the usual notion of height of the algebraic number $\alpha \in K$. Observe that the consequence of embedding $\mathcal{F}$ as a projective point at a finite distance has strong consequences for the derived height H_1, when $\mathcal{F}$ is contained in the ring of algebraic integers of K. In this case, only the archimedean absolute values contribute to the height and the following holds :

$$H_1(\mathcal{F}) = (\prod_{\nu \in S} \max\{1, \mid b_i \mid_\nu : 0 \leq i \leq N\}^{n_\nu})^{\frac{1}{[K:\mathbb{Q}]}}.$$

Using the height H_1 as introduced above, we can derive the following notion of logarithmic height for a finite set $\mathcal{F}$:

$$\text{the } \textit{logarithmic height } ht(\mathcal{F}) := \log H_1(\mathcal{F}).$$

As our main concern are metric estimates for multivariate polynomials $P \in R[X_1, \ldots, X_n]$, and since we do not have to relate the obtained estimates with any particular coefficient of the polynomial, we can identify the polynomial P with the finite set $\mathcal{F}$ of cardinality N of its coefficients b_i. This will do for us using any arbitrary enumeration of the coefficients.

Now, we place the point obtained from the coefficients of P at finite distance as before, and obtain a definition for the *height of the polynomial* P denoted by $H_1(P)$ as :

$$H_1(P) \quad := \quad (\prod_{\nu \in M_K} \max\{1, \mid b_i \mid_\nu : 0 \leq i \leq N\}^{n_\nu})^{\frac{1}{[K:\mathbb{Q}]}}$$

$$= \quad (\prod_{\nu \in S} \max\{1, |\, b_i \,|_\nu : 0 \leq i \leq N\}^{n_\nu})^{\frac{1}{[K:\mathbb{Q}]}}.$$

Similarly, we define the *logarithmic height of the polynomial* P as : $ht(P) := \log H_1(P)$. Observe that the logarithmic height ht defined above is non–negative. As in [64] and [66] we introduce the Mahler measure instead of archimedean absolute values to define the *invariant logarithmic height of a polynomial* P as :

$$\widetilde{ht}(P) := \frac{1}{[K:\mathbb{Q}]}(\sum_{\nu \in S} n_\nu m_\nu(P) + \sum_{\nu \in M_K \setminus S} n_\nu ht_\nu(P)).$$

Because of Weil's product formula (7) we easily conclude that $\widetilde{ht}$ is invariant under scalar multiplication by algebraic numbers i.e. for non–zero α in R and non–zero polynomials P in $R[X_1, \ldots, X_n]$ holds $\widetilde{ht}(\alpha P) = \widetilde{ht}(P)$. Just as the previously defined height ht, this new measure $\widetilde{ht}$ is also non–negative. From the proof of [64, Proposition 1.12]. we obtain the following result :

For every non–zero polynomial $P \in \mathbb{C}[X_1, \ldots, X_n]$ of degree d, there exists $\mu \in \mathbb{N}^{\mathrm{n}}, |\, \mu \,| \leq \mathrm{d}$, such that the coefficient P_μ of $\underline{X}^\mu$ is non–zero and for all archimedean absolute values $|\cdot|_\nu$ holds :

$$m_\nu(P) \geq \log |\, P_\mu \,|_\nu.$$

Since this inequality also holds for non–archimedean absolute values, we conclude :

$$\begin{aligned} \widetilde{ht}(P) &= \frac{1}{[K:\mathbb{Q}]} \sum_{\nu \in S} n_\nu m_\nu(P) + \sum_{\nu \in M_K \setminus S} n_\nu ht_\nu(P) \\ &\geq \frac{1}{[K:\mathbb{Q}]} \sum_{\nu \in M_K} n_\nu \log |\, P_\mu \,|_\nu = 0. \end{aligned}$$

Using the relation between the Mahler measure and the weight for archimedean absolute values we obtain for every polynomial $P \in R[X_1, \ldots, X_n]$ of degree at most D the estimation :

$$\widetilde{ht}(P) \leq \log \binom{D+n}{n} + ht(P).$$

Philippon's notion of invariant height $\widetilde{ht}$ as defined above has been chosen because of the good behaviour of the Mahler measure in terms of multiplication of polynomials. This has been illustrated by a Bézout equality in [66], [67], [68].

Observe that using the above definition of invariant height $\widetilde{ht}$, for any two multivariate polynomials $f, g \in R[X_1, \ldots, X_n]$ holds $\widetilde{ht}(fg) = \widetilde{ht}(f) + \widetilde{ht}(g)$. This property will be useful to relate the height of a variety to the height of its irreducible components in a very natural form.

One might argue that the behaviour of Philippon's invariant height $\widetilde{ht}$ with respect to other arithmetic operations with polynomials (such as additions) is more difficult to analyze. However, this drawback is less relevant since the height depends essentially on the non–scalar arithmetic operations (as remarked in [44]). The problem appearing when dealing with additions can be overcome using the good relations between the Mahler measure and the weight, whose behaviour with respect to additions is excellent. This is the reason why in our demonstrations the weight appears as a technical tool in the estimations.

Remark For the statements of our results we shall mainly work with $ht(P)$ and $\widetilde{ht}(P)$, the remaining notation will be used only in the proofs. Let us also observe that all our statements concerning $\widetilde{ht}(P)$ will equally hold using any reasonably defined notion of invariant logarithmic height (as for example found in [50]). The same applies to the following invariant weight $\widetilde{wt}$:

$$\widetilde{wt}(P) := \frac{1}{[K:\mathbb{Q}]}(\sum_{\nu \in S} n_\nu \log wt_\nu(P) + \sum_{\nu \in M_K \setminus S} n_\nu ht_\nu(P)).$$

We shall need the relations between the Mahler measure of a polynomial and the Mahler measure of its coefficients with respect to some distinguished variable. These relations can be resumed in the following Lemma :

Lemma 11 *Let $P \in R[X_1, \ldots, X_n][T]$ be a polynomial of total degree N and degree D with respect to the variable T. Let us assume that P has the following form :*

$$P := a_D T^D + a_{D-1} T^{D-1} + \cdots + a_0$$

where $a_i \in R[X_1, \ldots, X_n]$, for $0 \leq i \leq D$ and $a_D \neq 0$. Then the following estimates hold :

i) For every absolute value $|\cdot|_\nu$,

$$ht_\nu(a_i) \leq ht_\nu(P) = \max\{ht_\nu(a_i) : 0 \leq i \leq D\},$$

$$wt_\nu(a_i) \leq wt_\nu(P) = \sum_{i=0}^{D} wt_\nu(a_i).$$

ii) For every archimedean absolute value $|\cdot|_\nu$, we have the following relations between the Mahler measure of P and the Mahler measure of its coefficients :

$$m_\nu(a_i) \leq m_\nu(P) + \log \binom{D}{i} \leq m_\nu(P) + D \log D,$$

$$m_\nu(P) \leq N \log(n+1) + \sum_{i=0}^{D} m_\nu(a_i).$$

Proof.– Property *i)* follows immediately. The first inequality of ii) is a consequence of [64, Lemme 1.13]. The second inequality follows since the Mahler measure is bounded by the weight :

$$M_\nu(P) \leq wt_\nu(P) = \sum_{i=0}^{D} wt_\nu(a_i) \leq \sum_{i=0}^{D} M_\nu(a_i)(1+n)^{\deg(a_i)}.$$

As a consequence, we obtain the following Corollary :

Corollary 12 (Coefficients) *With the same notations and assumptions, we have :*

i) $ht(a_i) \leq ht(P) = \max\{ht(a_i) : 0 \leq i \leq D\}$

ii) $\widetilde{ht}(a_i) \leq \widetilde{ht}(P) + D \log D$

iii) $\widetilde{ht}(P) \leq N \log(n+1) + (D+1) + \sum_{i=0}^{D} \widetilde{ht}(a_i)$

2.2 Non–scalar straight–line programs

In the sequel we will work with the complexity model of non–scalar straight–line programs (see for instance [35], [80], [63], [59] or [44]) : a non–scalar straight–line program is a structure which evaluates (and hence represents) a given polynomial of $R[X_1, \ldots, X_n]$, taking R–linear operations for free.

Remark : We shall tacitly assume that our straight–line program does not contain any division.

We represent a straight–line program for the evaluation of a polynomial $P \in R[X_1, \ldots, X_n]$ by a *directed acyclic graph* $\mathcal{G}$ whose nodes are labelled gates which perform arithmetical operations. Therefore we identify the nodes of $\mathcal{G}$ with the corresponding gates. The graph $\mathcal{G}$ disposes of $n+1$ particular nodes labelled by the variables $X_1, \ldots, X_n$ and the constant 1. These nodes are called the input gates

of $\mathcal{G}$. We define the depth of a gate ν of our graph as the length of the longest path which joins ν with some input gate. Let us denote the gates of the directed acyclic graph 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 to the set of gates of depth i (this notation for the analysis of parallel complexity has been inspired by [58] and [57]).

Definition 13 (Non-scalar straight–line program) *A* division-free non–scalar straight–line program *with inputs $X_1,\ldots,X_n$ is a pair $\Gamma := (\mathcal{G},Q)$, where $\mathcal{G}$ is a directed acyclic graph, with $n+1$ input gates, unbounded fan–in, and Q is a function that assigns to every gate (i,j) one of the following instructions :*

$$i=0 : Q_{0,1} := 1\ ,\ Q_{0,2} := X_1\ ,\ \ldots\ ,\ Q_{0,n+1} := X_n$$

$$1 \leq i \leq \ell : Q_{i,j} := \Big(\sum_{\substack{r\leq i-1\\ 1\leq s\leq L_r}} A_{i,j}^{r,s}\, Q_{r,s}\Big)\cdot\Big(\sum_{\substack{r'\leq i-1\\ 1\leq s'\leq L_{r'}}} B_{i,j}^{r',s'}\, Q_{r',s'}\Big)$$

Here, $A_{i,j}^{r,s}$ and $B_{i,j}^{r',s'}$ are indeterminates called the parameters *introduced in Γ. The* non–scalar size of the straight–line program *Γ is $L(\Gamma) = L_0+\ldots+L_\ell$ (where $L_0 := n+1$) and its* non–scalar depth *$\ell(\Gamma)=\ell$ (these notions coincide with the notions of size and depth of the underlying computation graph).*

Observe that the rather complicated notation in Definition 13 (non–scalar straight–line program) arises from the fact that a single non–scalar node in the graph represents the total of all scalar (i.e. R–linear) operations contributing to this node.

Let us mention that in our notation the sub–indices i,j of the parameters $A_{i,j}^{r,s}$ and $B_{i,j}^{r',s'}$ represent the gate of the multiplication they are assigned to and the super–indices r,s correspond to the previous result they involve in the multiplication. We abbreviate $\underline{A} = (A_{i,j}^{r,s})$ and $\underline{B} = (B_{i,j}^{r',s'})$. Semantically speaking the straight–line program Γ defines an evaluation algorithm of the polynomials (intermediate results) :

$$Q_{i,j} = \sum_{|\,\mu\,|\leq 2^i} Q_{i,j}^{\mu}(\underline{A},\underline{B})\, X_1^{\mu_1}\ldots X_n^{\mu_n}. \tag{10}$$

Here, each coefficient $Q_{i,j}^{\mu}(\underline{A},\underline{B})$ belongs to the polynomial ring $\mathbb{Z}[\underline{A},\underline{B}]$. The result $Q_{i,j}$ has degree at most 2^i with respect to the variables $X_1,\ldots,X_n$.

We obtain a *non–scalar straight–line program over a ring R* by *specialisation* of the non–scalar straight–line program Γ, substituting the parameter lists $\underline{A}$ and $\underline{B}$ by elements of the ring R $\underline{\alpha} = (\alpha_{i,j}^{r,s})$ and $\underline{\beta} = (\beta_{i,j}^{r',s'})$ (we insist on the fact that $\alpha_{i,j}^{r,s}, \beta_{i,j}^{r',s'}$ belong to R).

A specialisation$\underline{A}\to\underline{\alpha}$, $\underline{B}\to\underline{\beta}$ of the parameters of Γ induces a straight–line program (computation) in $R[X_1,\ldots,X_n]$ in the most obvious way. The intermediate results of this specialized straight–line program γ are the polynomials of the form $Q_{i,j}(\underline{\alpha},\underline{\beta},X_1,\ldots,X_n)$. In this sense we shall say that a given polynomial $P\in R[X_1,\ldots,X_n]$ is evaluable, or computable, by (a specialisation of) the straight–line program Γ if there exists a specialisation $\underline{A}\longrightarrow\underline{\alpha}$, $\underline{B}\longrightarrow\underline{\beta}$ of the parameters of Γ such that for some gate (i,j) the following equality holds :

$$P(X_1,\ldots,X_n) = Q_{i,j}(\underline{\alpha},\underline{\beta},X_1,\ldots,X_n). \tag{11}$$

Taking into account the representation of (10) we can rewrite Identity (11) as :

$$P^{\mu} = Q_{i,j}^{\mu}(\underline{\alpha},\underline{\beta})$$

for all μ with $|\,\mu\,|\leq 2^i$ and $P^{\mu}=0$ for $|\,\mu\,|>2^i$. Let us remark that the *degree of such a polynomial $P = Q_{i,j}(\underline{\alpha},\underline{\beta},X_1,\ldots,X_n)$* is generically equal to 2^i in the space of parameters.

Finally, $P \in R[X_1, \ldots, X_n]$ is computable by a straight–line program Γ with parameters in the finite set $\mathcal{F} := \{\alpha_{ij}^{rs}, \beta_{ij}^{r's'}\}$.

2.3 Evaluation and height: Some useful bounds

In this Section we resume how the notions of straight–line program (Subsection 2.2) and height (Subsection 2.1.4) relate, establishing bounds for polynomials given by straight–line programs using the different notions of height.

First of all, we can easily bound the number of parameters used by a non–scalar straight–line program Γ of size L in n variables by $2L(L-(n+1))$. We can also bound the degrees of the polynomials $Q_{i,j}^{\mu}$ (of Formula (10)) as elements in $\mathbb{Z}[\underline{A}, \underline{B}]$:

Lemma 14 ([44]) *Given a non–scalar straight–line program Γ, the degree of all polynomials $Q_{i,j}^{\mu} \in \mathbb{Z}[\underline{A}, \underline{B}]$ is $2^{i+1}-2$ (independently from μ and j).*

Lemma 15 ([44]) *Let Γ be a non–scalar straight–line program over R of size L, non–scalar depth ℓ and parameters in a finite set $\mathcal{F} \subseteq R$ that evaluates a polynomial $P \in R[X_1, \ldots, X_n]$.*

i) For $\nu \in S$ holds $\max\{m_\nu(P), ht_\nu(P)\} \leq \log wt_\nu(P) \leq (2^{\ell+1}-2)[\log L + ht_\nu(\mathcal{F})]$.

ii) For $\nu \notin S$ holds $ht_\nu(P) \leq \log wt_\nu(P) \leq (2^{\ell+1}-2)ht_\nu(\mathcal{F})$.

iii) As estimates for the two notions of logarithmic height introduced on page 13 we have :

$$ht(P) \leq (2^{\ell+1}-2)(\log L + ht(\mathcal{F})) \text{ and } \widetilde{ht}(P) \leq (2^{\ell+1}-2)(\log L + ht(\mathcal{F})).$$

Proof.– Claims *i)* and *ii)* follow as in [44, Proposition 15]. As for claim *iii)* we have for the logarithmic height ht :

$$\begin{aligned} ht(P) &= \frac{1}{[K:\mathbb{Q}]}\Big(\sum_{\nu\in S} n_\nu \max\{0, ht_\nu(P)\} + \sum_{\nu\in M_K\setminus S} n_\nu \max\{0, ht_\nu(P)\}\Big) \\ &\leq \frac{1}{[K:\mathbb{Q}]}\Big(\sum_{\nu\in S} n_\nu (2^{\ell+1}-2)(\log L + \max\{0, ht_\nu(\mathcal{F})\}) \\ &\quad + \sum_{\nu\in M_K\setminus S} n_\nu (2^{\ell+1}-2)\max\{0, ht_\nu(\mathcal{F})\}\Big). \end{aligned}$$

Since Identity (8) holds, we conclude :

$$\begin{aligned} ht(P) &\leq (2^{\ell+1}-2)\log L + \frac{(2^{\ell+1}-2)}{[K:\mathbb{Q}]}\Big(\sum_{\nu\in M_K} n_\nu \max\{0, ht_\nu(\mathcal{F})\}\Big) \\ &= (2^{\ell+1}-2)\log L + (2^{\ell+1}-2)ht(\mathcal{F}). \end{aligned}$$

On the other hand, for the invariant logarithmic height $\widetilde{ht}$ holds :

$$\begin{aligned} \widetilde{ht}(P) &= \frac{1}{[K:\mathbb{Q}]}\sum_{\nu\in S} n_\nu m_\nu(P) + \sum_{\nu\in M_K\setminus S} n_\nu ht_\nu(P) \\ &\leq \frac{1}{[K:\mathbb{Q}]}\sum_{\nu\in M_K} n_\nu \log wt_\nu(P) \\ &\leq \frac{1}{[K:\mathbb{Q}]}\Big(\sum_{\nu\in S} n_\nu (2^{\ell+1}-2)(\log L + ht_\nu(\mathcal{F})) \\ &\quad + \sum_{\nu\in M_K\setminus S} n_\nu (2^{\ell+1}-2)ht_\nu(\mathcal{F})\Big). \end{aligned}$$

Again by Identity (8), we have :

$$\begin{aligned}\widetilde{ht}(P) &\leq (2^{\ell+1}-2)\log L \\ &\quad + \frac{(2^{\ell+1}-2)}{[K:\mathbb{Q}]}\Big(\sum_{\nu\in S} n_\nu ht_\nu(\mathcal{F}) + \sum_{\nu\in M_K\setminus S} n_\nu ht_\nu(\mathcal{F})\Big) \\ &= (2^{\ell+1}-2)\log L + (2^{\ell+1}-2)ht(\mathcal{F}).\end{aligned}$$

■

Lemma 16 ([44], Proposition 15) *Given an integer $a \in \mathbb{Z}$ by a division-free straight–line program of size L, non–scalar depth ℓ and parameters in a finite set $\mathcal{F} \subseteq \mathbb{Z}$ of bounded height H, the height of a can be bounded as :*

$$|\, a \,| \leq (LH)^{(2^{\ell+1}-2)}.$$

Lemma 17 (Composition) *Let $g_1, \ldots, g_m$ be polynomials in $R[X_1, \ldots, X_n]$ of degree at most D. Let $f \in R[Y_1, \ldots, Y_m]$ be a polynomial evaluable by a non–scalar straight–line program Γ of size L, non–scalar depth ℓ and parameters in a finite subset $\mathcal{F} \subseteq R$. Let $G \in R[X_1, \ldots, X_n]$ be the polynomial given by the composition of f with $g_1, \ldots, g_m$, i.e. the polynomial given by :*

$$G := f(g_1, \ldots, g_m) \in R[X_1, \ldots, X_n].$$

Then,

i) for every non–archimedean absolute value $|\cdot|_\nu$ we have

$$ht_\nu(G) \leq 2^\ell \max_{1\leq i\leq m}\{ht_\nu(g_i)\} + (2^{\ell+1}-2)ht_\nu(\mathcal{F}),$$

ii) for every archimedean absolute value $|\cdot|_\nu$ we have

$$\begin{aligned}m_\nu(G) &\leq \log wt_\nu(G) \\ &\leq 2^\ell \max_{1\leq i\leq m}\{\log wt_\nu(g_i)\} + (2^{\ell+1}-2)\cdot(\log L + ht_\nu(\mathcal{F})) \\ &\leq D2^\ell(n+1) + (2^{\ell+1}-2)\cdot(\log L + ht_\nu(\mathcal{F})) \\ &\quad + 2^\ell \max_{1\leq i\leq m}\{m_\nu(g_i)\}.\end{aligned}$$

iii) As for the height with respect to an archimedean absolute value $|\cdot|_\nu$ we have :

$$\begin{aligned}ht_\nu(G) &\leq \log wt_\nu(G) \\ &\leq (n+1)2^\ell \log D + (2^{\ell+1}-2)(\log L + ht_\nu(\mathcal{F})) \\ &\quad + 2^\ell \max_{1\leq i\leq m}\{ht_\nu(g_i)\}.\end{aligned}$$

Moreover, if D is an upper bound for the degrees of the polynomials $g_1, \ldots, g_m$, we have :

$$m_\nu(G) \leq 2^\ell \max_{1\leq i\leq m}\{m_\nu(g_i)\} + (2^{\ell+1}-2)(m_\nu(\mathcal{F}) + \log L) + D\log(1+n).$$

Proof.– Consider the following estimates :

i) If $|\cdot|_\nu$ is non–archimedean,

$$\deg(f) \max_{1\leq i\leq m}\{ht_\nu(g_i)\} + ht_\nu(f) \leq 2^\ell \max_{1\leq i\leq m}\{ht_\nu(g_i)\} + (2^{\ell+1}-2)ht_\nu(\mathcal{F}).$$

ii) If $|\cdot|_\nu$ is archimedean we have :

$$m_\nu(G) \leq \log wt_\nu(G), \qquad \log wt_\nu(G) \leq (2^{\ell+1}-2)(\log L + ht_\nu(\mathcal{F})),$$

and, finally $\log wt_\nu(G) \leq \deg(f) \max_{1\leq i\leq m}\{\log wt_\nu(g_i)\} + \log wt_\nu(f)$. The third inequality follows since $\log wt_\nu(g_i) \leq D\log(n+1) + m_\nu(g_i)$.

iii) We apply the same upper bounds as in ii), noting that $ht_\nu(G) \leq \log wt_\nu(G)$ and $\log wt_\nu(g_i) \leq (n+1)\log D + ht_\nu(g_i)$. ∎

Corollary 18 (Composition) *With the same notation as in the previous Lemma we conclude :*

i) $ht(G) \leq (n+1)2^\ell \log D + (2^{\ell+1}-2)(\log L + ht(\mathcal{F})) + 2^\ell \max_{1\leq i\leq m}\{ht(g_i)\}$,

ii) $\widetilde{ht}(G) \leq D2^\ell \log(n+1) + (2^{\ell+1}-2)(\log L + ht(\mathcal{F})) + 2^\ell \max_{1\leq i\leq m}\{\widetilde{ht}(g_i)\}$.

Proof.– We make use of the well-known fact that $\frac{1}{[K:\mathbb{Q}]}\sum_{\nu\in S} n_\nu = 1$. Then, the quantities $(n+1)2^\ell \log D$ and $(2^{\ell+1}-2)\log L$ (or $D2^\ell \log(n+1)$ and $(2^{\ell+1}-2)\log L$) follow from the bounds in the previous Lemma 17. ∎

2.4 Non-scalar straight-line programs : Technical lemmata

The height estimates for the arithmetic Nullstellensatz announced in Section 1 are based on a detailed analysis of the algorithm for geometric solving of multivariate polynomial equation systems defining affine algebraic varieties as developped in [29], [43], [28], [25], [30] and [60].

The height estimates are obtained by bounding appropriately the height of all elements appearing in a "geometric solution" produced by the afore mentioned eliminiation algorithm (see Section 3.4 for a discussion of this approach).

This involves neccessarily the height analysis of the algorithmic ingredients given in terms of straight–line programs, using the notions of height defined in Subsection 2.1.4. Therefore we resume here briefly some of the results obtained in [29], [43], [28], [25], [30] and [60] for the straight–line program complexity of the subalgorithms involved.

The elimination algorithm as developped in [25] has been analyzed and described in detail in [60], which should be considered as a primary reference for the proofs of the following statements.

Let us recall the notation : R is the ring of algebraic integers of a number field K and $\mathbb{K}$ an algebraic closure of K. We denote by A the ring $K[X_1,\ldots,X_r]$ and by F the quotient field $K(X_1,\ldots,X_r)$ of A.
Due to the iterative character of our algorithms and the fact that we distinguish between free and dependent variables, we want to state the technical lemmata in a more general form. To facilitate the notation, the ring A will include the free variables and the dependent variables are explicitly named.

Berkowitz's algorithm One of the central tasks appearing naturally in elimination algorithms when computing with polynomials, is the *efficient* computation of the determinant and characteristic polynomial of a matrix over a polynomial ring. The classical Gaussian elimination algorithm computes a solution using $O(N^3)$ arithmetic operations. Even though this appears already satisfactory, this approach has two drawbacks : first of all the algorithm uses divisions, which makes it unsuitable for computations over an arbitrary domain, and second, it has an intrinsically sequential character, thus preventing further improvements through parallelism.

These aspects were treated in [20], giving a first parallel algorithm, with restrictions on the characteristic of the ground field though. These restrictions were removed in a very complicated way in [11], and finally, [18] and [8] give practicable algorithms for the computation of the determinant as well as the remaining coefficients of the characteristic polynomial of a matrix over an arbitrary domain.

The next Proposition describes the non–scalar complexity bounds resulting from the analysis made in [44] using the algorithm given in [8].

Proposition 19 ([8], [44]) *Let A be a ring. There exists a non–scalar straight–line program of size $O(n^5)$, non–scalar depth $2\log_2 n + 7$ and parameters in $\{-1, 0, 1\}$ which computes from the entries of every matrix $M \in \mathcal{M}_n(A)$ the coefficients of its characteristic polynomial and, in particular, its determinant $det(M)$.*

Vermeidung von Divisionen The technique of computing the homogeneous components of a polynomial together with the use of the formal power series expansion of a rational function are the main ingredients for the following algorithm due to V. Strassen and formulated for non–scalar straight–line programs in [44].

Proposition 20 ([79], [44]) *Let Γ be a non–scalar straight–line program of size L, non–scalar depth ℓ and parameters in a set $\mathcal{F} \subseteq R$ that computes $\{f_0, \ldots, f_m\} \subseteq R[X_1, \ldots, X_n]$. Assume that $f_0 \neq 0$ and that f_0 divides f_i in $R[X_1, \ldots, X_n]$ for all i, $1 \leq i \leq m$. Then there exists a non–scalar straight–line program Γ' verifying :*

i) Γ' computes polynomials $\{P_1, \ldots, P_m\}$ in $R[X_1, \ldots, X_n]$ and an integer $\theta \in R - \{0\}$ such that for $1 \leq i \leq m$ holds :

$$\theta^{-1} P_i = \frac{f_i}{f_0},$$

ii) Γ' has size of order $d^{O(1)}L$, where $d = \max \deg(f_i)$, non–scalar depth of order $O(\ell)$ and parameters in the set $\mathcal{F} \cup \{0, \ldots, L(d+1)^2\}$,

iii) the non–scalar depth of Γ' is of order $O(\ell)$.

Evaluation in a matrix Instead of considering only straight–line programs over a polynomial ring $R[X_1, \ldots, X_n]$, we will also make use of its flexible evaluation possibilities to compute results over a matrix ring in the following form :

Lemma 21 (Evaluation of a polynomial in matrices, [33])
Given algebraically independent variables $X_1, \ldots, X_n$ over the ring R, let $g \in R[X_1, \ldots, X_n]$ be a polynomial of degree d_1 with respect to the variables $X_{r+1}, \ldots, X_n$ which can be computed by a straight–line program Γ of size L, non–scalar depth ℓ and parameters in a finite subset $\mathcal{F} \subset R$. For a fixed t with $1 \leq t \leq n$ let A be the ring of polynomials with coefficients in R in the variables $X_1, \ldots, X_t$ (i.e. $A = R[X_1, \ldots, X_t]$). Let $M_{t+1}, \ldots, M_n$ be $N \times N$ matrices with entries in A such that $M_i \cdot M_j = M_j \cdot M_i$ for all i, j and let $\rho \in A$ be a non–zero polynomial. Then there exists a non–scalar straight–line program Γ' of size $(d_1 + 1)^2 N^{O(1)} L$ and non–scalar depth $O(\ell)$, such that using parameters in $\mathcal{F}$ and taking as inputs the polynomial ρ and the entries of the matrices $M_{t+1}, \ldots, M_n$, the straight–line program Γ' evaluates all the entries of a matrix $M_g \in \mathcal{M}_N(A)$ and a non–zero polynomial ρ_g such that

$$g(X_1, \ldots, X_t, \rho^{-1} M_{t+1}, \ldots, \rho^{-1} M_n) = \rho_g^{-1} M_g.$$

Moreover, if ρ is a unit in A, the straight–line program Γ' can be chosen of size $LN^{O(1)}$, non–scalar depth $\ell + O(1)$ and a similar parameter set as before.

Jacobian and pseudo—jacobian. The distinction of singular from non–singular points of a variety yields the condition of the "Jacobian" criterion ([47, Chapter VI, Theorem 1.15]) whose "straight–line program" version is presented here (and which will be used to check the condition of reduced regular sequence). Combining the formal rules of derivation with Proposition 19, one concludes :

Lemma 22 *Let $f_1, \ldots, f_n$ be a family of polynomials of $A[X_1, \ldots, X_n]$ evaluated by a straight–line program β of size L and non–scalar depth ℓ. Then there exists a straight–line program over A with inputs $X_1, \ldots, X_n$ 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 Section 4.2 we shall work with a specific polynomial called the *pseudo—jacobian determinant* of a given regular sequence. We now introduce this polynomial and say how it can be evaluated.

Notation 23 *Let $f_1, \ldots, f_n \in A[X_1, \ldots, X_n]$ be a regular sequence in $F[X_1, \ldots, X_n]$. Furthermore, let $Y_1, \ldots, Y_n$ be new variables. We write $Y = (Y_1, \ldots, Y_n)$. Fix $1 \leq j \leq n$. By $f_j^{(Y)} := f_j(Y_1, \ldots, Y_n)$ we denote the polynomial obtained from f_j substituting the variables $X_1, \ldots, X_n$ by $Y_1, \ldots, Y_n$. In the polynomial ring $A[Y_1, \ldots, Y_n, X_1, \ldots, X_n]$ we decompose the polynomial $f_j^{(Y)} - f_j$ in the following (non–unique) way :*

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

where $l_{k,j}$ are polynomials in $A[Y_1, \ldots, Y_n, X_1, \ldots, X_n]$. Let us consider the determinant Δ of the matrix $M = (l_{k,j})_{1 \leq k,j \leq n}$, namely $\Delta := \det(M)$. This determinant is called a pseudo–jacobian determinant *of the regular sequence of polynomials $f_1, \ldots, f_n$.*

Proposition 24 ([28], [60]) *If d is a bound for the degrees of $f_1, \ldots, f_n$ and these polynomials are given by a non–scalar straight–line program Γ of size L and non–scalar depth ℓ, then there exists a straight–line program Γ' 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 Γ' uses apart from the same parameters as Γ only parameters of $\mathbb{Z}$ in $\{0, \ldots, d^c\}$.*

2.5 The equivalence problem for straight–line programs

This Subsection deals with the zero–equivalence problem for multivariate polynomials given by straight–line programs. This subject was initiated in in the late seventies and early eighties by several authors (cf. e.g. [85], [72], [36], [38]).

The renewed interest in the subject is motivated by several recent advances in Symbolic and Numeric Solving (see for example [73], [74], [75], [29], [1], [25]).

We can state the problem in the following form :

Problem 1 (Zero–equivalence) *Let K be a number field. Given a division free straight–line program Γ that evaluates a polynomial $f \in K[X_1, \ldots, X_n]$ of degree at most d, decide whether $f \equiv 0$ or not.*

The simple-minded approach of computing the coefficients of the dense representation does not work. As observed in [53], deciding whether the $k-$th coefficient of the polynomial $(1 + X^{e_1}) \cdots (1 + X^{e_n})$ is zero or not includes the Knapsack problem and is hence at least NP–complete.
There are three main approaches to avoid these difficulties, all of them involving the following computational problem :

Problem 2 *Let K be a number field. Let Γ be a division free straight–line program that evaluates a polynomial $f \in K[X_1, \ldots, X_n]$ of degree at most d. If the polynomial f is not identically zero in $K[X_1, \ldots, X_n]$, compute a point $x \in K^n$ such that $f(x) \neq 0$.*

The method used to solve Problem 2 is the main difference between the following three approaches :

- Probabilistic zero–tests [72], [86]
- Correct test sequences [36], [43]
- Witness methods,

2.5.1 Correct test sequences

The approach based on a non–uniform complexity model using density arguments is used by J. Heintz and C. P. Schnorr in [36] to establish the existence of short correct test sequences.

Definition 25 *Given a set $\mathcal{F} \subset R[X_1, \ldots, X_n]$ (which contains the null polynomial) we say that a finite set of points $\mathcal{Q} \subset R^n$ is a* correct test sequence *for $\mathcal{F}$ iff for all $P \in \mathcal{F}$ the following holds :*

$$P \mid_{\mathcal{Q}} = 0 \Longrightarrow P \equiv 0 \ .$$

Let $\mathcal{W}(n, d, L)$ be the class of all polynomials in n variables with degree bounded by d which can be evaluated by a straight–line program of size L. The following Theorem taken from [36] states that the height of correct test sequences for $\mathcal{W}(n, d, L)$ is moderate.

Theorem 26 ([36]) *Let $L, d \in \mathbb{N}$ and let $u := 2L(d+1)^2$, $s := 6(L+n)(L+n+1)$. Then, the number of correct test sequences for $\mathcal{W}(d, n, \nu)$ in the set $\{1, \ldots, u\}^{ns}$ is at least $u^{ns}(1 - u^{-s/6})$.*

Let us define the set $W(n, L, \ell)$ of all polynomials in n variables over R which can be evaluated by a non–scalar straight–line program of size L and non–scalar depth ℓ. The following Proposition states the existence of a correct test sequence for $W(n, L, \ell)$ of small size and height.

Proposition 27 ([44]) *Given $n, L, \ell \in \mathbb{N}$ with $L \geq n+1$, let $u := (2^{\ell+1} - 2)\,(2^{\ell} + 1)^2$ and $t := 6\,(\ell L)^2$. 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 $\mathcal{W}(n, L, \ell)$ (therefore it contains at least one correct test sequence of this length).*

2.5.2 Witness Theorem

In [36] and more recently in [10] (cf. also [9]) the authors give deterministic methods for the solution of Problem 2. The common approach is based on the notion of *witness*.

Definition 28 ([10]) *Let K be an algebraic number field and $f \in K[X_1, \ldots, X_n]$. A* witness *for f is a point $w \in K^n$ such that holds :*

$$f(w) = 0 \Longrightarrow f = 0.$$

The result due to Heintz and Schnorr can be resumed as :

Theorem 29 ([36]) *Let $f \in \mathbb{Z}[X_1, \ldots, X_n]$ be a polynomial of degree bounded by d such that the weight of f is bounded by m. Then, the following point is a witness for f :*

$$w := ((2m), (2m)^{d+1}, \ldots, (2m)^{(d+1)^{n-1}}).$$

By a similar argument (due to Kronecker) as that of Theorem 29 above, but using Weil's height, we obtain the following statement :

Theorem 30 ([10]) *Let $f(X_1,\ldots,X_n) \in K[X_1,\ldots,X_n]$ be a polynomial that can be evaluated by a division free non–scalar straight–line program of size L with parameters in $\{x_1,\ldots,x_s\}$. Then a witness for f can be obtained as the sequence :*

$$(w_1, (w_1)^{2^{4nL^2+4L}}, \ldots, (w_1)^{2^{4nL^2+4L}(n-1)}),$$

where w_1 can be chosen in

$$\{2^{2^{4nL^2+4L}}, x_1^{2^{4nL^2+4L}}, \ldots, x_s^{2^{4nL^2+4L}}\}.$$

Observe that the proof is similar to that of [36], with the bounds for the weight written in terms of the size of the straight–line program. For more recent results in this direction refer to the book [10]. As a final remark we give the following Theorem, which improves on the height bounds established in Theorem 30 above by considering the parallel complexity measure of a straight–line program evaluating the polynomial.

Theorem 31 (Witness Theorem with parallel estimates, [16]) *Let f be a polynomial in $\mathbb{Z}[T_1,\ldots,T_r,X_1,\ldots,X_n]$ evaluable by a non–scalar straight–line program Γ of size L, non–scalar depth ℓ and parameters in $\{-1,0,1\}$. Let $x_1,\ldots,x_r \in K$ be some algebraic numbers, and $\omega_0 \in \{2,x_1,\ldots,x_r\}$ such that*

$$H_1(x_0) = \max\{2, H_1(x_1),\ldots,H_1(x_r)\}$$

Let $f \in K[X_1,\ldots,X_r]$ be the polynomial given by $f := F(x_1,\ldots,x_r,X_1,\ldots,X_r)$. Then, for $N \in \mathbb{N}$ such that

$$\log_2 N > \log_2(\ell+1) + (\ell+2)(\log_2\log_2 L + \max\{2,\log_2 r\})$$

the point $(\omega_1,\ldots,\omega_n) \in K^n$ given by :

$$\omega_1 = \omega_0^N, \qquad \omega_i = \omega_{i-1}^N \qquad \text{for } i = 2,\ldots,n$$

is a witness point for f.

3 Complete intersection varieties

In this Section we first recall how the degree and height of an ideal–theoretic complete intersection diophantine variety $V \subseteq \mathbb{K}^n$ are defined. The standard method (see e.g. [83, Chap.I.1.]) associates to V a birationally isomorphic hypersurface defined as a generic projection with respect to a Noether normalisation (see Subsection 3.2). The height and degree of the resulting hypersurface are then defined as height and degree of its defining polynomial. This polynomial, called *elimination polynomial* of V with respect to a given Noether normalisation, is closely related with the notion of *geometric solution* as introduced in [29], [44], [28], [25].

Recently we have discovered that a similar notion has already been considered by Kronecker in his work dedicated to Kummer [46]. These ideas have been discussed in [52] and [83]. Unfortunately, the developing elimination theory was not able to make good use of Kronecker's ideas. At that time, mathematicians thought that using Kronecker's representation would yield an excessive growth in the degrees and heights of the polynomials computed. This impression is wrong since we are in a situation similar to Gaussian elimination, where the "cleaning" of common denominators is crucial for the resulting complexity of the algorithm.

3.1 Notation

Let us recall the notation : R is the ring of algebraic integers of a number field K and $\mathbb{K}$ an algebraic closure of K. We denote by A the ring $K[X_1,\ldots,X_r]$ and by F the quotient field $K(X_1,\ldots,X_r)$

of A. An affine algebraic variety $V \subseteq \mathbb{K}^n$ is said to be R–definable, if there exist polynomials $f_1, \ldots, f_s \in R[X_1, \ldots, X_n]$ such that :

$$V := V(f_1, \ldots, f_s) = \{x \in \mathbb{K}^n : \mathrm{f_1(x)} = 0, \ldots, \mathrm{f_s(x)} = 0\}.$$

In the following we are going to consider only R–definable varieties. For such a variety $V \subseteq \mathbb{K}^n$ we denote by $I(V)$ the ideal in $K[X_1, \ldots, X_n]$ of all polynomials vanishing on V, i.e.

$$I(V) := \{f \in K[X_1, \ldots, X_n] \ : \ f(x) = 0, \forall x \in V\}.$$

We also denote by $K[V]$ the reduced residue ring (or coordinate ring of V) $K[V] := K[X_1, \ldots, X_n]/I(V)$ and recall that the ideal $I(V)$ is radical, i.e. $\sqrt{(f_1, \ldots, f_s)} = I(V)$ holds.

For polynomials $g \in K[X_1, \ldots, X_n]$ we denote by $\bar{g}$ the equivalence class defined by g in the residue ring $K[V]$. Let us denote by r the dimension of the R–definable variety V and by s the codimension of V (i.e. $s + r = n$).

One of the main technical difficulties of the algorithms for *geometric solving* of multivariate polynomial equation systems (as e.g. in [28], [25] and [60]) is possibly the very tight relation between geometric reasoning and algebraic language used.

We shall mainly use terminology and elementary facts that can be found in classical textbooks on commutative algebra, see for example [47, Chapter VI], [54, Chapters 5+6], [84, Appendix 6]).

3.2 Variables in Noether position

We denote by A the ring $K[X_1, \ldots, X_r]$ and by F the quotient field $K(X_1, \ldots, X_r)$ of A. Let $V \subseteq \mathbb{K}^n$ be an algebraic variety of dimension r and $I(V)$ its associated ideal. We say that the variables $X_1, \ldots, X_n$ are *in Noether position* with respect to V if the following is an integral ring extension :

$$K[X_1, \ldots, X_r] \hookrightarrow K[V].$$

The variables $X_1, \ldots, X_r$ are called the free variables (with respect to V) and $X_{r+1}, \ldots, X_n$ are called the dependent variables. Let us denote by $\mathcal{M}_n(K)$ the space of all $n \times n$ matrices with entries in K ($\mathcal{M}_n(K) \cong K^n$).

It is well–known that there exist generically many matrices $N \in \mathcal{M}_n(K)$ such that the linear change of coordinates given by the following relation :

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = N \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$$

puts the variables $Y_1, \ldots, Y_n$ in Noether position with respect to the variety V. Let $\mathcal{N}(V) \subseteq \mathcal{M}_n(K)$ be the set of all matrices which put the variables in Noether position with respect to V.

The "generically many" condition means that $\mathcal{N}(V)$ contains a non–empty Zariski-open subset. As for the practical consequences, refer to Section 5 for more details. In the sequel we are interested in the case of matrices with coordinates in a ring of algebraic integers. We denote by $\mathcal{N}_R(V)$ and $\mathcal{N}_{\mathbb{Z}}(V)$ the sets $\mathcal{N}(V) \cap R^{n \times n}$ and $\mathcal{N}(V) \cap \mathbb{Z}^{n \times n}$, respectively.

We say that an R–definable variety $V \subseteq \mathbb{K}^n$ of codimension s is an *ideal–theoretic complete intersection* if there exist polynomials $f_1, \ldots, f_s$ in $R[X_1, \ldots, X_n]$ such that $I(V) = (f_1, \ldots, f_s)$ holds in $K[X_1, \ldots, X_n]$.

Lemma 32 (Radical, [60]) *Let K be a field of characteristic 0 and $g_1, \ldots, g_t$ a regular sequence in $K[X_1, \ldots, X_n]$. Let us assume that the variables $X_1, \ldots, X_n$ are in Noether position with respect to the*

ideal $I = (g_1, \ldots, g_t)$, i.e. $A = K[X_1, \ldots, X_r] \hookrightarrow K[X_1, \ldots, X_n]/I = B$ is an integral ring extension, where $r + t = n$. Let $J(g_1, \ldots, g_t)$ be the determinant of the jacobian matrix given by

$$\left(\frac{\partial g_i}{\partial x_j}\right)_{1 \leq i \leq t, r+1 \leq j \leq n}.$$

Then, the ideal I is radical if and only if $\bar{J}(g_1, \ldots, g_t)$ is not a zero divisor in $K[X_1, \ldots, X_n]/(g_1, \ldots, g_t)$.

Proof.– [60, Proposition 27] ∎

An elementary inductive argument (based on Quillen–Suslin's Theorem proving Serre's conjecture, cf. [49], [47]) shows the following statement :

Let $V \subseteq \mathbb{K}^n$ be an ideal–theoretic complete intersection algebraic variety of dimension r. Let us assume that the variables $X_1, \ldots, X_n$ are in Noether position with respect to V. Then, $K[V]$ is a free $K[X_1, \ldots, X_r]$–module of finite rank. For a proof of this statement see [69], [4] or [31, Lemma 3.3.1].

3.3 Geometric degree

In [34] a notion of (geometric) degree for affine algebraic varieties is introduced. Alternative notions can be found in [24] and [82]. If V is an irreducible algebraic set of dimension r, the geometric degree of V is defined as the maximum number of points of the intersections of V with affine linear spaces of dimension $n - r$. For a general variety V the degree is defined as the sum of the degrees of its irreducible components. We denote by $\deg(V)$ the geometric degree of the affine algebraic variety $V \subseteq \mathbb{K}^n$.

A *Bézout Inequality* can be established for this notion of geometric degree, (cf. [34], [24], and [82]) i.e. given affine algebraic sets $V, W \subseteq \mathbb{K}^n$ we have :

$$\deg(V \cap W) \leq \deg(V) \deg(W).$$

This notion of geometric degree has an interesting translation in terms of Noether normalisations :

Let V be an ideal–theoretic complete intersection of dimension r, and $\mathcal{N}(V)$ the Zariski open subset of $\mathcal{M}_n(K)$ of all non–singular matrices which put the variables in Noether position with respect to V. For every matrix $N \in \mathcal{N}(V)$, let us denote by $rk_{A_N} K[V]$ the rank of $K[V]$ as free A_N–module, where

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = N \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$$

are the new variables and $A_N := K[Y_1, \ldots, Y_r]$ such that $A_N \hookrightarrow K[V]$ is an integral ring extension. The following equality may be seen in [34] :

$$\deg(V) = \max\{rk_{A_N} K[V] \ : \ N \in \mathcal{N}(V)\}.$$

As observed in [15, Proposition 1.11] the geometric degree of an affine algebraic variety agrees with the geometric degree of its projective closure without counting multiplicities.

However, one has to observe that the existing relations between equations and degree in projective geometry and commutative algebra cannot be directly translated to the affine case. For instance, let $X_0, X_1, \ldots, X_n$ be homogeneous coordinates and $g_1, \ldots, g_s \in K[X_0, X_1, \ldots, X_n]$ a regular sequence of homogeneous polynomials. The degree of the set of common zeroes of $g_1, \ldots, g_s$ defined by the Hilbert polynomial is exactly the product of the degrees $\deg(g_1) \cdots \deg(g_s)$.

This number is usually called the *Bézout number* of $g_1, \ldots, g_s$. This behaviour does not occur in the affine case. As a simple example, let us consider the regular sequence of affine polynomials given by :

$$g_1 = x_1^2 + x_1 + 1, g_2 = x_2 - x_1^2, \ldots, g_s = x_s - x_{s-1}^2.$$

The geometric degree of the affine variety $V(g_1, \ldots, g_s)$ is exactly 2, whereas the Bézout number is 2^s. As the geometric degree does not take into account neither components in the infinity hyperplane nor multiplicities, this yields a more "geometric" behaviour which is just what we are looking for, as illustrated by the example in Section 3.1.

3.4 Geometric Solving

In [63], [25] the notion of *geometric solving* was introduced to formalize a way of describing the ring $K[V]$, where V is an ideal–theoretic complete intersection variety of dimension r. Basically, this ring has two main properties. One is the free module character of $K[V]$ inherited from a Noether normalisation :

$$A := K[X_1, \ldots, X_r] \hookrightarrow K[V].$$

This can be easily described by means of a basis of $K[V]$ as a free module. The second property is the A–algebra character of $K[V]$. This means to describe the product operation in the ring $K[V]$. This is achieved by means of the following method :

For every $g \in K[X_1, \ldots, X_n]$ we identify the residual class $\bar{g}$ and the $K[X_1, \ldots, X_r]$–module endomorphism η_g defined by : $\eta_g : K[V] \longrightarrow K[V]$, where $\eta_g(f) := \bar{g}f$, for all $f \in K[V]$. Furthermore, for a fixed free module basis of $K[V]$, we can represent the endomorphism η_g by a matrix which we denote by M_g. If $g = X_i$ is a dependent variable, we denote $M_i := M_{X_i}$ for $r+1 \leq i \leq n$ and we call these matrices the *tensor matrices* of the algebra $K[V]$.

Let us observe that if $g \in K[X_1, \ldots, X_n]$ and a basis of $K[V]$ is fixed, the matrix M_g is given by the following formula :

$$M_g := g(X_1, \ldots, X_r, M_{r+1}, \ldots, M_n).$$

Thus, the ring $K[V]$ will be completely described by means of the following elements :

- the Noether normalisation, $K[X_1, \ldots, X_r] \hookrightarrow K[V]$,
- the basis of $K[V]$ as a free module, and
- the tensor matrices $M_{r+1}, \ldots, M_n$.

There exists a geometrical interpretation of the matrices M_g and, more precisely, the characteristic and minimal polynomials of M_g. Suppose that the variables are in Noether position with respect to $V \subseteq \mathbb{K}^n$ and that $g \in K[X_1, \ldots, X_n]$. Let us consider the regular morphism :

$$G : \mathbb{K}^n \longrightarrow \mathbb{K}^{r+1}, \mathrm{G}(\mathrm{X}_1, \ldots, \mathrm{X}_n) := (\mathrm{X}_1, \ldots, \mathrm{X}_r, \mathrm{g}(\mathrm{X}_1, \ldots, \mathrm{X}_n)).$$

We observe that (since the variables are in Noether position) the image of V under the action of this mapping G, $G(V) \subseteq \mathbb{K}^{r+1}$, is a hypersurface $\mathcal{H}_G \subseteq \mathbb{K}^{r+1}$.

Proposition 33 *With this notation, let $\chi_g, m_g \in A[T]$ be the characteristic and minimal polynomial of M_g, respectively. We have :*

i) $m_g = \frac{\chi_g}{\gcd(\chi_g, \chi_g')}$, *where χ_g' is the derivative of χ_g with respect to the variable T,*

ii) $V(\chi_g) = V(m_g) = \mathcal{H}_G$ *in* $\mathbb{K}^{r+1}$,

iii) $I(\mathcal{H}_G) = (m_g)$ *in* $K[X_1, \ldots, X_r, T]$,

iv) $\deg(\mathcal{H}_G) = \deg(m_g) \leq \deg(V) \cdot \deg(g)$,

v) $\deg_T m_g \leq \deg_T \chi_g = rk_{K[Y_1,\ldots,Y_r]}(K[V]) \leq \deg(V)$.

Up to now there is no method of admissible complexity known for the computation of a basis of $K[V]$ as free A–module. Recent progress in this sense may be seen in [2]. Thus, alternative descriptions of the algebra $K[V]$ have been introduced (cf. [46], [26], [27], [23], [43], [29], [28], [53], [60] and [25] for more details).

One of these alternative descriptions is the following one. Suppose, as before, that you have a Noether normalisation : $A := K[X_1, \ldots, X_r] \hookrightarrow K[V] =: B$. Let $F = K(X_1, \ldots, X_r)$ be the quotient field of A and B' the zero–dimensional F–algebra obtained by extending scalars to F, i.e. $B' = F \otimes_A B$.

For most elimination problems, a description of the F–algebra B' will be sufficient to proceed. Thus, a *geometric solution* of an ideal–theoretic complete intersection variety V consists of a Noether normalisation

$$A = K[X_1, \ldots, X_r] \hookrightarrow K[V] = B$$

together with a suitable description of B'.

We are going to show that the following two approaches for the description of ideal theoretic complete intersection affine algebraic varieties are equivalent : the description using the *elimination polynomial* or *Chow form* with respect to a given Noether normalisation (see for example [81] or the works [66], [67], [68]) and the description by a geometric solution (consider e.g. [46], [26], [27], [23], [44] and [25]). For an application of both approaches (even for arbitrary dimension) in the context of polynomial factorization see [17] and [32].

3.4.1 The elimination polynomial

This approach describes the algebra $K[V]$ by means of a generic projection in terms of the dependent variables. With the previous notation, let $U_{r+1}, \ldots, U_n$ be new indeterminates. Let us denote by R_u, A_u, F_u, B_u, B'_u respectively the rings obtained by extending scalars in the following form :

$$R_u := R[U_{r+1}, \ldots, U_n], \qquad A_u := A[U_{r+1}, \ldots, U_n],$$

$$F_u := F(U_{r+1}, \ldots, U_n), \qquad B_u := A_u \otimes_A B, \qquad B'_u := F_u \otimes_F B'.$$

We have that $A_u \hookrightarrow B_u$ is also an integral ring extension and B_u is also a free A_u–module. We also have

$$rk_{A_u} B_u = rk_A B, \qquad \dim_{F_u} B'_u = \dim_F B',$$

and the bases of B and B' extend respectively to bases of B_u and B'_u. Let $\mathcal{U}$ be the linear form given in terms of the dependent variables by $\mathcal{U} := U_{r+1}X_{r+1} + \cdots + U_nX_n$ and let us consider the endomorphism given by :

$$\eta_{\mathcal{U}} : \ B_u \longrightarrow B_u : \ \bar{g} \mapsto \bar{\mathcal{U}} \cdot \bar{g}.$$

Proposition 34 *The characteristic polynomial $\chi_{\mathcal{U}} \in A_u[T]$ of $\eta_{\mathcal{U}}$ agrees with its minimal polynomial $\mathfrak{m}_{\mathcal{U}} \in A_u[T]$. Both have degree equal to $rk_A B$ and B'_u is isomorphic to the F_u–algebra :*

$$F_u[T]/(\mathfrak{m}_{\mathcal{U}}(T)).$$

Since R is the ring of algebraic integers of the number field K, there exists a minimal non–zero integer number $C_{\mathcal{U}} \in \mathbb{Z} \setminus \{0\}$ such that $C_{\mathcal{U}} \cdot \mathfrak{m}_{\mathcal{U}} \in R[X_1, \ldots, X_r, U_{r+1}, \ldots, U_n][T]$ and this constant $C_{\mathcal{U}}$ is the coefficient of the highest degree term in T of the minimal polynomial $\mathfrak{m}_{\mathcal{U}}$. From now on we denote by $\mathfrak{m}_{\mathcal{U}}$ this polynomial $C_{\mathcal{U}} \cdot \mathfrak{m}_{\mathcal{U}}$ in $R[X_1, \ldots, X_r, U_{r+1}, \ldots, U_n][T]$. It has the form

$$\mathfrak{m}_{\mathcal{U}} = C_{\mathcal{U}} T^D + G(X_1, \ldots, X_r, U_{r+1}, \ldots, U_n, T)$$

where $\deg_T G \leq D - 1, D = rk_A K[V]$. It will be called the *elimination polynomial* of V with respect to the Noether Normalisation $A \hookrightarrow K[V]$.

3.4.2 The primitive element

The second approach for the description of the algebra $K[V]$ is most commonly used in the design of elimination procedures because of its efficiency. The underlying idea consists in specializing the generic parameters U_i used to define the elimination polynomial. We take some concrete data $u_{r+1}, \ldots, u_n \in R$ and the linear form

$$u := u_{r+1}X_{r+1} + \cdots + u_nX_n \in R[X_{r+1}, \ldots, X_n].$$

With the same notations as before, we say that u is a *primitive element* of $K[V]$ with respect to the Noether normalisation $A \hookrightarrow K[V]$ if the characteristic polynomial χ_u and the minimal polynomial $\mathfrak{m}_u$ of η_u agree (i.e. if $\chi_u = \mathfrak{m}_u$ holds). In fact, a primitive element u verifies that $B' = F \otimes_A K[V]$ and $F[T]/(\mathfrak{m}_u(T))$ are isomorphic.

This is equivalent to saying that for $D = rk_A K[V]$ and $\bar{u}$ the class of u modulo $I(V)$ the set $\{1, \bar{u}, \ldots, \bar{u}^{D-1}\}$ is a basis of the zero–dimensional algebra B' if and only if u is primitive element of $K[V]$ with respect to the Noether normalisation $A \hookrightarrow K[V]$.

All these equivalent properties may be illustrated by the following geometric property. Let U be the regular mapping given by :

$$U : \mathbb{K}^{\mathrm{n}} \longrightarrow \mathbb{K}^{\mathrm{r+1}} : \ \mathrm{U}(\mathrm{X}_1, \ldots, \mathrm{X}_\mathrm{n}) = (\mathrm{X}_1, \ldots, \mathrm{X}_\mathrm{r}, \mathrm{u}(\mathrm{X}_{\mathrm{r+1}}, \ldots, \mathrm{X}_\mathrm{n})).$$

Then, u is a primitive element if and only if U defines a birational isomorphism between V and the hypersurface $\mathcal{H}_U$ given by :

$$\mathcal{H}_U := \{(X_1, \ldots, X_{r+1}) \in \mathbb{K}^{\mathrm{r+1}} : \mathfrak{m}_\mathrm{u}(\mathrm{X}_1, \ldots, \mathrm{X}_{\mathrm{r+1}}) = 0\}.$$

Since $A \hookrightarrow K[V]$ is integral, the inverse U^{-1} restricted to V of the birational isomorphism U can be obtained in the following way :

$$U^{-1} := (X_1, \ldots, X_r, \rho_{r+1}^{-1} v_{r+1}(X_1, \ldots, X_{r+1}), \ldots, \rho_n^{-1} v_n(X_1, \ldots, X_{r+1})),$$

where for $r+1 \leq i \leq n$, the $\rho_i \in K[X_1, \ldots, X_r]$ are non–zero polynomials and the $v_i \in K[X_1, \ldots, X_r, T]$ are polynomials whose degree with respect to the variable T is at most $D-1$. The polynomials $\rho_{r+1}X_{r+1} - v_{r+1}, \ldots, \rho_nX_n - v_n$ are then called a *canonical parametrization* of the ideal–theoretic complete intersection variety V.

In other words, the following identity between ideals in $F[x_{r+1}, \ldots, x_n]$ holds :

$$F \otimes_A I(V) = (\mathfrak{m}_u(u), \rho_{r+1}X_{r+1} - v_{r+1}, \ldots, \rho_nX_n - v_n)$$

Observe that for $i = r+1, \ldots, n$ the dependent variable X_i is parametrized by $\rho_i^{-1}v_i$.

Proposition 35 (Proposition 16, [28]) *Suppose the polynomials $\rho_{r+1}X_{r+1} - v_{r+1}, \ldots, \rho_nX_n - v_n$ define a canonical parametrization of an ideal–theoretic complete intersection variety V. Then, the polynomials $\rho_i \in R[X_1, \ldots, X_r] \setminus \{0\}, r+1 \leq i \leq n$ and the coefficients of the polynomials $v_i \in R[X_1, \ldots, X_r][t]$ verify the conditions :*

- $\deg \rho_i \leq (\deg V)^3$,
- *the degree of the coefficients of the v_i is $\leq 2(\deg V)^3$,*
- *in $K(Y_1, \ldots, Y_r)[Y_{r+1}, \ldots, Y_n]$ holds the identity $(\mathfrak{m}_u, \rho_{r+1}X_{r+1} - v_{r+1}, \ldots, \rho_nX_n - v_n) = I(V)$,*
- *and $\rho_i\bar{X}_i - v_i(X_1, \ldots, X_r, \bar{u}) = 0$ in $K[V]$.*

Let us observe that the information provided by $\mathcal{H}_U$, U, and U^{-1} is sufficient to describe $K[V]$ completely. The set $\{1, \bar{u}, \ldots, \bar{u}^{D-1}\}$ is a basis of $F \otimes_A K[V]$ as a vector space. The matrix M_u is the companion matrix of $\mathfrak{m}_u$ with respect to this basis. The tensor matrices M_i, for $r+1 \leq i \leq n$, will be given by :

$$M_i := \rho_i^{-1} v_i(M_u). \tag{12}$$

The elimination polynomial can be obtained as the characteristic polynomial of the matrix given by :

$$\sum_{i=r+1}^{n} U_i \cdot \rho_i^{-1} v_i(M_u). \tag{13}$$

Definition 36 (Geometric Solution) *Let $V \subseteq \mathbb{K}^n$ be an ideal–theoretic complete intersection R–definable variety $V = V(f_1, \ldots, f_t)$ of dimension r, i.e. $r + t = n$. A* geometric solution *of V is the following list of data :*

- *a non–singular matrix $N \in \mathcal{N}(V)$ such that the set of variables*

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = N \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$$

  are in Noether position with respect to V, this means the ring $A_N := K[Y_1, \ldots, Y_r]$ verifies that $A_N \hookrightarrow K[V]$ is an integral ring extension,

- *a primitive element $u = u_{r+1}Y_{r+1} + \cdots + u_nY_n \in R[Y_{r+1}, \ldots, Y_n]$ of the integral ring extension $A_N \hookrightarrow K[V]$,*

- *a polynomial $P \in R[Y_1, \ldots, Y_r][T]$ of the form*

$$P = CT^D + g(Y_1, \ldots, Y_r, T),$$

  where $C \in \mathbb{Z} \setminus \{0\}, \deg_T g \leq D-1$ and $C^{-1}P$ is the minimal polynomial of u with respect to $K[V]$ (let us observe that $\deg_T P = rk_{A_N} K[V]$) and finally

- *a representation of U^{-1} given as the list $\rho_{r+1}, \ldots, \rho_n \in R[Y_1, \ldots, Y_r]$, $v_{r+1}, \ldots, v_n \in R[Y_1, \ldots, Y_r][T]$ with $\deg v_j \leq D-1$ such that*

$$I(V) = (P(u), \rho_{r+1}X_{r+1} - v_{r+1}(u), \ldots, \rho_nX_n - v_n(u))$$

  is an equality of ideals in $K(Y_1, \ldots, Y_r)[Y_{r+1}, \ldots, Y_n]$.

Observe that for the minimal polynomial P of the primitive element u holds :

$$K[X_1, \ldots, X_n]/(P(u), \rho_{r+1}X_{r+1} - v_{r+1}(u), \ldots, \rho_nX_n - v_n(u)) = K[T]/(P(T)).$$

In [25], [60] a procedure that computes geometric solutions for the varieties $V_i = V(f_1, \ldots, f_i)$ for $1 \leq i \leq t$ is shown. The main statement is describe in Section 6 below.

3.5 Height of complete intersection varieties.

Being well conscious about the existing differences between the commutative algebra, projective and affine geometrical context, we introduce a notion of height for complete intersection varieties which is strongly inspired by the works [61], [62] and [66], [67], [68]. These authors focused their attention on the elimination polynomial of equidimensional projective varieties in order to define an appropriate notion of height. In spite of the non–homogeneous condition of our ideals we can condense a notion of

height for affine varieties in the elimination polynomial $\mathfrak{m}_{\mathcal{U}}$. This depends on the condition of having the variables in Noether position, but this is not a relevant restriction as we will see.

Our main goal here is to show that elimination polynomial and geometric solution are not only computationally equivalent. They are also equivalent in terms of height and we are therefore free to use either in our forthcoming statements.

Definition 37 *Let $V \subseteq \mathbb{K}^n$ be an ideal–theoretic complete intersection R–definable variety of dimension r. Let $N \in \mathcal{N}(V)$ be a linear change of coordinates that puts the variables in Noether position with respect to V. Let $Y_1, \ldots, Y_n$ be the new variables and $A = K[Y_1, \ldots, Y_r]$ be the ring of polynomials such that $A_N \hookrightarrow K[V]$ is an integral ring extension. We define :*

i) the degree of V with respect to A_N *as* $\deg(V, N) := rk_{A_N} K[V]$. *Let us observe that if $\mathfrak{m}_{\mathcal{U}} \in R[Y_1, \ldots, Y_r][U_{r+1}, \ldots, U_n][T]$ is the elimination polynomial of V with respect to A_N (see Subsection 3.4.1) we have :*

$$\deg(V, N) = \deg_T \mathfrak{m}_{\mathcal{U}}.$$

ii) the height of V with respect to the Noether normalisation A_N *as the logarithmic height*

$$ht(V, N) := ht(\mathfrak{m}_{\mathcal{U}}).$$

iii) Finally, Philippon's invariant height of V with respect to the Noether normalisation A_N *is :*

$$\widetilde{ht}(V, N) := \widetilde{ht}(\mathfrak{m}_{\mathcal{U}}).$$

These notions of degree and height may be seen as mappings :

$$\deg_V : \mathcal{N}(V) \longrightarrow \mathbb{R}, \qquad \mathrm{ht_V} : \mathcal{N}(\mathrm{V}) \longrightarrow \mathbb{R}, \qquad \widetilde{\mathrm{ht}}_{\mathrm{V}} : \mathcal{N}(\mathrm{V}) \longrightarrow \mathbb{R}.$$

To state the forthcoming results in a concise form, we shall restrict the domains of these mappings, while trying to minimize the loss of generality. First, we work mainly with the set of Noether normalisations $N \in \mathcal{N}_{\mathbb{Z}}(V)$ which have integer entries. Second, there exists a universal constant $c > 0$ independent from V such that there exist matrices $N \in \mathcal{N}_{\mathbb{Z}}(V), N = (n_{ij})_{1 \leq i,j \leq n}, n_{ij} \in \mathbb{Z}$ verifying

$$| n_{ij} | \leq (n \deg(V))^c. \tag{14}$$

Finally, we restrict our Noether normalisations to the class of matrices

$$N(V) := \{N \in \mathcal{N}_{\mathbb{Z}}(V) : H_1(N) \leq (n \deg(V))^c, \deg(V, N) = \deg(V)\}.$$

Definition 38 (Heights) *With the previous notations, for an ideal–theoretic complete intersection R–definable variety $V \subseteq \mathbb{K}^n$, we define*

i) the height *of V as* $ht(V) := \max\{ht(V, N) : N \in N(V)\}$,

ii) and Philippon's invariant height *of V as* $\widetilde{ht}(V) := \max\{\widetilde{ht}(V, N) : N \in N(V)\}$.

3.6 Relations between both approaches

This Section shows that the two approaches for the description of $F \otimes_A K[V]$ via *elimination polynomial* and *geometric solution* are essentially equivalent, both in terms of computational and height estimates.

3.6.1 Computational equivalence

From the geometric solution to the elimination polynomial Let us assume that we have a complete intersection variety $V \subseteq \mathbb{K}^n$ of dimension r, generated by and that $I(V) = (f_1, \ldots, f_{n-r})$. Let $N \in \mathcal{N}_{\mathbb{Z}}(V)$ be a linear change of coordinates which puts the variables in Noether position with respect to V, i.e. the new set of variables $(Y_1, \ldots, Y_n)$ given by

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = N \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$$

verifies that the following is an integral ring extension : $A = K[Y_1, \ldots, Y_r] \hookrightarrow K[Y_1, \ldots, Y_n]/I(V) = B$. Let $D \in \mathbb{N}$ be the rank of B as free A–module. Let $U_{r+1}, \ldots, U_n$ be a new set of variables and

$$\mathcal{U} = U_{r+1}X_{r+1} + \cdots + U_nX_n$$

the generic projection. The elimination polynomial $\mathfrak{m}_{\mathcal{U}}$ as introduced in Subsection 3.4.1 can be obtained as the characteristic polynomial $\chi_{\mathcal{U}}$ of the matrix :

$$M_{\mathcal{U}} = T_{r+1}M_{r+1} + \cdots + T_nM_n$$

where the matrices M_i are the tensor matrices M_{X_i} of $A \hookrightarrow B$ describing the multiplication by the dependent variables X_i for $r + 1 \leq i \leq n$.

Thus, using Proposition 19 (Berkowitz) we can obtain the characteristic polynomial $\chi_{\mathcal{U}}$ of $M_{\mathcal{U}}$ by a straight–line program Γ_0 of size D^6, non–scalar depth $2\log_2 D + 7 = O(\log_2 D)$ and parameters in $\{-1, 0, 1\}$ which takes as inputs the entries of the matrix $M_{\mathcal{U}}$ and outputs the coefficients of the elimination polynomial $\chi_{\mathcal{U}}$ in $A_T := A[U_{r+1}, \ldots, U_n]$.

Now, let us consider a geometric solution of the variety V (as introduced in Section 3.4) consisting of :

- a primitive element u (Subsection 3.4.2),
- the minimal polynomial $\mathfrak{m}_u \in A[Z]$ of u and
- the canonical parametrizations $\rho_i X_i - v_i(Z)$ for $r + 1 \leq i \leq n$.

Let M_u be the companion matrix of $\mathfrak{m}_u$. Then, by Equation (12) we can compute a multiple of the tensor matrix M_i as $\rho_i M_i = v_i(M_u)$. Defining $\rho := \prod_{i=r+1}^{n} \rho_i$, we have :

$$\rho M_{\mathcal{U}} := U_{r+1}(\prod_{i \neq r+1} \rho_i) \cdot v_{r+1}(M_u) + \cdots + U_n(\prod_{i \neq n} \rho_i)v_n(M_u).$$

Thus, applying Proposition 19 (Berkowitz) there exists a non–scalar straight–line program Γ_1 of size $O(n \cdot D)$, non–scalar depth $O(\max\{\log_2 n, \log_2 D\})$, and parameters in $\{-1, 0, 1\} \subseteq \mathbb{Z}$, which takes as inputs

- the new variables $U_{r+1}, \ldots, U_n$,
- the coefficients of p,
- the coefficients of the polynomials $v_{r+1}, \ldots, v_n$ and
- the polynomials $\rho_{r+1}, \ldots, \rho_n$

and outputs the entries of the matrix $\rho M_{\mathcal{U}}$. Finally, let us consider the coordinate change given by the variables Z and Z' related by $Z' = \rho Z$. Then, we have :

$$\rho^D \det(Z - M_{\mathcal{U}}) = \det(\rho Z - \rho M_{\mathcal{U}}) = \det(Z' - \rho M_{\mathcal{U}}).$$

So, the coefficients of the characteristic polynomial $\chi_{\mathcal{U}}$ can be obtained by dividing the coefficients of the characteristic polynomial of $\rho M_{\mathcal{U}}$ (as obtained by the straight–line program Γ_1) by $\frac{1}{\rho^D}$. We then conclude the following Proposition :

Proposition 39 *There exists a non–scalar straight–line program Γ of size $O(n \cdot D) + D^{O(1)}$, non–scalar depth $O(\log_2 n + \log_2 D)$, and parameters in $\{-1, 0, 1\}$, which takes as inputs*

- *the variables $U_{r+1}, \ldots, U_n$,*
- *the coefficients of the minimal polynomial $\mathfrak{m}_u$ of the primitive element u,*
- *the coefficients of the polynomials $v_{r+1}, \ldots, v_n$ and*
- *the polynomials $\rho_{r+1}, \ldots, \rho_n$*

and, applying Proposition 20 (Vermeidung von Divisionen)*, outputs the coefficients of the elimination polynomial $\chi_{\mathcal{U}}$.*

From the elimination polynomial to the geometric solution Conversely, let us suppose now that we are given an elimination polynomial of the variety V with respect to a fixed Noether normalisation N. In [43], [44] a well-parallelizable method was exposed, which transforms the coefficients of the elimination polynomial into the coefficients of the geometric solution of the variety V. Roughly speaking, the method is expressed as a well-parallelizable straight–line program (of appropriate size) performing this transformation. A brief sketch of this method runs as follows :

Let $\mathcal{U} := U_{r+1}X_{r+1} + \cdots + U_nX_n$ be the generic projection with respect to a Noether normalisation $A = K[X_1, \ldots, X_r] \hookrightarrow K[V]$. Let $\mathfrak{m}_{\mathcal{U}}$ be its minimal polynomial in $A[U_{r+1}, \ldots, U_n][T]$ with respect to the variety V. Let us recall that $\mathfrak{m}_{\mathcal{U}}$ is monic (up to a constant in $\mathbb{Z}$) with respect to the variable T.

Let us now consider for $r + 1 \leq i \leq n$ the projections :

$$z_i := U_{r+1}X_{r+1} + \cdots + U_{i-1}X_{i-1} + U_{i+1}X_{i+1} + \cdots + U_nX_n$$

and the polynomials $Q_i := \mathfrak{m}_{\mathcal{U}}(X_1, \ldots, X_r, U_{r+1}, \ldots, U_{i-1}, 0, U_{i+1}, \ldots, U_n, T)$,

$$G_i := \mathfrak{m}_{\mathcal{U}}(X_1, \ldots, X_r, 0, \ldots, 0, 1, 0, \ldots, 0, T).$$

Then, we have the following

Lemma 40 ([44]) *There exists a geometric solution of the variety V given by :*

- $u := u_{r+1}X_{r+1} + \cdots + u_nX_n \in \mathbb{Z}[X_{r+1}, \ldots, X_n]$,
- $P_u \in R[X_1, \ldots, X_r][T]$,
- $\rho_i \in K[X_1, \ldots, X_r]$ *for* $r + 1 \leq i \leq n$ *and*
- $v_i \in K[X_1, \ldots, X_r][T]$ *for* $r + 1 \leq i \leq n$,

such that the following holds :

i) $|\, u_i \,| \leq (\deg(V))^{O(1)}$ *for* $r + 1 \leq i \leq n$,

ii) $m_u(X_1,\ldots,X_r) := \mathfrak{m}_{\mathcal{U}}(X_1,\ldots,X_r,u_{r+1},\ldots,u_n)$.

Let us consider for $r+1 \leq i \leq n$ *the polynomials*

$$q_i := Q_i(X_1,\ldots,X_r,U_{r+1},\ldots,U_{i-1},U_{i+1},\ldots,U_n,T),$$

$$g_i := G_i(X_1,\ldots,X_r,0,\ldots,0,1,0,\ldots,0,T).$$

Then, there exists a non–scalar straight–line program of size $(n\deg(V))^{O(1)}$*, non–scalar depth* $O(\log\deg(V))$ *and parameters in* $\{-1,0,1,u_{r+1},\ldots,u_n\}$ *which from the coefficients with respect to the variable* T *of the polynomials* $q_{r+1},\ldots,q_n$*,* $g_{r+1},\ldots,g_n$ *computes the coefficients with respect to the variable* T *of the polynomials* $v_{r+1},\ldots,v_n$ *and the polynomials* $\rho_{r+1},\ldots,\rho_n$*.*

Moreover, this procedure for computing the geometric solution of V from the elimination polynomial can be performed by an algorithm running in bounded error probability, probabilistic time $(n\deg(V))^{O(1)}$.

3.6.2 Equivalence of height estimates

Let us observe that the two main statements shown in the previous Subsection say that we may pass from the elimination polynomial to the geometric solution and vice versa by means of an algorithmic procedure with low bounds in terms of parallel complexity (non-scalar depth). Since height estimates depend mainly on the non-scalar depth (see Section 2.3) we may easily conclude the following two Theorems.

Theorem 41 *There exists a universal constant* $c > 0$ *independent of all involved data such that for every ideal–theoretic complete intersection* R*–definable variety* $V \subseteq \mathbb{K}^n$*, there exist the following elements :*

i) a Noether normalisation $N \in N(V)$*,*

ii) a geometric solution of V *with respect to* N *(see Definition 36), i.e.*

- *a primitive element* $u = u_{r+1}Y_{r+1} + \cdots + u_nY_n$*,*
- *the minimal polynomial* $P \in K[Y_1,\ldots,Y_r][T]$*,*
- *polynomials* $\rho_i \in R[Y_1,\ldots,Y_r]$ *and polynomials* $v_i \in R[Y_1,\ldots,Y_r][T]$

such that the following holds :

i) the data $N,u,P,\rho_{r+1},\ldots,\rho_n,v_{r+1},\ldots,v_n$ *is a geometric solution of* V*,*

ii) $|\,u_i\,| \leq H_1(u) \leq (\deg(V))^c$*,*

iii) $\max\{ht(P),ht(\rho_iX_i - v_i(T))\} \leq \deg(V)^c((n-r)+ht(V))$*, and*

iv) $\max\{\widetilde{ht}(P),\widetilde{ht}(\rho_iX_i - v_i(T))\} \leq \deg(V)^c((n-r)+\widetilde{ht}(V))$*.*

Moreover, all these polynomials verify the degree bounds stated in Proposition 35 on page 28.

Proof.– Combining the Lemmata 11, 14, 15, 17 and 40. ∎

Theorem 42 *For the height estimates of the elimination polynomial holds :*

$$ht(\chi_{\mathcal{U}}) \leq (nD)^{O(1)}(ht(\mathfrak{m}_u)) + \sum_{i=r+1}^{n} ht(\rho_i X_i - v_i(Z)),$$

$$\widetilde{ht}(\chi_{\mathcal{U}}) \leq (nD)^{O(1)}(\widetilde{ht}(\mathfrak{m}_u) + \sum_{i=r+1}^{n} \widetilde{ht}(\rho_i X_i - v_i(Z)).$$

Proof.– Applying Proposition 39, there exists a non–scalar straight–line program of size $(nD)^{O(1)}$, non-scalar depth $O(\log_2 n + \log_2 D)$ and parameters in $\{-1, 0, 1\}$ which, taking as input the coefficients of the polynomials $\mathfrak{m}_u$, $\rho_1, \ldots, \rho_n$ and $v_1, \ldots, v_n$ with respect to the variable Z, evaluates the coefficients of $\chi_{\mathcal{U}}$ with respect to the variable Z. Applying Corollary 18 (Composition), we obtain that the coefficients of $\chi_{\mathcal{U}}$ verify that both ht and $\widetilde{ht}$ are bounded by the heights of the coefficients of $\mathfrak{m}_u, v_1, \ldots, v_n$ and the heights of $\rho_1, \ldots, \rho_n$. Next, applying Corollary 12 (Coefficients) shows that also $ht(\chi_{\mathcal{U}})$ and $\widetilde{ht}(\chi_{\mathcal{U}})$ are bounded by these estimates. Finally, the heights of the coefficients of $\mathfrak{m}_u$, $v_1, \ldots, v_n$ and also $\rho_1, \ldots, \rho_n$ are appropriately bounded, see Corollary 12. ∎

4 Interpolation modulo complete intersection varieties

Trace formulae have been used recently in several papers treating problems in algorithmic elimination theory. There are two main applications of this kind of identities : computation of monomial bases of low degree (as in [3], [5]) or interpolation modulo complete intersection varieties (as in [23], [43], [44], [25]). Here we follow the second approach to solve the following problem :

Let A be a ring of polynomials over a given number field. Let F be the quotient field of A, $\mathbb{F}$ the algebraic closure of F and let $A[X_1, \ldots, X_n]$ be the ring of n–variate polynomials with coefficients in A. Let $f_1, \ldots, f_n$ be polynomials in the ring $A[X_1, \ldots, X_n]$ of degree at most d in the variables $X_1, \ldots, X_n$ such that the following holds :

- the ideal $(f_1, \ldots, f_n)$ is radical and
- for $B := A[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$ the morphism $A \hookrightarrow B$ is an integral ring extension representing a Noether normalisation of the variety $V = V(f_1, \ldots, f_n)$ defined by the polynomials $f_1, \ldots, f_n$ in a suitable affine space.

Thus, B is a free A–module of rank bounded by the degree of the variety $V(f_1, \ldots, f_n)$. Moreover, the A–algebra B is Gorenstein and the following statements are based on this fact.

Now the interpolation problem can be stated in the following terms :

Problem 3 (Interpolation modulo complete intersection variety) *Given an element $g \in B$, compute a polynomial $g_1 \in A[X_1, \ldots, X_n]$ such that $\bar{g}_1 = g$ holds in B.*

Let us explain why this can be considered as an "interpolation" problem. The residue class $g \in B$ of a polynomial can be given in terms of a matrix M_g as described in Section 3. However, the method we are going to show, does not require all of the information available in this matrix.
Let $V \subseteq \mathbb{F}$ be the zero–dimensional algebraic variety defined by

$$V := V(f_1, \ldots, f_n) = \{\underline{x} \in \mathbb{F}^n : f_i(\underline{x}) = 0 \text{ for } 1 \leq i \leq n\},$$

and let us assume that $V = \{\alpha_1, \ldots, \alpha_D\}$. The procedure for the solution of Problem 3 we will exhibit in the sequel will also solve the following task :

Given a list of eigenvalues $\{\beta_1, \ldots, \beta_D\} \subseteq \mathbb{F}$ of a matrix M_g which describes the endomorphism of multiplication by an element $g \in B$ with respect to some fixed basis, compute a polynomial $g_1 \in A[X_1, \ldots, X_n]$ (if it exists) such that holds : $g_1(\alpha_i) = \beta_i$ for $1 \leq i \leq D$.

In some cases, in particular our case the existence of g_1 can be guaranteed : Let f, h be two elements of B such that f is not a zero–divisor in B and f divides h in B. Then, there exists a $g_1 \in A[X_1, \ldots, X_n]$ such that

$$g_1(\alpha_i) = \frac{h(\alpha_i)}{f(\alpha_i)} = \beta_i \text{ for } 1 \leq i \leq D.$$

The polynomial g_1 computed by our procedure verifies $\bar{g_1} \cdot f = h$. The objective for any constructive solution of the Interpolation Problem 3 will be of course to minimize the degree of g_1 with respect to the variables $X_1, \ldots, X_n$.

4.1 Trace and duality

With the above notations we are going to sketch a few standard facts related with the solution of the Interpolation Problem 3.

Recall that we are considering ideal-theoretic complete intersection varieties given by a sequence of polynomials $f_1, \ldots, f_n \in A[X_1, \ldots, X_n]$ generating a radical ideal of codimension n. The A–algebra $B := A[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$ is reduced and Gorenstein (see Section 3). Let B^* denote the dual of B by $B^* := \mathrm{Hom}_A(B, A)$ as a B–module by the scalar product $B \times B^* \longrightarrow B^*$ which associates to any (b, τ) in $B \times B^*$ the A–linear map $b \cdot \tau : B \longrightarrow A$ defined by $(b \cdot \tau)(x) := \tau(bx)$ for any element x of B.

Since we know by our short discussion in Section 3 that the A–algebra B is Gorenstein, its dual B^* is a free B–module of rank one. Any element σ of B^* which generates B^* as B–module is called a *canonical trace* of B or simply a trace.

There exists a particular element Tr of B^* relevant for our purposes. The mapping $Tr \in B^*$ and is given in the following way : given $b \in B$, let $\eta_b : B \longrightarrow B$ the A–linear map defined by multiplying by b any given element of B. The image $Tr(b)$ under the map Tr is defined as the trace of the endomorphism η_b of B. This mapping Tr is called the *standard trace* of B and it should be remarked that it is not necessarily a canonical trace in the above sense, i.e. does not necessarily generate B^*.

Let us introduce some additional notations, which we will need to show how to compute a canonical trace σ. For any element $g \in A[X_1, \ldots, X_n]$ we denote by $\bar{g}$ its image in B, i.e. the residue class of g modulo the ideal $(f_1, \ldots, f_n)$. Let $Y_1, \ldots, Y_n$ be new variables and let $Y := (Y_1, \ldots, Y_n)$. Let $1 \leq j \leq n$ and let $f_j^Y := f_j(Y_1, \ldots, Y_n)$ be the polynomial of $A[Y_1, \ldots, Y_n]$ obtained from f_j by substituting the variables $X_1, \ldots, X_n$ by $Y_1, \ldots, Y_n$. Let us consider the polynomial

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

where the l_{jk} are polynomials belonging to $A[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ with total degree at most $(d-1)$. Let us now consider the determinant Δ of the matrix $(l_{jk})_{1 \leq j,k \leq n}$ which can be written (non uniquely) as

$$\Delta = \sum_m a_m(X_1, \ldots, X_n) b_m(Y_1, \ldots, Y_n) \in A[X_1, \ldots, X_n, Y_1, \ldots, Y_n],$$

with the a_m being elements of $A[X_1, \ldots, X_n]$ and b_m elements of $A[Y_1, \ldots, Y_n]$ (observe that it will not be necessary to find the polynomials a_m and b_m algorithmically, we need just their existence for our argumentation). The polynomial Δ is called a *pseudo–jacobian determinant* of the regular sequence $(f_1, \ldots, f_n)$, as defined in Subsection 2.4.

Observe that the polynomials a_m and b_m can (and will) be chosen to have degrees bounded by $n(d-1)$ in the variables $X_1, \ldots, X_n$ and $Y_1, \ldots, Y_n$ respectively. Let $c_m \in A[X_1, \ldots, X_n]$ be the polynomial we obtain from b_m by substituting the variables $Y_1, \ldots, Y_n$ by $X_1, \ldots, X_n$. Denoting by $\bar{J}$ the class of the Jacobian determinant $J(f_1, \ldots, f_n)$ in B, we have the identity

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

Moreover the image of the polynomial Δ in the residue class ring

$$A[X_1, \ldots, X_n, Y_1, \ldots, Y_n]/(f_1, \ldots, f_n, f_1^Y, \ldots, f_n^Y)$$

is independent of the particular choice of the matrix $(l_{kj})_{1 \leq k,j \leq n}$. This justifies the name *pseudo–jacobian determinant* for the polynomial Δ.

With these notations there exists a unique canonical trace $\sigma \in B^*$ such that the following identity holds in B :

$$\bar{1} = \sum_m \sigma(\bar{a}_m) \cdot \bar{c}_m.$$

This canonical trace σ is called the *canonical trace associated to the pseudo–jacobian determinant*. The main property of the canonical trace σ, known as "trace formula" ("Tate's trace formula", see [48, Appendix F] or [39], as a particular case) is the following statement : for any $g \in A[X_1, \ldots, X_n]$ the identity

$$\bar{g} = \sum_m \sigma(\bar{g} \cdot \bar{a}_m) \cdot \bar{c}_m \tag{15}$$

holds true in B. Let us observe that the polynomial $\sum_m \sigma(\bar{g} \cdot \bar{a}_m) \cdot c_m \in A[X_1, \ldots, X_n]$ underlying Identity (15) is of degree at most $n(d-1)$ in the variables $X_1, \ldots, X_n$. The next Proposition shows how to relate the standard trace Tr and a canonical trace $\sigma \in B^*$ (see also [25]) :

Proposition 43 ([70])

$$\sigma(\bar{g}) = \mathrm{Tr}(\bar{g} \cdot \bar{J}^{-1})$$

Tate's trace formula (15) solves the Interpolation Problem 3 in the following terms :

Given $g \in B$, let us consider the polynomial $g_1 \in A[X_1, \ldots, X_n]$ of degree at most $n(d-1)$ given by

$$g_1 := \sum_m \sigma(\bar{g} \cdot \bar{a}_m) \cdot c_m. \tag{16}$$

Then, $\bar{g}_1 = g$ in B.

The use of these monomial expressions of (16) inhibits us from taking advantage of any special "semantical" features of the A–algebra B : one "a priori" needs all monomials of degree at most $n(d-1)$ for the description of the polynomials c_m (and a_m). Therefore, we replace the trace formula (15) by the following alternative one, which solves the problem in a suitable linear vector space :

First, recall that in our case A is a ring of polynomials over a number field, $f_1, \ldots, f_n$ are polynomials in the ring $A[X_1, \ldots, X_n]$ of degree at most d in the variables $X_1, \ldots, X_n$, generating a radical ideal. The extension $A \hookrightarrow B := A[X_1, \ldots, X_n]/(f_1, \ldots, f_n)$ is an an integral ring extension. Thus, we are given an ideal-theoretic complete intersection variety, where the A–algebra B is reduced and Gorenstein (see Section 3).

Proposition 44 (Trace Formula, [25]) *With the same notations as before, let us consider the free $A[X_1, \ldots, X_n]$–module $B[X_1, \ldots, X_n]$ given by extending scalars to B (this means we consider*

the tensor product $B[X_1,\ldots,X_n] := B \otimes_A A[X_1,\ldots,X_n]$*) and let us also consider the polynomial* $\Delta_1 \in A[X_1,\ldots,X_n]$ *given by :*

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

Then for any $g \in A[X_1,\ldots,X_n]$ *the following identity holds in* $A[X_1,\ldots,X_n]$ *:*

$$\bar{g} = \sum_m \sigma(\bar{g}\cdot\bar{a}_m)\cdot c_m = \widetilde{\mathrm{Tr}}(\bar{J}^{-1}\cdot\bar{g}\cdot\Delta_1)$$

(where $\widetilde{\mathrm{Tr}} := \mathrm{Tr}\otimes Id_{A[X_1,\ldots,X_n]} : B[X_1,\ldots,X_n] \longrightarrow A[X_1,\ldots,X_n]$ *is the trace obtained from the standard trace* $\mathrm{Tr} : B \longrightarrow A$ *by extending scalars).*

The reader will observe that the duality techniques used here agree in the case of $n = 1$ with the standard Lagrange interpolation.

4.2 Division modulo complete intersection ideals

One of the main applications of these interpolation techniques will be the division modulo complete intersection ideals. This problem can be stated in the following terms :

Given a sequence of polynomials $f_1,\ldots,f_t \in R[X_1,\ldots,X_n]$ of degree at most d defining a radical ideal $(f_1,\ldots,f_t)$ of codimension t. Let V be the complete intersection variety given by $V = (f_1,\ldots,f_t)$. Let us assume that the variables are in Noether position with respect to the variety V, i.e. the following is an integral ring extension :

$$A = K[X_1,\ldots,X_{n-t}] \hookrightarrow B = K[V] = K[X_1,\ldots,X_n]/(f_1,\ldots,f_t).$$

We have thus the same conditions as in the previous Subsection. Then, there exists a pseudo–jacobian determinant defined by $f_1,\ldots,f_t$ with respect to the variables $X_{n-t+1},\ldots,X_n$. There exist $a_m, c_m \in A[X_{n-t+1},\ldots,X_n]$ such that

$$\Delta = \sum_{1\le m\le N} a_m \otimes c_m \in B\otimes B,$$

where the polynomials c_m can be chosen as polynomials in the variables $Y_{n-t+1},\ldots,Y_n$ of degree at most $t(d-1)$. Let b_m be the monomial given as $c_m(X_{n-t+1},\ldots,X_n)$. Moreover, the polynomials $a_m \in K[X_1,\ldots,X_n]$ have total degree at most $t(d-1)$. The problem we want to solve is the following :

Problem 4 (Division Problem) *With the previous notations, given two polynomials* f, g *in* $R[X_1,\ldots,X_n]$ *such that* $\bar{f}$ *is not a zero divisor in* B*, and* $\bar{f}$ *divides* $\bar{g}$ *in* B*, this means there exists some* $q \in B$ *such that*

$$qf - g \in (f_1,\ldots,f_t).$$

Then, compute *some polynomial* $q_1 \in K[X_1,\ldots,X_n]$ *such that* $q_1 f - g \in (f_1,\ldots,f_t)$ *holds.*

First, we give a formal statement showing how the trace formulae of the previous Section 4.1 interferes in the solution of Problem (4). Then we show how to use this statement in a computational solution for the Division Problem.

Let $\sigma \in B^*$ be the trace associated to the pseudo–jacobian determinant Δ. Let $q \in K[X_1,\ldots,X_n]$ be any polynomial such that $\bar{q}\cdot\bar{f} = \bar{g}$ holds in B. Let F be the quotient field of A, $B' := F\otimes_A B$ the zero–dimensional F–algebra and $\sigma' : B' \to F$ the canonical trace on B' obtained by extending scalars on σ (i.e. $\sigma' = \sigma$ on B). Then, since $\bar{f}$ is not a zero divisor in B, $\bar{f}$ is a unit in B'. Hence, $\bar{q} = (\bar{f})^{-1}\cdot\bar{g}$ holds in B'. We then conclude that for every $h \in K[X_1,\ldots,X_n]$ the following holds :

$$\sigma'((\bar{f})^{-1}\cdot\bar{g}\cdot\bar{h}) = \sigma'(\bar{q}\cdot\bar{h}) = \sigma(\bar{q}\cdot\bar{h}) \in A.$$

In particular, we conclude :

Proposition 45 *With the previous hypotheses and notations, the polynomial*

$$q_1 = \sum_{1 \leq m \leq N} \sigma'((\bar{f})^{-1} \cdot \bar{g} \cdot \bar{h}) \cdot b_m \in K[X_1, \ldots, X_n]$$

verifies that the degree of q_1 with respect to the variables $X_{n-t+1}, \ldots, X_n$ is at most $t(d-1)$, and $q_1 f - g \in (f_1, \ldots, f_t)$.

Moreover, let $\widetilde{Tr}' : B'[X_{n-t+1}, \ldots, X_n] \to F[X_{n-t+1}, \ldots, X_n]$ be the extension of the standard trace

$$\widetilde{Tr} : B[X_{n-t+1}, \ldots, X_n] \to A[X_{n-t+1}, \ldots, X_n]$$

by localization at $A \setminus \{0\}$. Let $\Delta_1 = \sum_{1 \leq m \leq N} \bar{a}_m \cdot b_m \in B[X_{n-t+1}, \ldots, X_n]$ be the pseudo–jacobian determinant seen as an element of $B'[X_{n-t+1}, \ldots, X_n]$. Finally, let $\bar{J} \in B$ be the residual class defined by the jacobian determinant of the polynomials $f_1, \ldots, f_t$ with respect to the variables $X_{n-t+1}, \ldots, X_n$. Then, the polynomial q_1 of the previous Proposition 45 can also be obtained as :

$$q_1 = \widetilde{Tr}'((\bar{J})^{-1} \cdot (\bar{f})^{-1} \cdot \bar{g} \cdot \Delta_1). \tag{17}$$

Now, for the computational solution of the Division Problem 4, we have to represent the entities appearing in Equation (17). We can do this by associating to each endomorphism its corresponding matrix of multiplication in a suitable basis, following Section 3. We thus obtain the following :

$$q_0 = \widetilde{Tr}'(M_{\bar{J}}^{-1} \cdot M_{\bar{f}}^{-1} \cdot M_g \cdot M_{\Delta_1}), \tag{18}$$

We can compute this polynomial using the method described in Lemma 21 in Section 2.4.

Proposition 46 *With the previous assumptions and conventions, let D be the rank of B as free A–module (observe that $D \leq \deg(V)$ holds). Let us also assume that there exists a non–scalar straight–line program Γ_1 of size L_1, depth ℓ_1 and parameters in $\mathcal{F}_1 \subseteq R$ such that Γ_1 evaluates $f, f_1, \ldots, f_t \in R[X_1, \ldots, X_n]$. Let us suppose $\deg(f_i) \leq d, \deg(f) \leq d$ with respect to the variables $X_1, \ldots, X_n$. Let us also assume that $g \in R[X_1, \ldots, X_n]$ has degree at most d with respect to the variables $X_{n-t+1}, \ldots, X_n$. Let us finally assume that there exists a non–scalar straight–line program Γ_2 of size L_2, non–scalar depth ℓ_2 and parameters in a finite set $\mathcal{F}_2 \subseteq R$ which evaluates g. Then, there exists a non–scalar straight–line program Γ over A, taking as input a geometric solution of $V(f_1, \ldots, f_t)$ (see Definition 36 on page (36)) with the following properties :*

i) the size of Γ is at most $(L_1 + L_2)(tdD)^{O(1)}$,

ii) the non–scalar depth of Γ is at most $O(\log_2 t + \ell_1 + \ell_2 + \log_2 D)$,

iii) the parameters are in $\mathcal{F}_1 \cup \mathcal{F}_2 \cup \{z \in \mathbb{Z} : |z| \leq (td)^{O(1)} L_1\}$, and

iv) the straight–line program Γ evaluates two polynomials $q_0 \in R[X_1, \ldots, X_n]$ and $\Theta \in R[X_1, \ldots, X_{n-t}]$ such that holds :

$$q_1 = \frac{q_0}{\Theta} \in K[X_1, \ldots, X_n] \text{ and } q_1 f - g \in (f_1, \ldots, f_t). \tag{19}$$

Here we simply sketch the proof of this Proposition. A more explicit description can be found in [33] or [25]. The key point can be understood as the following : One wishes to compute the polynomial $q_1 \in K[X_1, \ldots, X_n]$ verifying the desired properties. Thus, the Trace Formula (17) of Proposition 45 in the computational form of Equation (18) shows how to compute q_1 from the geometric solution of the variety V. However, as the geometric solution yields tensor matrices (describing the multiplication by the variables X_i in B) whose entries are quotients of polynomials, we will have to find a common denominator polynomial for these. Moreover, inverting the matrices M_J and M_f will also introduce

denominators. By our method, these will be "carried on" by keeping numerators and denominators separate in order to express q_1 as the quotient

$$q_1 = \frac{q_0}{\Theta} \tag{20}$$

where q_0 and Θ are polynomials in $R[X_1, \ldots, X_n]$ computed from the coefficients of the geometric solution of V (or equivalently, from the coefficients of the elimination polynomial $\mathfrak{m}_{\mathcal{U}}$ using only addition, subtraction and multiplication).

The polynomials q_0 and Θ in $R[X_1, \ldots, X_n]$ are given by straight–line program encoding, which means given as the list of coefficients of the geometric solution and a list of arithmetic operations required to evaluate them. As we know that Θ divides q_0 in $R[X_1, \ldots, X_n]$, the computation of q_1 concludes with the application of Strassen's *Vermeidung von Divisionen* as in Lemma 20, yielding a straight–line program for the polynomial q_1.
We will have to iterate divisions of precomputed polynomials which involve precomputed quotients. The naïve approach, simply iterating the above procedure, would yield an excessive growth of the complexity of the method. Therefore, we combine in the proofs of Theorem 1 and Theorem 2 the strategy of Proposition 46 with two methods, namely *Pasodoble effect* and *iterated matrix product*, which improve the complexity and height estimates (depending mainly on the non–scalar depth of the straight–line programs describing our algorithm).

5 Equations in general position : Geometric degree and height

This Section is dedicated to the proof of Corollary 5 given in Section 1. We introduce the notion of *polynomials in general position* as the central property of our inductive algorithm, and show how to maintain this condition while controlling the height of the appearing coefficients in terms of the *geometric degree of the system*. Then, we show how to deduce the claims made in Corollary 5 from Theorems 1 and 2.

5.1 Geometric degree and height of a system

Here we introduce the notions of *geometric degree* and *height* of a system of polynomials. Observe that this can be done in both cases in a very similar way.

Definition 47 (General position) *A sequence of polynomials $h_1, \ldots, h_t \in R[X_1, \ldots, X_n]$ is said to be in* general position *if the following holds :*

- *$h_1, \ldots, h_{t-1}$ is a regular sequence in $K[X_1, \ldots, X_n]$,*
- *the ideals $(h_1, \ldots, h_i)$ are radical in $K[X_1, \ldots, X_n]$ for $1 \leq i \leq t-1$, and*
- *h_t is not a zero divisor in $K[X_1, \ldots, X_n]/(h_1, \ldots, h_{t-1})$.*

Definition 48 (Geometric degree of a sequence) *Given a sequence of polynomials $h_1, \ldots, h_t \in R[X_1, \ldots, X_n]$ in general position, we denote by δ the* geometric degree of the sequence $h_1, \ldots, h_t$ *:*

$$\delta(h_1, \ldots, h_t) := \max\{\deg V(h_1, \ldots, h_i) : 1 \leq i \leq t-1\}.$$

Let us notice that $\delta(h_1, \ldots, h_t) \leq \prod_{i=1}^{t-1} \deg(h_i)$ holds. Observe, that the δ thus defined does not just depend on the variety V but also on the polynomials $h_1, \ldots, h_t$ and their order.

Similarly, we define the logarithmic height and invariant logarithmic height of a sequence in general position.

Definition 49 (Height of a sequence) *Given a sequence of polynomials $h_1, \ldots, h_t \in R[X_1, \ldots, X_n]$ in general position, we define :*

i) the logarithmic height of the sequence $\eta(h_1, \ldots, h_t) := \max\{htV(h_1, \ldots, h_i) : 1 \leq i \leq t-1\}$,

ii) the invariant logarithmic height of the sequence $\widetilde{\eta}(h_1, \ldots, h_t) := \max\{\widetilde{ht}V(h_1, \ldots, h_i) : 1 \leq i \leq t-1\}$.

Definition 50 (Geometric degree of a system) *Let $S = \{f_1, \ldots, f_s\}$ be a system of polynomials of degree at most d in $R[X_1, \ldots, X_n]$. We consider the set $\tilde{S}$ of all families $\{h_1, \ldots, h_t : 1 \leq t \leq n+1\}$ of polynomials such that the following holds : There exist integer numbers $\lambda_{ij} \in \mathbb{Z}, 1 \leq i \leq t, 1 \leq j \leq s$ such that :*

- $h_i := \sum_{j=1}^{s} \lambda_{ij} f_j$,
- $(h_1, \ldots, h_t) = (f_1, \ldots, f_s) = (1)$,
- $h_1, \ldots, h_t$ *are in general position and*
- $| \lambda_{ij} | \leq (nd\delta(h_1, \ldots, h_t))^c \leq (nd^t)^c$.

We define

i) the geometric degree δ_S of the system S *as* $\delta_S := \max\{\delta(h_1, \ldots, h_t) : \{h_1, \ldots, h_t\} \in \tilde{S}\}$.

ii) the logarithmic height η_S of the system S *as* $\eta_S := \max\{\eta(h_1, \ldots, h_t) : \{h_1, \ldots, h_t\} \in \tilde{S}\}$.

iii) and the invariant logarithmic height $\widetilde{\eta}_S$ of the system S *as*

$$\widetilde{\eta}_S := \max\{\widetilde{\eta}(h_1, \ldots, h_t) : \{h_1, \ldots, h_t\} \in \tilde{S}\}.$$

Observe that initially, we are given polynomials $f_1, \ldots, f_s \in R[X_1, \ldots, X_n]$. Passing from these polynomials to a sequence $h_1, \ldots, h_t$ in general position as described in Section 5.2 is a constructive, algorithmic process. Therefore, in our estimates, we are forced to assume worst-case estimates, which means taking *maximums* in our definitions of *geometric degree* and *height*.

Nevertheless, our Theorems are of a double nature : existential statement and at the same time algorithmic solution. The existential statements made in Corollary 5 and Corollary 6 also hold for any particular sequence $h_1, \ldots, h_t$ in general position which minimizes the products $\delta_S \eta_S$ or $\delta_S \widetilde{\eta}_S$ respectively.

5.2 Computing equations in general position

The proof of Corollaries 5 and 6 requires some additional effort for the preparation of the input polynomials $f_1, \ldots, f_s \in R[X_1, \ldots, X_n]$. We show how to proceed in the case of the arithmetic Nullstellensatz, the membership problem for complete intersection ideals follows in the same way. In the following we exhibit an efficient procedure that, taking as inputs the polynomials $f_1, \ldots, f_s$, outputs a sequence of polynomials $h_1, \ldots, h_t \in R[X_1, \ldots, X_n]$ with $t \leq n+1$ such that $(h_1, \ldots, h_t) = (f_1, \ldots, f_s) = (1)$. For this sequence of polynomials $h_1, \ldots, h_t$ holds :

i) h_i is a linear combination of $f_1, \ldots, f_s$ for $1 \leq i \leq t$,

ii) $(h_1, \ldots, h_t)$ defines the trivial ideal in $K[X_1, \ldots, X_n]$ and

iii) $(h_1, \ldots, h_t)$ verifies that 1) the ideals $(h_1, \ldots, h_i)$ are radical ideals in $K[X_1, \ldots, X_n]$ of codimension i, for $1 \leq i \leq t-1$, and 2) the polynomial h_t is not a zero divisor in the residue ring

$$K[X_1, \ldots, X_n]/(h_1, \ldots, h_{t-1}).$$

Let us observe that this effectively shows that the set $\tilde{S}$ appearing in Definition 50 is non–empty. Since $\{h_1, \ldots, h_t\} \in \tilde{S}$ are linear combinations of $f_1, \ldots, f_s$, they can be evaluated by a non–scalar straight–line program of size $L + ts$, non–scalar depth $\ell + 1 = O(\log_2 L)$ and parameters in $\mathcal{F} \cup \mathcal{P}$, where $\mathcal{P} \subseteq \mathbb{Z}$ is a finite set whose height we are going to bound.

Lemma 51 (Zero divisor, Lemma 24, [60]) *Let $g_1, \ldots, g_t$ be a regular sequence generating a radical ideal and assume that the variables $X_1, \ldots, X_n$ are in Noether position with respect to the ideal $I = (g_1, \ldots, g_t)$. Let $g \in K[X_1, \ldots, X_n]$ be a new polynomial, η_g the endomorphism defined by multiplication by g and M_g the matrix of η_g in some fixed basis. Then we have :*

i) g is not a zero divisor in B if and only if $\det(M_g) \in K[X_1, \ldots, X_r] \setminus \{0\}$.

ii) If g is not a zero divisor in B, the ideal $(g_1, \ldots, g_t)$ is the trivial ideal in $K[X_1, \ldots, X_n]$ if and only if $\det(M_g) \in K \setminus \{0\}$.

Using Bertini's Theorem as stated in [40, Theorem 6.3] we may obtain the following statement :

Proposition 52 (Proposition 29, [60]) *Let $h_1, \ldots, h_t$ be a regular sequence in $K[X_1, \ldots, X_n]$ such that the ideal $I = (h_1, \ldots, h_t)$ is a radical ideal in $K[X_1, \ldots, X_n]$. Let $f_1, \ldots, f_s$ be polynomials in $K[X_1, \ldots, X_n]$ such that they generate the trivial ideal. Let $T_1, \ldots, T_s$ some new variables and let h be the polynomial*

$$h = T_1 f_1 + \cdots + T_s f_s.$$

Let F be the field $K(T_1, \ldots, T_s)$. Then,

i) h is not a zero divisor in $F[X_1, \ldots, X_n]/(h_1, \ldots, h_t)$, and

ii) either $(h_1, \ldots, h_t, h)$ is the trivial ideal in $F[X_1, \ldots, X_n]$ or $(h_1, \ldots, h_t, h)$ is a radical ideal in $F[X_1, \ldots, X_n]/(h_1, \ldots, h_t)$.

Proposition 53 *There exists a universal constant $c > 0$ such that the following holds : Given $f_1, \ldots, f_s \in R[X_1, \ldots, X_n]$ polynomials of degree at most d such that $(f_1, \ldots, f_s)$ is the trivial ideal in $K[X_1, \ldots, X_n]$, there exists $t \in \mathbb{N}, 1 \leq \mathrm{t} \leq \mathrm{n} + 1$ and integer numbers $\lambda_{ij} \in \mathbb{Z}$, $1 \leq i \leq t$, $1 \leq j \leq s$, such that the following holds :*

- *the polynomials $h_1, \ldots, h_t$ given by $h_i = \sum_{j=1}^{s} \lambda_{ij} f_j$, $1 \leq i \leq t$ are in general position,*
- *$(h_1, \ldots, h_t) = (f_1, \ldots, f_s) = (1)$ in $K[X_1, \ldots, X_n]$, and*
- *$\mid \lambda_{ij} \mid \leq (nd\delta(h_1, \ldots, h_i))^c$ for $1 \leq i \leq t$ (where $\delta(\emptyset) := 1$).*

Proof.– The proof follows follows by means of an inductive argument. Thus, let us assume that there exist $h_1, \ldots, h_i \in R[X_1, \ldots, X_n]$ $\mathbb{Z}$–linear combinations of $f_1, \ldots, f_s$ such that the ideal $(h_1, \ldots, h_i)$ is a proper ideal of codimension i. Let us also assume that the variables $X_1, \ldots, X_n$ are in Noether position with respect to the ideal $(h_1, \ldots, h_i)$, i.e. the following is an integral ring extension

$$A = K[X_1, \ldots, X_{n-i}] \hookrightarrow K[X_1, \ldots, X_n]/(h_1, \ldots, h_i) = B.$$

Let us now introduce some new variables $T_1, \ldots, T_s$ and the polynomial

$$h = T_1 f_1 + \cdots + T_s f_s \in K(T_1, \ldots, T_s)[X_1, \ldots, X_n].$$

Let A' and B' be the algebras obtained from A and B by extending scalars, i.e.

$$A' = K(T_1, \ldots, T_s) \otimes_K A = K(T_1, \ldots, T_s)[X_1, \ldots, X_{n-i}],$$

$$B' = K(T_1, \ldots, T_s) \otimes_K B.$$

Again, we have an integral ring extension $A' \hookrightarrow B'$ and B' is a free A'–module. We observe that the basis of B as A–module is also a basis of B' as A'–module and that for every polynomial $f \in K[X_1, \ldots, X_n]$ the matrix of the endomorphism $\eta_f : B \longrightarrow B$ is also the matrix of the endomorphism $\eta'_f : B' \longrightarrow B'$. In other words, $M'_f = M_f$ for all polynomials f in $K[X_1, \ldots, X_n]$. In particular, let η'_h be the endomorphism $\eta'_h : B' \longrightarrow B'$ defined by multiplying by h. We have

$$M'_h = T_1 M_{f_1} + \cdots + T_s M_{f_s}.$$

The entries of M'_h are polynomials in $K[T_1, \ldots, T_s, X_1, \ldots, X_{n-i}]$ of degree at most 1 in the variables $T_1, \ldots, T_s$. Now, let χ_h be the characteristic polynomial of M'_h, which can be written in the following way :

$$\chi_h = Z^\delta + a_{\delta-1} Z^{\delta-1} + \cdots + a_0,$$

with $\delta = rk_A B = rk_{A'} B'$, coefficients $a_i \in K[T_1, \ldots, T_s, X_1, \ldots, X_{n-i}]$ and $a_0 = \det(M'_h)$. The coefficients a_i are polynomials of degree at most δ in the variables $T_1, \ldots, T_s$. Now, we have two possibilities : either A) $a_0 \in K[T_1, \ldots, T_s]$ or B) $a_0 \in K[T_1, \ldots, T_s, X_1, \ldots, X_{n-i}] \setminus K[T_1, \ldots, T_s]$.

A) In the first case, let us choose a point $\underline{t} := (t_1, \ldots, t_s) \in \mathbb{Z}^s$ such that $a_0(t_1, \ldots, t_s) \neq 0$. The polynomial

$$h_{i+1} = t_1 h_1 + \cdots + t_s h_s$$

verifies that h_{i+1} is not a zero divisor modulo $(h_1, \ldots, h_i)$ and $(h_1, \ldots, h_{i+1})$ is the trivial ideal in $K[X_1, \ldots, X_n]$. As the degree of a_0 is bounded by δ, the point $\underline{t} = (t_1, \ldots, t_s) \in \mathbb{Z}^s$ may be chosen such that $|\, t_i \,| \leq \delta$, for $1 \leq i \leq s$. In this case we have finished since $h_1, \ldots, h_{i+1}$ are in general position and $(h_1, \ldots, h_{i+1}) = (f_1, \ldots, f_s)$.

B) As for the second case, we have to make an additional effort. First we perform a linear change of coordinates $(X_1, \ldots, X_n) \to (Y_1, \ldots, Y_n)$ such that for $A'_1 := K(T_1, \ldots, T_s)[Y_1, \ldots, Y_{n-i-1}]$ and the A'_1–algebra

$$B'_1 := K(T_1, \ldots, T_s)[Y_1, \ldots, Y_n]/(h_1, \ldots, h_i, h)$$

the new variables $Y_1, \ldots, Y_n$ verify that $A'_1 \hookrightarrow B'_1$ is an integral ring extension. In fact, this can be done simply by transforming the polynomial a_0 in such a way that

$$a_0(T_1, \ldots, T_s, Y_1, \ldots, Y_{n-i}) = b_D Y_{n-i}^D + \cdots + b_0 \tag{21}$$

where $b_i \in K[T_1, \ldots, T_s, Y_1, \ldots, Y_{n-i-1}]$. The degree D is at most $\delta \cdot d$ as shown in [29, Lemma 11]. Of course, the degree of the polynomials b_i with respect to the variables $T_1, \ldots, T_s$ is at most δ. Now, we proceed as in [29, Section 4] or [28, Section 5], to compute a primitive element of the integral ring extension $A'_1 \hookrightarrow B'_1$.

Let $u = \lambda_{n-i} Y_{n-i} + \cdots + \lambda_n Y_n$ be such a primitive element with $\lambda_j \in \mathbb{Z}$ for $n - i \leq j \leq n$. Now, there exists a universal constant $c_1 > 0$ such that the degrees of the geometric solution given by the polynomials $\mathfrak{m}_u, \rho_{n-i}, \ldots, \rho_n,\ v_{n-i}, \ldots, v_n$ with respect to the variables $T_1, \ldots, T_s$ are at most $(d\delta)^{c_1}$.

Finally, we consider the Jacobian determinant $J = \det J(h_1, \ldots, h_i, h)$, which is not a zero divisor in B'_1. This simply means that we consider the matrix M'_J of the endomorphism $\eta'_J : B'_1 \longrightarrow B'_1$.

The determinant of M'_J is a polynomial in $K[T_1, \ldots, T_s, Y_1, \ldots, Y_{n-i-1}]$ whose degree in the variables $T_1, \ldots, T_s$ is at most $(nd\delta)^c$ for some universal constant $c \geq c_1 > 0$. Thus, let us consider the following two polynomials

$$F_1 = \det(M_h) \in K[T_1, \ldots, T_s, Y_1, \ldots, Y_{n-i}] \text{ and } F_2 = \det(M'_J) \in K[T_1, \ldots, T_s, Y_1, \ldots, Y_{n-i-1}].$$

Both polynomials are not in $K[T_1, \ldots, T_s]$. Let us choose two points $\underline{y}_1 = (y_1^{(1)}, \ldots, y_{n-i}^{(1)})$ and $\underline{y}_2 = (y_1^{(2)}, \ldots, y_{n-i}^{(2)}) \in \mathbb{Z}^{n-i}$ such that the following polynomials $\mathfrak{F}_1$ and $\mathfrak{F}_2$ verify :

$$\mathfrak{F}_1 = F_1(T_1, \ldots, T_s, \underline{y}_1) - F_1(T_1, \ldots, T_s, \underline{y}_2) \neq 0 \text{ and } \mathfrak{F}_2 = F_2(T_1, \ldots, T_s, \underline{y}_1) - F_2(T_1, \ldots, T_s, \underline{y}_2) \neq 0.$$

Finally, the polynomial $\mathfrak{F}_1 \cdot \mathfrak{F}_2 \in K[T_1, \ldots, T_s]$ is a non zero polynomial of degree at most $(nd\delta)^c + \delta$. For every point $(t_1, \ldots, t_s) \in \mathbb{Z}^s$ such that $\mathfrak{F}_1 \cdot \mathfrak{F}_2(t_1, \ldots, t_s) \neq 0$ we have that F_1 and F_2 are non–zero polynomials. In particular, let h_{i+1} be the polynomial $h_{i+1} = t_1 f_1 + \cdots + t_s f_s$. Then, we obtain that h_{i+1} is not a zero divisor modulo $(h_1, \ldots, h_i)$, and the ideal $(h_1, \ldots, h_i, h_{i+1})$ is a proper radical ideal of codimension $i + 1$.

The coordinates of the point $(t_1, \ldots, t_s) \in \mathbb{Z}^s$ can be obviously chosen such that $| t_i | \leq (nd\delta)^c + \delta$. ■

5.3 The case of trivial ideals

Now we are in conditions to give the proof of Corollary 5 from Theorems 1 and 2 :

From Proposition 53 we easily deduce the existential statements of Corollary 5 (i.e. claims $ii), iii), iv)$ and $v)$ as a consequence of the bounds given in Theorem 1 and 2.

As for claim $vi)$, the proof of Proposition 53 essentially shows how to compute polynomials $h_1, \ldots, h_t \in \mathbb{Z}[X_1, \ldots, X_n]$ given as linear combinations of the input polynomials $f_1, \ldots, f_s$ and verifying the conditions described in Proposition 53. To see how this works, we shall explain the inductive step :

Suppose that we already have computed polynomials $h_1, \ldots, h_i$ (for a fixed $i, 1 \leq i \leq m$) such that

i) $(h_1, \ldots, h_j)$ is a radical ideal of codimension j in $K[X_1, \ldots, X_n]$ for $1 \leq j \leq i$, and

ii) $h_1, \ldots, h_i$ are linear combinations of $f_1, \ldots, f_s$ of the form

$$h_k := \sum_{j=1}^{s} \lambda_{kj} f_j \text{ with } | \lambda_{kj} | \leq (nd\delta_S)^c.$$

Now, suppose that we have computed a Noether normalisation of $(h_1, \ldots, h_i)$, i.e. a matrix $N \in M_n(\mathbb{Z})$ such that the variables

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = N \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$$

are in Noether position with respect to $h_1, \ldots, h_i$, i.e. the following is an integral ring extension

$$A = K[Y_1, \ldots, Y_{n-i}] \hookrightarrow K[Y_1, \ldots, Y_n]/(h_1, \ldots, h_i) = B.$$

We may also assume that a geometric solution (Def. 36 on page 29) of $V(h_1, \ldots, h_i)$ has been computed with respect to the Noether normalisation N. As observed in Lemma 40, all this can be done in time

$$(nd(L + s)\delta_S)^{O(1)}.$$

Now, we proceed as follows :

i) Introduce some new variables $T_1, \ldots, T_s$.

ii) Consider the polynomial $H = T_1 f_1 + \cdots + T_s f_s \in R[T_1, \ldots, T_s][Y_1, \ldots, Y_n]$.

iii) Consider $A[T] := A[T_1, \ldots, T_s]$, $B[T] = A[T] \otimes_A B$ and the homothesy : $\eta_H : B[T] \to B[T]$.

iv) Compute the determinant of the matrix of η_H (using the geometric solution), yielding the polynomial $P_1(Y_1, \ldots, Y_{n-i}, T_1, \ldots, T_s) \in A[T]$.

v) Now, using a probabilistic algorithm (as described in Section 2.5.1 or [87], [72]) decide (according to Lemma 51 on page 41) whether $P_1(Y_1, \ldots, Y_{n-i}, T_1, \ldots, T_s)$ is in $K[T_1, \ldots, T_s]$ or not.

vi) If $P_1(Y_1,\ldots,Y_{n-i},T_1,\ldots,T_s) \in K[T_1,\ldots,T_s]$, choose a point in $\mathbb{Z}^s$, say $(\lambda_{i+1,1},\ldots,\lambda_{i+1,s})$, such that $|\,\lambda_{i+1,k}\,| \leq (nd\delta_s)^s$ and P_1 does not vanish : $P_1(Y_1,\ldots,Y_{n-i},\lambda_{i+1,1},\ldots,\lambda_{i+1,s}) \neq 0$. The algorithm terminates by writing $t = i+1$, $h_t = \lambda_{t,1}f_1 + \cdots + \lambda_{t,s}f_s$.

vii) Else, compute a Noether normalisation of the ideal $(h_1,\ldots,h_i,H)$ as an ideal of codimension $i+1$ in $K(T_1,\ldots,T_s)[Y_1,\ldots,Y_n]$. In other words, compute $N' \in M_n(\mathbb{Z})$ a regular matrix such that

$$\begin{pmatrix} Y_1' \\ \vdots \\ Y_n' \end{pmatrix} = N' \cdot \begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix}$$

such that for $A'[T] := K(T_1,\ldots,T_s)[Y_1',\ldots,Y_{n-i+s}']$ the following

$$A'[T] \hookrightarrow K(T_1,\ldots,T_s)[Y_1',\ldots,Y_n']/(h_1,\ldots,h_i,H)$$

is an integral ring extension. Then, compute the Jacobian determinant of the sequence $(h_1,\ldots,h_i,H)$ with respect to the variables $Y_{n-i}',\ldots,Y_n'$. Let $J(Y_1',\ldots,Y_{n-i-1}',T_1,\ldots,T_s)$ in $R[T_1,\ldots,T_s,Y_1',\ldots,Y_{n-i-1'}]$ be this polynomial. Finally, using a probabilistic algorithm (as described in Section 2.5.1 or [87]) choose a point $(\lambda_{i+1,1},\ldots,\lambda_{i+1,s}) \in \mathbb{Z}^s$ with $|\,\lambda_{i+1,k}\,| \leq (nd\delta_s)^c$ for $1 \leq k \leq s$ such that

$$P_1(Y_1,\ldots,Y_{n-i},\lambda_{i+1,1},\ldots,\lambda_{i+1,s}) \neq 0 \text{ and}$$

$$J(Y_1',\ldots,Y_{n-i-1},\lambda_{i+1,1},\ldots,\lambda_{i+1,s}) \neq 0 \text{ holds.}$$

We now set $h_{i+1} = \lambda_{i+1,1}f_1 + \cdots + \lambda_{i+1,s}f_s$ and obtain thus the hypotheses made at the beginning and continue the induction.

This procedure runs in the desired time because all polynomials computed by the procedure are represented by the straight–line program which evaluates them. ∎

6 Proof of Theorem 1

This Section contains the proofs for the two statements of Theorem 1, 1) the complexity estimates and 2) the degree bounds claimed.

6.1 The degree bound

In this Subsection we give a proof for the degree bound for the polynomials g_i stated in claim 2) of Theorem 1.

We are given a finite sequence of polynomials $f_1,\ldots,f_t \in R[X_1,\ldots,X_n]$ with $t \leq n+1$ such that the following properties hold :

i) for every $i, 1 \leq i \leq t-1$, the ideals $(f_1,\ldots,f_i)$ are radical ideals of codimension i,

ii) the polynomial f_{i+1} is not a zero divisor in the residue ring $B_i := K[X_1,\ldots,X_n]/(f_1,\ldots,f_i)$ for $1 \leq i \leq t-1$,

iii) $\deg(f_i) \leq d, ht(f_i) \leq h$, for every $i, 1 \leq i \leq t$.

We are also given an additional polynomial $f \in R[X_1,\ldots,X_n]$ with $\deg(f) \leq d$ and $ht(f) \leq h$. Assuming that f belongs to the ideal $(f_1,\ldots,f_t)$ in $K[X_1,\ldots,X_n]$, we wish to compute $a \in R$ and $g_1,\ldots,g_t \in R[X_1,\ldots,X_n]$ such that the following identity holds :

$$af = g_1f_1 + \cdots + g_tf_t.$$

We consider the intermediate varieties $V_i := V(f_1, \ldots, f_i)$ for $1 \leq i \leq t-1, D_i := \deg(V_i)$ and $\delta := \max\{D_1, \ldots, D_{t-1}\}$.

We will make use of the following Proposition, saying that we can compute geometric solutions for all intermediate varieties V_i. The proof of this Proposition can be found for example in [44], [28], [25] and [60].

Proposition 54 (Geometric solutions, [25]) *With the previous hypotheses and notations, given a non–scalar straight–line program Γ of size L, non–scalar depth ℓ and parameters in a finite set $\mathcal{F} \subseteq R$, such that Γ evaluates the polynomials $f_1, \ldots, f_t, f \in R[X_1, \ldots, X_n]$ verifying the hypotheses of Theorem 1 above. Then there exists a bounded error probability Turing machine which, taking as input this straight–line program Γ computes the following items :*

i) a regular matrix $N \in \mathcal{M}_n(\mathbb{Z}), N = (\nu_{ij})_{1 \leq i,j \leq n}$ such that

(a) $|\, \nu_{ij} \,| \leq (n\delta)^c$, where c is the universal constant of Equation (14) on Page 30,

(b) the variables $Y_1, \ldots, Y_n$ given by :

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = N \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$$

are in Noether position with respect to all intermediate varieties V_i, i.e.

$$A_i := K[Y_1, \ldots, Y_{n-i}] \hookrightarrow B_i := K[Y_1, \ldots, Y_n]/(f_1, \ldots, f_i)$$

is an integral ring extension for $1 \leq i \leq t-1$,

ii) a non–scalar straight–line program Γ' of size $O(ndL\delta)^{O(1)}$ and parameters in $\mathcal{F} \cup \{z \in \mathbb{Z} : |\, z \,| \leq (ndL\delta)^c\}$, such that Γ' evaluates the geometric solutions of all the varieties $V_1, \ldots, V_{i-1}$ with respect to the Noether normalisation N, i.e. Γ' evaluates :

- *linear forms $u_i \in \mathbb{Z}[Y_{n-i+1}, \ldots, Y_n], 1 \leq i \leq t-1$, such that u_i is a primitive element of the integral ring extension $A_i \hookrightarrow B_i$. Moreover, u_i may be chosen such that $ht(u_i) \leq (ndL\delta)^c$.*
- *polynomials $p_i \in R[Y_{n-i+1}, \ldots, Y_n][T]$ for $1 \leq i \leq t-1$ of degree D_i with respect to the variable T. We may assume that p_i has the form*

$$p_i = \alpha_i T^{D_i} + h_i$$

where $\alpha_i \in R \setminus \{0\}$ is the leading coefficient of p_i and $\deg_T h_i \leq \deg p_i \leq D_i$. Moreover, $\alpha_i^{-1} p_i$ is the minimal equation of the endomorphism : $\eta_{u_i} : B_i' \to B_i'$ in the basis given by $\{1, \bar{u}_i, \ldots, \bar{u}_i^{D_i - 1}\}$.

- *for $1 \leq i \leq t-1$ polynomials $\rho_{n-i+1}^{(i)}, \ldots, \rho_n^{(i)} \in R[Y_{n-i+1}, \ldots, Y_n]$,*
- *for $1 \leq i \leq t-1$ polynomials $v_{n-i+1}^{(i)}, \ldots, v_n^{(i)} \in R[Y_{n-i+1}, \ldots, Y_n][T]$ with $\deg_T v_j^{(i)} \leq D_i - 1$. Moreover, for $1 \leq i \leq t-1$ and for $n-i+1 \leq j \leq n$, the polynomial $\rho_j^{(i)} Y_j - v_j^{(i)}(u_i)$ lies in the ideal generated by $(f_1, \ldots, f_i)$ in $K[Y_1, \ldots, Y_n]$.*

As observed in Section 3.2, B_i is a free A_i–module of rank at most D_i (and also bounded by the geometric degree δ). For every polynomial $g \in K[Y_1, \ldots, Y_n]$ we denote by $\bar{g}$ the residual class $g + (f_1, \ldots, f_i) \in B_i$, writing simply $\bar{g} \in B_i$ when no confusion may occur. We denote by $F_i := K(Y_1, \ldots, Y_{n-i})$ the quotient field of A_i (according to the *Nomenklatur* of [54]) and by B_i' the zero–dimensional F_i–algebra obtained by extending scalars in B_i, i.e.

$$B_i' := F_i \otimes_{A_i} B_i.$$

It is clear that B_i' is a F_i–vector space of finite dimension and that its dimension equals the rank of B_i as free A_i–module. For every A_i–module morphism $\sigma \in B_i^*$ ($:= \mathrm{Hom}_{A_i}(B_i, A_i)$) we denote by $\sigma' \in (B_i')^*$ ($:= \mathrm{Hom}_{F_i}(B_i', K_i)$) the F_i–linear mapping defined by extending scalars to B_i'. In particular, if $\sigma \in B_i^*$ is a canonical trace, the trace $\sigma' := \mathrm{Id}_{F_i} \otimes_{A_i} \sigma$ in $(B_i')^*$ is also a canonical trace (in the sense of Section 4.1).

Following our discussion in Section 4.1, we know that there exists a canonical trace $\sigma_i \in B_i^*$ associated to the pseudo–jacobian determinant defined by the sequence $f_1, \ldots, f_i$ with respect to the variables $Y_{n-i+1}, \ldots, Y_n$.

Let $\Delta_i \in B_i \otimes_{A_i} B_i$ be a pseudo–jacobian determinant defined by the sequence $f_1, \ldots, f_i$. Let us consider the set $\mathcal{M}_i$ of all monomials of degree at most $i(d-1)$ in the variables $\{Y_{n-i+1}, \ldots, Y_n\}$. Let us denote the monomials contained in $\mathcal{M}_i$ in the following way :

$$\mathcal{M}_i := \{b_k^{(i)} : 1 \leq k \leq N_i\},$$

where N_i is the cardinality of $\mathcal{M}_i$. Then, there exist polynomials $a_k^{(i)} \in A_i[Y_{n-i+1}, \ldots, Y_n], 1 \leq k \leq N_i$ of total degree bounded by $i(d-1)$ such that holds :

$$\Delta_i = \sum_{k=1}^{N_i} \overline{a_k^{(i)}} \otimes \overline{b_k^{(i)}} \in B_i \otimes_{A_i} B_i. \tag{22}$$

We want to apply the alternative trace formula given by Proposition 44. As discussed in Section 4.1, for $1 \leq i \leq t-1$ we have the canonical trace $\sigma_i' \in B_i'$ obtained by extending scalars to B_i'. Similarly, we may consider $\tilde{B}_i := B_i[Y_{n-i+1}, \ldots, Y_n] = A_i[Y_{n-i+1}, \ldots, Y_n] \otimes_{A_i} B_i$ and $\tilde{B}_i' := B_i'[Y_{n-i+1}, \ldots, Y_n]$.

Now, let us denote by $\Delta_1^{(i)}$ the pseudo–jacobian determinant Δ_i seen as an element in $\tilde{B}_i' = B_i'[Y_{n-i+1}, \ldots, Y_n]$. In other words, let $\Delta_1^{(i)}$ be the following element :

$$\Delta_1^{(i)} = \sum_{k=1}^{N_i} \overline{a_k^{(i)}} \otimes b_k^{(i)} \in B_i[Y_{n-i+1}, \ldots, Y_n].$$

Let us recall from Proposition 46 on page 38 that $\Delta_1^{(i)}$ can be evaluated by a non–scalar straight–line program of low complexity. Now, we consider the standard traces :

$$\widetilde{Tr}_i : \tilde{B}_i \to A_i[Y_{n-i+1}, \ldots, Y_n] = K[Y_1, \ldots, Y_n], \text{ and } \widetilde{Tr}_i' : \tilde{B}_i' \to F_i[Y_{n-i+1}, \ldots, Y_n],$$

where $\widetilde{Tr}_i'$ is $\mathrm{Id}_{F_i} \otimes_{A_i} \widetilde{Tr}_i$.

Let J_i denote the jacobian determinant of the sequence $f_1, \ldots, f_i$ with respect to the variables $Y_{n-i+1}, \ldots, Y_n$. Then, by Proposition 44 holds for every $g \in A_i[Y_{n-i+1}, \ldots, Y_n]$ the following identity :

$$g_1 = \sum_{1 \leq k \leq N_i} \sigma_i'(\bar{g} \cdot \bar{a}_k^{(i)}) b_k^{(i)} = \widetilde{Tr}_i'(\bar{J}_i^{-1} \cdot \bar{g} \cdot \Delta_1^{(i)})$$

$$\text{and } \bar{g}_1 - \bar{g} = 0 \text{ in } B_i.$$

This will allow us to compute a single division step in B_i as shown in Proposition 45.

The degree bound We are now in conditions to show the degree bound for the polynomials g_i appearing in the Bézout identity $af = g_1 f_1 + \cdots + g_t f_t$ of Theorem 1. We define inductively a sequence of polynomials $G_1, \ldots, G_t$ and $Q_1, \ldots, Q_t$ in $K[X_1, \ldots, X_n]$ in the following way :

$$G_t := \widetilde{Tr}_{t-1}'(\bar{J}_{t-1}^{-1} \cdot \bar{f}_t^{-1} \cdot \bar{f} \cdot \bar{\Delta}_1^{(t-1)}), \qquad Q_t := f - G_t f_t. \tag{23}$$

For $2 \leq i \leq t-1$, given Q_{i+1} we define:

$$G_i := \widetilde{Tr}'_{i-1}(\bar{J}_{i-1}^{-1} \cdot \bar{f}_i^{-1} \cdot \bar{Q}_{i+1} \cdot \bar{\Delta}_1^{(i-1)}), \qquad Q_i := Q_{i+1} - G_i f_i. \tag{24}$$

As for $i = 1$, we define

$$G_1 := \frac{Q_2}{f_1}, \qquad Q_1 := 0. \tag{25}$$

For the polynomials G_i and Q_i such defined holds :

$$f = G_1 f_1 + \cdots + G_t f_t. \tag{26}$$

Because of our discussion in Section 4.2 one now easily sees from their definition that the polynomials $G_1, \ldots, G_t$ are in $K[Y_1, \ldots, Y_n]$ and that they verify Identity (26).

The degree bound on the polynomials g_i as claimed in Theorem 1 (first stated in [28]) follows by an elementary inductive argument as that of [45] or [60]. We have to find a suitable common denominator $a \in R \setminus \{0\}$, such that defining $g_i := a \cdot G_i$, for $1 \leq i \leq t$ we obtain the expression stated in Theorem 1, i.e. $af = g_1 f_1 + \cdots + g_t f_t$, and $g_i \in R[Y_1, \ldots, Y_n]$. The forthcoming Section will show how to construct this denominator a for the polynomials $G_1, \ldots, G_t$.

6.2 The size of the straight–line program

Sketch of proof The following lines intend to give an overview for the proof of claim 1) of Theorem 1 – the complexity estimates in terms of size and non-scalar depth for a straight–line program evaluating polynomials $g_1, \ldots, g_t \in R[X_1, \ldots, X_n]$ and a non–zero constant $a \in R \setminus \{0\}$ such that $af = g_1 f_1 + \cdots + g_t f_t$ holds.

Since we are going to exhibit as precisely as possible the procedures underlying the straight–line programs evaluating the polynomials $g_1, \ldots, g_t \in R[X_1, \ldots, X_n]$ and the constant $a \in R \setminus \{0\}$ verifying the conditions of Theorem 1, we will have to pay a price in terms of style and notation. This outline hopefully clarifies the reasons for the necessarily detailed notations introduced in the proof.

The main technical tool we are going to use is a combination of the following two ingredients :

i) an efficient algorithm for computing the geometric solutions of all intermediate varieties $V_i = V(f_1, \ldots, f_i)$ for $1 \leq i \leq t-1$ as found in [25] and resumed in Proposition 54,

ii) and the division procedure described in Section 4, resumed in Proposition 46.

More precisely, for $1 \leq i \leq n$ we consider the intermediate varieties $V_i = V(f_1, \ldots, f_i)$ and the integral ring extensions

$$A_i := K[Y_1, \ldots, Y_{n-i}] \hookrightarrow B_i := K[Y_1, \ldots, Y_n]/(f_1, \ldots, f_i).$$

We show that there exist for $1 \leq i \leq t-1$ straight–line programs Γ_i in A_i taking as input the coefficients of a geometric solution for the variety V_i which performs the divison algorithm described in Section 4 and evaluate polynomials

$$\widetilde{G}_i \in R[X_1, \ldots, X_n], \qquad \widetilde{\Theta}_i \in R[X_1, \ldots, X_{n-i}] \tag{27}$$

with the following properties : 1) $\widetilde{\Theta}_i$ divides $\widetilde{G}_i$ in $K[X_1, \ldots, X_n]$, 2) $G_i = \frac{\widetilde{G}_i}{\widetilde{\Theta}_i}$, and for $1 \leq r \leq t$ the polynomial $f - \sum_{j=r}^{t} \frac{\widetilde{G}_j}{\widetilde{\Theta}_j} \cdot f_j$ is in $(f_1, \ldots, f_{r-1})$.

The geometric solutions of all intermediate varieties V_i are given by a straight–line program Γ' by Proposition 54. We use the information contained in this straight–line program Γ' as input for the straight–line programs Γ_i computing the divisions modulo the intermediate complete intersection

varietes. This composition of straight–line programs yields a new straight–line program which can be visualized by the scheme given in Figure 1, where the arrows signify "input", as indicated by Equations (23) to (25).

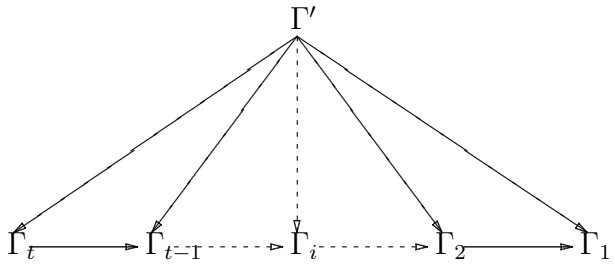

Figure 1: First Approach

Then, applying Strassen's *Vermeidung von Divisionen* technique (Proposition 20) to this straight–line program evaluating the polynomials $\widetilde{G}_i, \widetilde{\Theta}_i$ for $1 \leq i \leq t$, we would obtain a new straight–line program that evaluates a suitable constant $a \in R \setminus \{0\}$ and polynomials $g_1, \ldots, g_t \in R[X_1, \ldots, X_n]$ such that holds :

$$a^{-1} \cdot g_i = \frac{\widetilde{G}_i}{\widetilde{\Theta}_i} \text{ and } af = g_1 f_1 + \cdots + g_t f_t.$$

This strategy suffers one major drawback, called the *Pasodoble* effect :

Recall the method introduced in Section 4 to perform a single division modulo a complete intersection variety. This method will be applied in each straight–line program Γ_i, but the input of Γ_i is not just the geometric solution of the complete intersection variety $V_i = V(f_1, \ldots, f_i)$ but also the "remainder" of all previous divisions as expressed in the polynomials Q_j as introduced in Equations (23) to (25) on page 46 :

$$Q_j = f - \sum_{j=i}^{t} G_j \cdot f_j \text{ for } 1 \leq r \leq t.$$

The resulting effect on the dependency of the inputs is illustrated graphically in Figure 2.
Thus, to compute the polynomials $\widetilde{G}_i$ and $\widetilde{\Theta}_i$, all the previously computed straight–line programs $\Gamma_t, \ldots, \Gamma_{i+1}$ will be used. This "nesting" or dependence on the previous steps (therefore *Pasodoble* effect) causes an accumulated complexity increasal. If D_i denotes the geometric degree $\deg V_i$ of the intermediate variety V_i from the bounds obtained for a single division step in Section 4 follows for the straight–line programs Γ_i a complexity bound of order $(\prod_{j=r+1}^{t} D_j)^{O(1)}$, which is unsatisfactory.

Therefore, the main work in the forthcoming proof of Theorem 1 will be spent on showing a way how to avoid this *Pasodoble* effect.

The crucial observation for the proof of the complexity estimates of Theorem 1 is the fact that we can pre–compute some intermediate information in the form of some straight–line programs which we will denote by $\mathfrak{M}_1, \ldots, \mathfrak{M}_{t-1}$. This information will only depend on the geometric solutions of the intermediate varieties V_i and the input polynomials $f_1, \ldots, f_t$. In addition, we modify the straight–line programs Γ_i slightly to obtain some new straight–line programs Γ'_i such that the straight–line program of Table 1 above can be obtained as a straight–line program Γ'' in the following, alternative way illustrated in Figure 3.

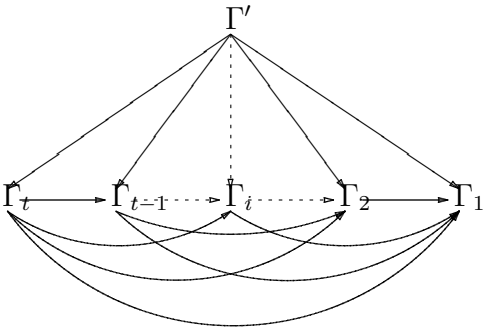

Figure 2: Consequences

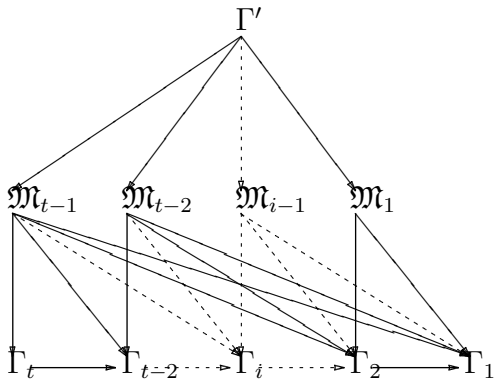

Figure 3: Alternative

For $t-1 \geq i \geq 1$ the straight–line programs $\mathfrak{M}_i$ will evaluate the polynomials listed in Proposition 64 on page 55. Then, using this information as input, the straight–line programs Γ_i evaluate the polynomials listed in Proposition 65 on page 57.

Applying Strassen's *Vermeidung von Divisionen* method (cf. Proposition 20) we obtain from the straight–line programs Γ_i a straight–line program evaluating the polynomials $g_1, \ldots, g_t$ and a non-zero constant $a \in R \setminus \{0\}$ such that $af = g_1 f_1 + \cdots + g_t f_t$ holds.

Roughly speaking, the new technical outcome may be explained as follows : We define inductively a sequence of polynomials $G_1, \ldots, G_t \in K[X_1, \ldots, X_n]$ by Equations (23) to (25) such that $f = G_1 f_1 + \cdots + G_t f_t$ holds. Suppose we have computed $G_t, \ldots, G_{i+1}$. Then, the polynomial G_i is given as :

$$\begin{aligned} G_i &= \widetilde{Tr}'_{i-1}(\bar{J}_{i-1}^{-1} \cdot \bar{f}_i^{-1} \cdot \bar{Q}_{i+1} \cdot \bar{\Delta}_1^{(i-1)}) \\ &= \widetilde{Tr}'_{i-1}(\bar{J}_{i-1}^{-1} \cdot \bar{f}_i^{-1} \cdot \bar{f} \cdot \bar{\Delta}_1^{(i-1)}) - \sum_{j=i+1}^{t} \widetilde{Tr}'_{i-1}(\bar{J}_{i-1}^{-1} \cdot \bar{f}_i^{-1} \cdot \bar{G}_j \cdot \bar{f}_j \cdot \bar{\Delta}_1^{(i-1)}). \end{aligned}$$

Now, the main point will be to determine which parts of $\bar{G}_j$ have some influence in the second part of the above formula, namely :

$$\widetilde{Tr}'_{i-1}(\bar{J}_{i-1}^{-1} \cdot \bar{f}_i^{-1} \cdot \bar{G}_j \cdot \bar{f}_j \cdot \bar{\Delta}_1^{(i-1)}). \tag{28}$$

The product $\bar{J}_{i-1}^{-1} \cdot \bar{f}_i^{-1} \cdot \cdot \bar{f}_j \cdot \bar{\Delta}_1^{(i-1)}$ depends just on the input system $S = \{f_1, \ldots, f_t\}$ and does not depend on the precomputed polynomials $G_t, \ldots, G_{i+1}$.

Now, we observe that the polynomial $G_j \in A_j[Y_{n-j+1}, \ldots, Y_n]$ has two main "components". First, we can see its "coefficients" being polynomials in $A_j \subseteq A_{i-1}$ and second, its "variables", namely $Y_{n-j+1}, \ldots, Y_n$. The main influence of the polynomial G_j in Equation (28) above depends on the action of the "variable" part of G_j under the trace $\widetilde{Tr}'_{i-1}$, i.e. the dependence on the variables $Y_{n-j+1}, \ldots, Y_n$, whereas the "coefficient" part of G_j does not interfere significantly.

We will show that this "variable" part of G_j depends only on the previously computed pseudo–jacobian determinants $\Delta_1^{(s)}$ for $t-1 \geq s \geq j$. These pseudo–jacobian determinants $\Delta_1^{(s)}$ are elements of $A_j[Y_{n-j+1}, \ldots, Y_n]$ and depend only on the input system $f_1, \ldots, f_t$, but not on the previously computed polynomials $G_t, \ldots, G_{i+1}$.

The task performed by the non–scalar straight–line programs $\mathfrak{M}_{t-1}, \ldots, \mathfrak{M}_{i-1}$ will be to "isolate" this "variable" part of the polynomials $G_t, \ldots, G_{i+1}$ to be reused in the computation of G_i. To clarify this idea : "isolate" does not mean to compute the monomials of G_j with respect to the variables

$Y_{n-j+1}, \ldots, Y_n$. It means a more sophisticated process which does not contain any "interpolation" steps and which we show explicitely in the sequel. As an additional complication interfers the necessity to "carry on" denominators as before, which increases the notational complexity of the proof once more. Unfortunately, we have not been able to exhibit this process using less notation.

Proof of the complexity estimates of Theorem 1 The complexity estimates of Theorem 1 follow by describing a suitable straight–line program that evaluates $G_1, \ldots, G_t$ from the information contained in the geometric solutions of the varieties $V_1, \ldots, V_{t-1}$. First of all, we want to give here a matricial expression of the equations (23), (24) and (25).

For every polynomial $g \in R[Y_1, \ldots, Y_n]$ we denote by $M_g^{(i)}$ the matrix of the endomorphism $\eta_g : B_i' \to B_i'$ in the basis given by the primitive element $\{1, \bar{u}_i, \ldots, \bar{u}_i^{D_i - 1}\}$.

Similarly, for every $\Delta \in B_i[Y_{n-i+1}, \ldots, Y_n]$ we denote by $M_\Delta^{(i)}$ the matrix associated to the endomorphism $\eta_\Delta : \widetilde{B}_i' \to \widetilde{B}_i'$ in terms of the basis given by the primitive element $\{1 \otimes 1, \bar{u}_i \otimes 1, \ldots, \bar{u}_i^{D_{i-1}} \otimes 1\}$.

Recall from page 46 that Δ_i denotes a pseudo–jacobian of $f_1, \ldots, f_i$ in $B_i \otimes_{A_i} B_i$ and that $\Delta_1^{(i)}$ is Δ_i seen as an element in $\tilde{B}_i' = B_i'[Y_{n-i+1}, \ldots, Y_n]$. Then, let us write $M^{(i)}_{\Delta_1^{(i)}}$ for the matrix of the endomorphism of multiplication by $\Delta_1^{(i)}$ in $\tilde{B}_i'$.

Then, the polynomials $G_t, \ldots, G_1$ we have defined recursively by Equations (23), (24) and (25) can be rewritten in terms of linear algebra using matrices as :

$$G_t = \widetilde{Tr}'_{t-1}((M_{J_{t-1}}^{(t-1)})^{-1} \cdot (M_{f_t}^{(t-1)})^{-1} \cdot M_f^{(t-1)} \cdot M^{(t-1)}_{\Delta_1^{(t-1)}})^{-1}), \qquad Q_t = f - G_t f_t$$

and, recursively for $t - 1 \geq i \geq 2$,

$$G_i = \widetilde{Tr}'_{i-1}((M_{J_{i-1}}^{(i-1)})^{-1} \cdot (M_{f_i}^{(i-1)})^{-1} \cdot M_{Q_{i+1}}^{(i-1)} \cdot M^{(i-1)}_{\Delta_1^{(i-1)}})^{-1}), \qquad Q_i = Q_{i+1} - G_i f_i$$

and finally $G_1 = \frac{Q_2}{f_1}, \qquad Q_1 := 0.$

All these expressions above involve divisions by non–constant polynomials (divisions by $\det(M_{J_{i-1}}^{(i-1)})$, $\det(M_{f_i}^{(i-1)})$ for instance. Even if the results of Section 3 would guarantee that the G_i's and the Q_i's are true polynomials (in $K[Y_1, \ldots, Y_n]$), the presence of intermediate divisions will hide (and make harder) the computation of the common denominator (in R) of the polynomials $G_1, \ldots, G_t \in R[Y_1, \ldots, Y_n]$. We are going to show a method for computing $G_t, \ldots, G_2$. The last step of computing G_1 can be done applying *Vermeidung von Divisionen*.

As we said before, our method "carries on" the occurring divisions by non–constant polynomials until the last moment. In this way, we obtain sequences of polynomials $\widetilde{G}_1, \ldots, \widetilde{G}_t$ in $R[Y_1, \ldots, Y_n]$ and $\widetilde{\Theta}_1, \ldots, \widetilde{\Theta}_t$ in $R[Y_1, \ldots, Y_n]$ such that the following identities hold for $2 \leq i \leq t$:

$$G_i = \frac{\widetilde{G}_i}{\widetilde{\Theta}_i}. \tag{29}$$

Then, applying Strassen's *Vermeidung von Divisionen* technique as stated in Lemma 20 together with the degree bound stated in Section 6.1 before will be sufficient to obtain a straight–line program of appropriate size and parameters which evaluates polynomials $g_1, \ldots, g_t \in R[Y_1, \ldots, Y_n]$ and a non–zero constant $a \in R \setminus \{0\}$ such that for $1 \leq i \leq t$ holds :

$$G_i = a^{-1} \cdot g_i, \tag{30}$$

where for $i = 1$ simply holds $\widetilde{\Theta}_1 = f_1$ and $\widetilde{G}_i = Q_1$. From this, the complexity estimates of Theorem 1 follow immediately.

Denominators in tensor matrices We are now interested in the description of the tensor matrices, i.e. the matrices in the basis $\{1, \bar{u}_i, \ldots, \bar{u}_i^{D_i-1}\}$ of the endomorphisms : $\eta_{Y_j} : B'_i \to B'_i$ for $1 \leq i \leq t-1, n-i+1 \leq j \leq n$. We have the following Lemma :

Lemma 55 *With the same notations and assumptions as before, there exists a non–scalar straight–line program of size $(ndL\delta)^{O(1)}$ and parameters in $\mathcal{F} \cup \{z \in \mathbb{Z} : |z| \leq (ndL\delta)^c\}$, such that the straight–line program evaluates the following polynomials :*

i) for every $i, 1 \leq i \leq t-1$, polynomials $\rho^{(i)} \in R[Y_1, \ldots, Y_{n-i}]$,

ii) for every $i, 1 \leq i \leq t-1$, and every $j, n-i+1 \leq j \leq n$, Γ'' evaluates the entries in $R[Y_1, \ldots, Y_{n-i}]$ of some $D_i \times D_i$ matrices $\mathcal{M}_{Y_j}^{(i)}$.

These polynomials verify that for every $i, 1 \leq i \leq t-1$, and every $j, n-i+1 \leq j \leq n$, the matrix $(\rho^{(i)})^{-1}\mathcal{M}_{Y_j}^{(i)}$ is the matrix of the endomorphisms $\eta_{Y_j} : B'_i \to B'_i$ in the basis $\{1, \bar{u}_i, \ldots, \bar{u}_i^{D_i-1}\}$.

Proof.– This follows by an argument similar to the one of Lemma 21. We first observe that the tensor matrices of multiplication by Y_j are given by

$$M_{Y_j}^{(i)} = (\rho_j^{(i)})^{-1} v_j^{(i)}(M_{u_i}),$$

where M_{u_i} is the companion matrix of the polynomial $\alpha_i^{-1} \cdot p_i \in A_i[T]$. Let us assume that

$$v_j^{(i)} := \sum_{k=0}^{D_i-1} a_{j,k}^{(i)} T^k \text{ with } a_{j,k}^{(i)} \in R[Y_1, \ldots, Y_{n-i}]$$

and let us define the polynomial $w_j^{(i)} := \sum_{k=0}^{D_i-1} a_{j,k}^{(i)} \alpha_i^{D_i-k-1} T^k$. The tensor matrix may then be seen as $M_{Y_j}^{(i)} = (\rho_j^{(i)})^{-1} \cdot \alpha_i^{-1} \cdot w_j^{(i)}(\alpha_i M_{u_i})$. Defining

$$\rho^{(i)} := \prod_{j=n-i+1}^{n} (\rho_j^{(i)} \alpha_i) \text{ and } \mathcal{M}_{Y_j}^{(i)} := \prod_{\substack{k=n-i+1 \\ k \neq j}}^{n} w_j^{(i)}(\alpha_i M_{u_i}),$$

we have $M_{Y_j}^{(i)} = (\rho_j^{(i)})^{-1}\mathcal{M}_{Y_j}^{(i)}$ and these obviously verify the desired conditions. ∎

Denominators of the homothesy matrices We are interested in the description of the denominators of the matrices describing the multiplication by elements in B_i.

Lemma 56 *With the previous notations and assumptions, let g be a polynomial in $R[Y_1, \ldots, Y_n]$ evaluable by a non–scalar straight–line program Γ_1 of size L_1 and parameters in $\mathcal{F}_1$. Then, there exists a non–scalar straight–line program Γ_g of size $(nd(L+L_1)\delta)^{O(1)}$ and parameters in $\mathcal{F} \cup \mathcal{F}_1 \cup \{z \in \mathbb{Z} : |z| \leq (ndL\delta)^c\}$ such that Γ_g evaluates*

- *a polynomial $\Theta_g^{(i)} \in R[Y_1, \ldots, Y_{n-i}] \setminus \{0\}$ and*
- *the entries in $R[Y_1, \ldots, Y_{n-i}]$ of a $D_i \times D_i$ matrix $\mathcal{M}_g^{(i)}$ such that :*

the matrix $M_g^{(i)}$ is given by $M_g^{(i)} = (\Theta_g^{(i)})^{-1} \cdot \mathcal{M}_g^{(i)}$.

If $g \in R[Y_1, \ldots, Y_n]$ is not a zero divisor in B_i (and B'_i), the matrix $M_g^{(i)}$ is a regular matrix. Thus, we are also interested in the computation of its inverse matrix, $(M_g^{(i)})^{-1}$.

Lemma 57 *With the notations and assumptions of the previous Lemma, if the polynomial* $g \in R[Y_1, \ldots, Y_n]$ *is not a zero divisor in* B_i*, there exists a non–scalar straight–line program* $\Gamma = (\Gamma_g^{(i)})^{-1}$ *of size* $(nd(L+L_1)\delta)^{O(1)}$ *and parameters in* $\mathcal{F} \cup \mathcal{F}_1 \cup \{z \in \mathbb{Z} : |\, z \,| \leq (ndL\delta)^c\}$ *such that* Γ *evaluates*

- *a polynomial* $\widetilde{\Theta}_g^{(i)} \in R[Y_1, \ldots, Y_{n-i}] \setminus \{0\}$ *and*
- *the entries in* $R[Y_1, \ldots, Y_{n-i}]$ *of a* $D_i \times D_i$ *matrix* $\widetilde{\mathcal{M}}_g^{(i)}$ *such that :*

the inverse matrix $(M_g^{(i)})^{-1}$ *may be obtained as* $(M_g^{(i)})^{-1} = (\widetilde{\Theta}_g^{(i)})^{-1} \cdot \widetilde{\mathcal{M}}_g^{(i)}$.

Proof.– First, we have the identity $M_g^{(i)} = (\Theta_g^{(i)})^{-1} \cdot \mathcal{M}_g^{(i)}$ with the bounds of the previous Lemma 56. Let $\det_g$ be the determinant of $\mathcal{M}_g^{(i)}$ and let Adj_g be the transposed of the adjoint matrix of $\mathcal{M}_g^{(i)}$. Then, we have :

$$(M_g^{(i)})^{-1} = (\det_g)^{-1} \cdot \Theta_g^{(i)} \cdot Adj_g$$

and thus, defining $\widetilde{\Theta}_g^{(i)} := (\det_g)$ and $\widetilde{\mathcal{M}}_g^{(i)} := \Theta_g^{(i)} \cdot Adj_g$ we conclude the proof. ■

Let us observe that for a given polynomial $\theta \in B_i[Y_{n-i+1}, \ldots, Y_n]$ the endomorphism

$$\eta_\theta : B_i'[Y_{n-i+1}, \ldots, Y_n] \to B_i'[Y_{n-i+1}, \ldots, Y_n]$$

represented in the basis $\{1 \otimes 1, \bar{u}_i \otimes 1, \ldots, \bar{u}_i^{D_i - 1} \otimes 1\}$ is given by the matrix $M_\theta^{(i)}$.

Lemma 58 *With the same notations and assumptions, let be given a polynomial* $\theta \in B_i[Y_{n-i+1}, \ldots, Y_n]$ *which can be evaluated by a non–scalar straight–line program* Γ_2 *of size* L_2 *and parameters in* $\mathcal{F}_2$*. Then, there exists a non–scalar straight–line program* Γ_θ *of size* $(nd(L+L_2)\delta)^{O(1)}$ *and parameters in* $\mathcal{F} \cup \mathcal{F}_2 \cup \{z \in \mathbb{Z} : |\, z \,| \leq (ndL\delta)^c\}$ *such that* Γ_θ *evaluates*

- *a polynomial* $\Theta_\theta^{(i)} \in R[Y_1, \ldots, Y_{n-i}]$ *and*
- *the entries in* $R[Y_1, \ldots, Y_n]$ *of a* $D_i \times D_i$ *matrix* $\mathcal{M}_\theta^{(i)}$ *such that :*

the matrix $M_\theta^{(i)}$ *may be obtained as* $M_\theta^{(i)} := (\Theta_\theta^{(i)})^{-1} \cdot \mathcal{M}_\theta^{(i)}$.

Proof.– Let us simply observe that :

$$M_\theta^{(i)} = \theta(Y_1, \ldots, Y_{n-i}, (\rho^{(i)})^{-1}\mathcal{M}_{Y_{j-i+1}}^{(i)}, \ldots, (\rho^{(i)})^{-1}\mathcal{M}_{Y_n}^{(i)}, Y_{n-i+1}, \ldots, Y_n)$$

and apply the technical tool of Lemma 21 as before to compute matrices and denominators separately. ■

Dependence on the input system These notations fixed, let us see how to compute our polynomials $G_1, \ldots, G_t$. We introduce the following additional notation for the entities we will compute (which will depend only on the input system $f_1, \ldots, f_t$) :

- for $1 \leq i \leq t-1$ the polynomial

$$\Theta^{(i)} := \widetilde{\Theta}_{J_{i-1}}^{(i-1)} \cdot \widetilde{\Theta}_{f_i}^{(i-1)} \cdot \Theta_f^{(i-1)} \cdot \Theta_{\Delta_1^{(i-1)}}^{(i-1)} \in R[Y_1, \ldots, Y_{n-i+1}],$$

- the matrices with entries in $R[Y_1, \ldots, Y_n]$ for $1 \leq i \leq t-1$:

$$\mathcal{M}^{(i)} := \widetilde{\mathcal{M}}_{J_{i-1}}^{(i-1)} \cdot \widetilde{\mathcal{M}}_{f_i}^{(i-1)} \cdot \mathcal{M}_f^{(i-1)} \cdot \mathcal{M}_{\Delta_1^{(i-1)}}^{(i-1)},$$

- for $1 \leq i \leq t-1$ and $i+1 \leq j \leq t$, the polynomials :

$$\Theta_j^{(i)} := \widetilde{\Theta}_{J_{i-1}}^{(i-1)} \cdot \widetilde{\Theta}_{f_i}^{(i-1)} \cdot \Theta_{f_j}^{(i-1)} \cdot \Theta_{\Delta_1^{(i-1)}}^{(i-1)} \in R[Y_1, \ldots, Y_{n-i+1}],$$

- for $1 \leq i \leq t-1$ and $i+1 \leq j \leq t$, the matrices with entries in $R[Y_1, \ldots, Y_n]$ given by :

$$\mathfrak{M}_j^{(i)} := \widetilde{\mathcal{M}}_{J_{i-1}}^{(i-1)} \cdot \widetilde{\mathcal{M}}_{f_i}^{(i-1)} \cdot \mathcal{M}_{f_j}^{(i-1)} \cdot \mathcal{M}_{\Delta_1^{(i-1)}}^{(i-1)},$$

- for $1 \leq i \leq t-1$, let $P_i \in R[Y_1, \ldots, Y_n]$ be the polynomial given by

$$P_i := \widetilde{Tr}_i'(\mathcal{M}^{(i)}).$$

Observe the following relevant fact which helps us to avoid the *Pasodoble* effect : the information $\Theta^{(i)}, \mathcal{M}^{(i)}, \Theta_j^{(i)}$ and $\mathcal{M}_j^{(i)}$ is independent of the intermediate results $G_1, \ldots, G_t, Q_1, \ldots, Q_t$. This leads us to the following Lemmata showing how to compute the polynomials $G_1, \ldots, G_t$.

Lemma 59 *With the previous notations and assumptions, for $j \geq i+1$ let $M_{G_j}^{(i)}$ be the matrix associated to the endomorphism $\eta_{G_j} : B_i' \to B_i'$. Then, the following identities hold :*

$$G_t = (\Theta^{(t-1)})^{-1} P_{t-1},$$

and for every $2 \leq i \leq t-1$:

$$G_i = (\Theta^{(i-1)})^{-1} P_{i-1} - \sum_{j=i+1}^{t} (\Theta_j^{(i-1)})^{-1} \widetilde{\mathrm{Tr}}_{i-1}'(\mathfrak{M}_j^{(i-1)} \cdot M_{G_j}^{(i-1)}).$$

Proof.– Observe that the following identities hold :

$$G_t = \widetilde{Tr}_{t-1}((M_{J_{t-1}}^{(t-1)})^{-1} \cdot (M_{f_t}^{(t-1)})^{-1} \cdot M_f^{(t-1)} \cdot M_{\Delta_1^{(t-1)}}^{(t-1)}),$$

$$\begin{aligned} G_i &= \widetilde{Tr}_{i-1}((M_{J_{i-1}}^{(i-1)})^{-1} \cdot (M_{f_i}^{(i-1)})^{-1} \cdot M_f^{(i-1)} \cdot M_{\Delta_1^{(i-1)}}^{(i-1)} \\ &\quad - \sum_{j=i+1}^{t} \widetilde{Tr}_{i-1}'((M_{J_{i-1}}^{(i-1)})^{-1} \cdot (M_{f_i}^{(i-1)})^{-1} \cdot M_{G_j}^{(i-1)} \cdot M_{f_j}^{(i-1)} \cdot M_{\Delta_1^{(i-1)}}^{(i-1)}). \end{aligned}$$

■

At this stage let us consider the entries of the matrices $\mathfrak{M}_j^{(i)}$. For $1 \leq i \leq t-1$ and $i+1 \leq j \leq t$, let $\mathfrak{M}_j^{(i)}$ be $(\mathfrak{m}_{k,l}^{(i,j)})_{1 \leq k,l \leq D_i}$ with $\mathfrak{m}_{k,l}^{(i,j)} \in R[Y_1, \ldots, Y_n]$.
According to Lemma 59 we can compute the following list of information :

Lemma 60 *With the previous notations and assumptions, there exists a non–scalar straight–line program Γ of size $(tdL\delta)^{O(1)}$ and parameters in*

$$\mathcal{F} \cup \{z \in \mathbb{Z} : |\, z \,| \leq (tdL\delta)^c\}$$

such that Γ evaluates the following polynomials :

- *the polynomials $\Theta^{(i)}$ for $1 \leq i \leq t-1$,*

- *the polynomials* $\Theta_j^{(i)}$ *for* $1 \leq i \leq t-1$ *and* $i+1 \leq j \leq t$,
- *the entries of the matrices* $\mathfrak{M}_j^{(i)}$ *for* $1 \leq i \leq t-1$ *and* $i+1 \leq j \leq t$, *and*
- *the polynomials* P_i *for* $1 \leq i \leq t-1$

verifying the conditions of Lemma 59 above.

Proof.– Observe that all this information is obtained by evaluating some polynomials f_i, f, J_i of $\Delta_1^{(i)}$ in the corresponding tensor matrices, which only depend on the input (i.e. $f_1, \ldots, f_t, f$) and not on the intermediate results $G_1, \ldots, G_t, Q_1, \ldots, Q_t$. ∎

Isolating the variable parts Let us consider for $1 \leq i \leq t-1$ and $i+1 \leq j \leq t$ the matrices $M_{G_j}^{(i)}$ whose entries are in F_i. Let us denote the entries of the matrices $M_{G_j}^{(i)}$ as follows :

$$M_{G_j}^{(i)} := (z_{k,l}^{(i,j)})_{1 \leq k,l \leq D_i}.$$

We have the following identities.

Proposition 61 *With the previous notations and assumptions, we have*

$$G_t = (\Theta^{(t-1)})^{-1} \cdot P_{t-1}$$

and for $2 \leq i \leq t-1$ *holds*

$$G_i = (\Theta^{(i-1)})^{-1} \cdot P_{i-1} - \sum_{j=i+1}^{t} (\Theta_j^{(i-1)})^{-1} \Big(\sum_{k=1}^{D_{i-1}} \Big(\sum_{l=1}^{D_{i-1}} \mathfrak{m}_{k,l}^{(i-1,j)} \cdot z_{l,k}^{(i-1,j)} \Big) \Big).$$

Proof.– Observe simply that in the expression $\widetilde{Tr}'_{i-1}(\mathfrak{M}_j^{(i-1)} \cdot M_{G_j}^{(i-1)})$ holds :

$$\mathfrak{M}_j^{(i-1)} \cdot M_{G_j}^{(i-1)} = \left(\sum_{l=1}^{D_{i-1}} \mathfrak{m}_{k,l}^{(i-1,j)} \cdot z_{l,\lambda}^{(i-1,j)} \right)$$

for $1 \leq k, \lambda \leq D_{i-1}$. ∎

Carrying on denominators Additionally, we have to introduce the matrices :

- for $1 \leq i \leq t-1$ and $r \leq i$, let us denote

$$M_{P_i}^{(r)} := P_i(Y_1, \ldots, Y_{n-r}, (\rho^{(r)})^{-1} \mathcal{M}_{Y_{n-r+1}}^{(r)}, \ldots, (\rho^{(r)})^{-1} \mathcal{M}_{Y_n}^{(r)}),$$

- for $1 \leq i \leq t-1$, $i+1 \leq j \leq t$, $r \leq i$ and $1 \leq k, l \leq D_{i-1}$ we consider :

$$M_{k,l}^{(i,j,r)} := M_{\mathfrak{m}_{k,l}^{(i,j)}}^{(r)} = \mathfrak{m}_{k,l}^{(i,j)}(Y_1, \ldots, Y_{n-r}, (\rho^{(r)})^{-1} \mathcal{M}_{Y_{n-r+1}}^{(r)}, \ldots, (\rho^{(r)})^{-1} \mathcal{M}_{Y_n}^{(r)}).$$

We have the following Lemma :

Lemma 62 *With the same notations and assumptions as before, there exists a non–scalar straight–line program* $\widetilde{\Gamma}$ *of size* $(tdL\delta)^{O(1)}$ *and parameters in* $\mathcal{F} \cup \{z \in \mathbb{Z} : |z| \leq (tdL\delta)^c\}$ *such that* $\widetilde{\Gamma}$ *evaluates the following polynomials :*

i) for $1 \leq i \leq t-1$ *and* $r \leq i$ *polynomials* $\alpha_i^{(r)} \in R[Y_1, \ldots, Y_{n-r}]$,

ii) for $1 \leq i \leq t-1$, $i+1 \leq j \leq t$, $r \leq i$ *polynomials* $\beta^{(i,r)} \in R[Y_1, \ldots, Y_{n-r}]$,

iii) for $1 \leq i \leq t-1$, $i+1 \leq j \leq t$ *and* $r \leq i$ *the entries in* $R[Y_1, \ldots, Y_{n-r}]$ *of some* $D_r \times D_r$ *matrices* $\mathfrak{M}_{P_i}^{(r)}$,

iv) for every i, j, k, l, r *with* $3 \leq j \leq t$, $i+1 \leq j$, $r \leq i$ *and* $1 \leq k, l \leq D_i$ *the entries* $\mathfrak{m}_{k,l}^{(i,j,r)}$ *in* $R[Y_1, \ldots, Y_{n-r}]$ *of some* $D_r \times D_r$ *matrices* $\mathfrak{M}_{k,l}^{(i,j,r)}$

verifying the following identities :

$$M_{P_i}^{(r)} = (\alpha_i^{(r)})^{-1} \cdot \mathfrak{M}_{P_i}^{(r)}, \qquad M_{k,l}^{(i,j,r)} = (\beta_j^{(i,r)})^{-1} \cdot \mathfrak{M}_{k,l}^{(i,j,r)}.$$

Proof.– Again we apply Lemma 21, noting that all the wanted information (i.e. the straight–line program that evaluates P_j and $\mathcal{M}_{k,l}^{(i,j)}$ and the geometric solution of the intermediate varieties $V(f_1, \ldots, f_i)$, $1 \leq i \leq t-1$) does not depend on the quotients G_j to be computed. ∎

The straight–line programs $\mathfrak{M}_i$ Now, we have established the following recurrence rules to compute the homothesy matrices $M_{G_i}^{(r)}$:

Lemma 63 *With the same notations and assumptions, we obtain that for* $r \leq t-1$ *holds :*

$$M_{G_t}^{(r)} = (\Theta^{(t-1)})^{-1} (\alpha_{t-1}^{(r)})^{-1} \cdot \mathfrak{M}_{P_{t-1}}^{(r)}$$

and for $1 \leq i \leq t-1$ *and* $r \leq i-1$ *holds :*

$$\begin{aligned} M_{G_i}^{(r)} &= (\Theta^{(i-1)})^{-1} (\alpha_{i-1}^{(r)})^{-1} \cdot \mathfrak{M}_{P_{i-1}}^{(r)} \\ &\quad - \sum_{j=i+1}^{t} (\Theta_j^{(i-1)})^{-1} \Big(\sum_{k=1}^{D_{i-1}} \Big(\sum_{l=1}^{D_{i-1}} (\beta_j^{(i-1,r)})^{-1} \mathfrak{M}_{k,l}^{(i-1,j,r)} \cdot z_{l,k}^{(i-1,j)} \Big) \Big). \end{aligned}$$

Proof.– This follows simply by applying the previous identity, noting that $z_{l,k}^{(i-1,j)} \in F_{i-1} \subseteq F_r$. ∎

With this, we have explained how to compute straight–line programs evaluating only from the input system $f_1, \ldots, f_t$ the parts of the polynomials $G_1, \ldots, G_t$ which we refered to as "coefficient" parts in the sketch of proof on page 49. We conclude from the above discussion the following :

Proposition 64 (Output of the straight–line programs $\mathfrak{M}_i$) *There exists a non–scalar straight–line program* Γ *of size* $(tdL\delta)^{O(1)}$ *and parameters in* $\mathcal{F} \cup \{z \in \mathbb{Z} : |z| \leq (tdL\delta)^c\}$ *such that* Γ *evaluates directly (i.e. from the input polynomials* $f_1, \ldots, f_t, f$ *and the geometric solutions of the intermediate varieties* $V_i = V(f_1, \ldots, f_i)$ *for* $1 \leq i \leq t-1$*) the following information :*

- $\Theta^{(i)} \in R[Y_1, \ldots, Y_{n-i+1}]$ *for* $1 \leq i \leq t-1$,
- $\Theta_j^{(i)} \in R[Y_1, \ldots, Y_{n-i+1}]$ *for* $1 \leq i \leq t-1$ *and* $i+1 \leq j \leq t$,
- $P_i \in R[Y_1, \ldots, Y_n]$ *for* $1 \leq i \leq t-1$,
- *the entries* $\mathfrak{m}_{k,l}^{(i,j)} \in R[Y_1, \ldots, Y_n]$ *of the matrices* $\mathfrak{M}_j^{(i)}$ *for* $1 \leq i \leq t-1$, $i+1 \leq j \leq t$ *and* $1 \leq k, l \leq D_i$,

- $\alpha_i^{(r)} \in R[Y_1, \ldots, Y_{n-r}]$ *for* $1 \leq i \leq t-1$ *and* $r \leq i$,
- $\beta_j^{(i,r)} \in R[Y_1, \ldots, Y_{n-r}]$ *for* $1 \leq i \leq t-1$, $i+1 \leq j \leq t$ *and* $r \leq i$,
- *the entries in* $R[Y_1, \ldots, Y_{n-r}]$ *of the matrices* $\mathfrak{M}_{P_i}^{(r)}$ *for* $1 \leq i \leq t-1$ *and* $r \leq i$, *and finally*
- *the entries in* $R[Y_1, \ldots, Y_{n-r}]$ *of the matrices* $\mathfrak{M}_{k,l}^{(i,j,r)}$ *for* $1 \leq i \leq t-1$, $i+1 \leq j \leq t$, $r \leq i$ *and* $1 \leq k, l \leq D_i$,

verifying :

$$G_t = (\Theta^{(t-1)})^{-1} P_{t-1} \text{ and } M_{G_t}^{(r)} = (\Theta^{(t-1)})^{-1} \cdot (\alpha_{t-1}^{(r)})^{-1} \mathfrak{M}_{P_{t-1}}^{(r)}.$$

and for $2 \leq i \leq t-1$

$$G_i = (\Theta^{(i-1)})^{-1} \cdot P_{i-1} - \sum_{j=i+1}^{t} (\Theta_j^{(i-1)})^{-1} \cdot \Big(\sum_{k=1}^{D_{i-1}} \Big(\sum_{l=1}^{D_{i-1}} \mathfrak{m}_{k,l}^{(i-1,j)} \cdot z_{k,l}^{(i-1,j)} \Big) \Big),$$

$$\begin{aligned} M_{G_i}^{(r)} &= (\Theta^{(i-1)})^{-1} (\alpha_{i-1}^{(r)})^{-1} \cdot \mathfrak{M}_{P_{i-1}}^{(r)} \\ &\quad - \sum_{j=i+1}^{t} (\Theta_j^{(i-1)})^{-1} \Big(\sum_{k=1}^{D_{i-1}} \Big(\sum_{l=1}^{D_{i-1}} (\beta_j^{(i-1,r)})^{-1} \mathfrak{M}_{k,l}^{(i,j,r)} \cdot z_{l,k}^{(i-1,j)} \Big) \Big) \end{aligned}$$

such that $f - (G_t f_t + \cdots + G_i f_i) \in (f_1, \ldots, f_{i-1})$ *holds.*

The straight–line programs $\mathfrak{M}_i$ compute for $1 \leq i \leq t-1$ the items listed in Proposition 64 verifying the above recurrence rules for G_i and $M_{G_i}^{(r)}$. The total complexity of the straight–line programs $\mathfrak{M}_i$ is $(tdL\delta)^{O(1)}$.

This shows how the influence of the previously computed polynomials G_j for $j \geq i+1$ depends on the polynomials $\mathfrak{m}_{k,l}^{(i-1,j)}$ and less on the entries $z_{k,l}^{(i-1,j)}$ of the matrices $M_{G_j}^{(i-1)}$.

The straight–line programs Γ_i From the recurrence rules resumed in Proposition 64 above we also obtain a way for computing the entries $z_{k,l}^{(i-1,j)}$ of the matrices $M_{G_j}^{(i-1)}$, which will be done by the straight–line programs Γ_i.

We explain how to compute from the information contained in the straight–line programs $\mathfrak{M}_i$ the polynomial G_i and how to "carry on" the denominators of G_i and the matrices $M_{G_i}^{(r)}$.

We define from the output of the straight–line program of Proposition 64 :

$$\zeta_t^{(r)} := (\Theta^{(t-1)}) \cdot \alpha_{t-1}^{(r)} \in R[Y_1, \ldots, Y_{n-r}]$$

and we denote by $\mu_{k,l}^{(r,t)} \in R[Y_1, \ldots, Y_{n-r}]$ the entries of the matrix $\mathfrak{M}_{P_{t-1}}^{(r)}$. From this we obtain denominators

$$z_{k,l}^{(r,t)} = (\zeta_t^{(r)})^{-1} \cdot \mu_{k,l}^{(r,t)}.$$

Then, we have

$$G_t = (\Theta^{(t-1)})^{-1} P_{t-1}, \qquad M_{G_t}^{(r)} = (\zeta_t^{(r)})^{-1} \cdot \mu_{k,l}^{(r,t)}, \qquad \mathfrak{M}_{G_t}^{(r)} := (\mu_{k,l}^{(r,t)})_{1 \leq k,l \leq D_r}.$$

Now, let us suppose we already have computed inductively $G_t, \ldots, G_{i+1}$ and for $i+1 \leq j \leq t$, $r \leq j-1$ and $1 \leq k, l \leq D_r$ the polynomials $\zeta_j^{(r)}$ and $\mu_{k,l}^{(r,j)}$ in $R[Y_1, \ldots, Y_{n-r}]$ such that the following holds :

$$z_{k,l}^{(r,j)} = (\zeta_j^{(r)})^{-1} \cdot \mu_{k,l}^{(r,j)}, \qquad M_{G_j}^{(r)} = (\zeta_j^{(r)})^{-1} \cdot \mu_{k,l}^{(r,j)}, \qquad \mathfrak{M}_{G_j}^{(r)} = (\mu_{k,l}^{(r,j)}).$$

Then, for $r \leq i$ the polynomial G_i and the matrices $M_{G_i}^{(r)}$ can be computed by the following recurrence rule for the polynomials $\zeta_j^{(i-1)}$ and $\mu_{k,l}^{(i-1,j)}$:

$$\begin{aligned} G_i &= (\Theta^{(i-1)})^{-1} \cdot P_{i-1} && (31) \\ &\quad - \sum_{j=i+1}^{t} (\Theta_j^{(i-1)})^{-1} \cdot \Big(\sum_{k=1}^{D_{i-1}} \Big(\sum_{l=1}^{D_{i-1}} \mathfrak{m}_{k,l}^{(i-1,j)} \cdot (\zeta_j^{(i-1)})^{-1} \cdot \mu_{k,l}^{(i-1,j)} \Big) \Big), && (32) \end{aligned}$$

$$\begin{aligned} M_{G_i}^{(r)} &= (\Theta^{(i-1)})^{-1} \cdot (\alpha_{i-1}^{(r)})^{-1} \mathfrak{M}_{P_{i-1}}^{(r)} - \sum_{j=i+1}^{t} (\Theta_j^{(i-1)})^{-1} \cdot && (33) \\ &\quad \cdot \Big(\sum_{k=1}^{D_{i-1}} \Big(\sum_{l=1}^{D_{i-1}} (\beta_j^{(i-1,r)})^{-1} \mathfrak{M}_{k,l}^{(i,j,r)} (\zeta_j^{(i-1)})^{-1} \cdot \mu_{l,k}^{(i-1,j)} \Big) \Big). && (34) \end{aligned}$$

Let us observe that we have used only the information contained in Proposition 64 plus the denominators $\zeta_j^{(i-1)}$ and the polynomials $\mu_{k,l}^{(i-1,j)}$ computed by the recurrence rules.

Carrying on separately the denominators appearing in the above recurrence rules (31) and (33), we can obtain polynomials $\mu_{k,l}^{(r,i)} \in R[Y_1, \ldots, Y_{n-r}]$ for $r \leq i-1$ and $1 \leq k, l \leq D_r$ as well as $\zeta_i^{(r)} \in R[Y_1, \ldots, Y_{n-r}]$ such that the following holds :

$$\mathfrak{M}_{G_i}^{(r)} = (\mu_{k,l}^{(r,i)})_{1 \leq k,l \leq D_r} \text{ and for } r \leq i \qquad M_{G_i}^{(r)} = ((\zeta_i^{(r)})^{-1} \cdot \mathfrak{M}_{G_i}^{(r)}.$$

These recurrence rules yield now a way to compute the polynomials G_i :

Proposition 65 *The straight–line program Γ_i evaluates from the information evaluated by the straight–line programs Γ (the polynomials $f_1, \ldots, f_t$), $\mathfrak{M}_{t-1}, \ldots, \mathfrak{M}_i$ and Γ_{i+1} the following list of items :*

- *for $i \leq j \leq t$ and $r \leq i$ the polynomials $\zeta_j^{(r)}$ and*
- *for $i \leq j \leq t, r \leq i$ and $1 \leq k, l \leq D_r$ polynomials $\mu_{k,l}^{(r,j)} \in R[Y_1, \ldots, Y_n]$*

such that, if we define for $i \leq j \leq t$

$$\mathfrak{M}_{G_j}^{(r)} = (\mu_{k,l}^{(r,j)})_{1 \leq k,l \leq D_r}$$

the following identity holds :

$$M_{G_j}^{(r)} = (\zeta_j^{(r)})^{-1} \cdot \mathfrak{M}_{G_j}^{(r)}.$$

Furthermore, the straight–line program Γ_i evaluates the polynomials

- $\mathfrak{m}_{k,l}^{(i-1,j)}$ *for $i+1 \leq j \leq t$ and $1 \leq k, l \leq D_i$,*
- $\mu_{k,l}^{(i-1,j)}$ *for $i+1 \leq j \leq t$ and $1 \leq k, l \leq D_i$,*
- $\widetilde{\Theta}_i := \Theta^{(i-1)} \cdot \prod_{j=i+1}^{t} \Theta_j^{(i-1)} \cdot \prod_{j=i+1}^{t} \zeta_j^{(i-1)}$
- *and the polynomials $\widetilde{P}_{i-1} := \frac{\widetilde{\Theta}_i}{\Theta^{(i-1)}} \cdot P_{i-1}$,*

such that defining

$$\widetilde{\mathfrak{m}}_{k,l}^{(i-1,j)} := \mathfrak{m}_{k,l}^{(i-1,j)} \cdot \mu_{k,l}^{(i-1,j)} \cdot \frac{\widetilde{\Theta}_i}{\Theta^{(i-1)} \cdot \zeta_j^{(i-1)}},$$

the following holds :

$$\widetilde{G}_i = \widetilde{P}_{i-1} - \sum_{j=i+1}^{t} (\sum_{k=1}^{D_{i-1}} (\sum_{l=1}^{D_{i-1}} \widetilde{\mathfrak{m}}_{k,l}^{(i-1,j)})).$$

The iteration step has to be performed t times and hence the total complexity for the straight–line programs Γ_i is $(t\delta)^{O(1)}$ for each inductive step for $2 \leq i \leq t$.

Noting that $\frac{\widetilde{G}_i}{\widetilde{\Theta}_i} = G_i$ holds, we apply Strassen's *Vermeidung von Divisionen* method (cf. Proposition 20) to obtain from the combination of the straight–line programs $\mathfrak{M}_i$ and the straight–line programs Γ_i a division free non–scalar straight–line program evaluating the polynomials G_i.

Thus, we obtain a total complexity of order $(tdL\delta)^{O(1)}$. This concludes the proof of Theorem 1. ∎

7 Proof of Theorem 2

The present Section 7 contains the proofs of Theorem 2 and the Corollaries from the Introduction.

In what follows, we are going to show an alternative method for the computation of the polynomials $a^{-1}g_1, \ldots, a^{-1}g_t$ of Theorem 1. This alternative method induces a major growth of the output size (and hence of the complexity of this procedure) but permits a better control of the non–scalar depth of the straight–line program describing the output. In fact, we are going to compute polynomials $h_1, \ldots, h_t \in R[X_1, \ldots, X_n]$ and a non–zero constant $b \in R \setminus \{0\}$ such that

$$a^{-1}g_i = b^{-1}h_i \text{ for } 1 \leq i \leq t,$$

where the non–zero integer a and the polynomials $g_1, \ldots, g_t$ are precisely those computed by the algorithm given in the proof of Theorem 1. The proof of Theorem 2 here uses mainly Tate's trace formula which involves all monomials up to a certain degree ($(t-1)d$ in the worst case) and this implies the growth of the size. Conversely, this reduces the division procedures to an iterated matrix product (which was already considered in [43] and [44]). The reason for starting with the elimination polynomial (and not with the input polynomials) is mainly based on the fact that Newton's method for complete local rings (as used in [25]) is not well-parallelizable. In contrast, this yields bounds for the height of the resulting polynomials which depend almost polynomially on the height and the degree of the intermediate varieties $V(f_1, \ldots, f_i)$.

As we are going to compute the same polynomials (up to a non–zero constant) the degree bound follows from the discussion put forward in Section 6.1.

7.1 The non–scalar depth bound

We assume the same conditions as those given at the beginning of Section 6. To recapitulate, let us denote by $N \in \mathcal{M}_n(\mathbb{Z})$ a linear change of coordinates such that :

i) the variables $Y_1, \ldots, Y_n$ given by

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = N \cdot \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$$

are in Noether position with respect to the sequence of intermediate varieties $V(f_1, \ldots, f_i)$ for $0 \leq i \leq t-1$. In other words,

$$A_i := K[Y_1, \ldots, Y_{n-i}] \hookrightarrow B_i := K[X_1, \ldots, X_n]/(f_1, \ldots, f_i)$$

is an integral ring extension for $0 \leq i \leq t-1$. Let us observe that $A_0 = B_0$ and $V_0 = V((0))$ holds.

ii) The matrix $N = (n_{ij})_{1 \leq i,j \leq n}$ describing the Noether position has coefficients $n_{ij} \in \mathbb{Z}$ of bounded height $| n_{ij} | \leq (ndL\delta)^c$.

iii) For every $i, 1 \leq i \leq t-1$ we have the elimination polynomial

$$\mathfrak{m}_i \in R[Y_1, \ldots, Y_{n-i}, U_{n-i+1}, \ldots, U_n][T].$$

In fact, $\mathfrak{m}_i$ has the form $\mathfrak{m}_i := \alpha_i \cdot T^{D_i} + h_i$, with $\alpha_i \in R \setminus \{0\}$, degree $D_i = rk_{A_i} B_i$ and degree in T $\deg_T h_i \leq D_i - 1$. Moreover, the polynomial

$$\alpha_i^{-1} \cdot \mathfrak{m}_i \in K[Y_1, \ldots, Y_{n-i}, U_{n-i+1}, \ldots, U_n][T]$$

is the minimal equation over A_i of the generic projection

$$\mathcal{U}_i := U_{n-i+1} X_{n-i+1} + \cdots + U_n X_n.$$

We will write $\mathfrak{m}_0 = 1$ when necessary.

iv) As observed in Lemma 55 before, there exists a non–scalar straight–line program Γ of size $(td\delta)^{O(1)}$ and non–scalar depth $O(\log_2 d + \log_2 \delta)$ such that Γ computes from the coefficients (with respect to the variable T) of $\mathfrak{m}_i$ the following polynomials :

(a) for $1 \leq i \leq t-1$ non–zero polynomials $\rho^{(i)} \in R[Y_1, \ldots, Y_{n-i}]$,

(b) for $1 \leq i \leq t-1$ and $n-i+1 \leq j \leq n$ the entries in $R[Y_1, \ldots, Y_{n-i}]$ of a $D_i \times D_i$ matrix $\mathfrak{M}_j^{(i)}$,

such that the matrix of the endomorphism $\eta_{Y_j} : B_i \to B_i$ is given by $M_{Y_j}^{(i)} := (\rho^{(i)})^{-1} \mathfrak{M}_j^{(i)}$.

Let us remark that these matrices $\mathfrak{M}_j^{(i)}$ and polynomials $\rho^{(i)}$ are not exactly the same as those in the previous Section 6.2. Here we have explicitly chosen those who can be obtained from the elimination polynomial whereas in Section 6.2 they were given by the description of the primitive element. Nevertheless, as they are essentially the same objects just described in different ways, we preserved the notation introduced before.

Following the introduction of Section 6, let us consider for $1 \leq i \leq t-1$ the pseudo–jacobian determinant $\Delta^{(i)} \in B_i \otimes_{A_i} B_i$. Let us also consider the set $\mathcal{M}_i$ of all monomials of degree at most $i(d-1)$ in the variables $\{Y_{n-i+1}, \ldots, Y_n\}$. Let us denote by

$$\mathcal{M}_i := \{b_k^{(i)} : 1 \leq k \leq N_i\}$$

such a set, where N_i is the cardinality of $\mathcal{M}_i$. Then, there exist polynomials $a_k^{(i)} \in R[Y_1, \ldots, Y_n], 1 \leq k \leq N_i$ of total degree bounded by $i(d-1)$ such that

$$\Delta^{(i)} := \sum_{k=1}^{N_i} \bar{a}_k^{(i)} \otimes \bar{b}_k^{(i)} \in B_i \otimes_{A_i} B_i,$$

where $\bar{}$ denotes taking residual classes in B_i (as before). The case $i = 0$ yields $\Delta^{(0)} = 1 \otimes 1$.

Let $\sigma_i \in B_i^*$ be the trace associated to $\Delta^{(i)}$ by Tate's trace formula. Let us also consider F_i as the quotient field of A_i, $B_i' = F_i \otimes_{A_i} B_i$ and $\sigma_i' \to F_i$ the trace obtained from σ_i by extending scalars. For $i = 0$ we consider $\sigma_0 = \mathrm{Id} B_i, \sigma_o' = \mathrm{Id} B_0'$. Now, we have the following rule to compute the quotients :

$$G_t := \sum_{k=1}^{N_{t-1}} \sigma_{t-1}'(\bar{a}_k^{(t-1)} \cdot \bar{f}_t^{-1} \cdot \bar{f}) \cdot b_k^{(t)} \in R[X_1, \ldots, X_n], \qquad Q_t := f - G_t \cdot f_t.$$

As for $2 \leq i \leq t-1$, we have :

$$G_i := \sum_{k=1}^{N_{i-1}} \sigma'_{i-1}(\bar{a}_k^{(i-1)} \cdot \bar{f}_i^{-1} \cdot \bar{Q}_{i+1}) \cdot b_k^{(i-1)} \in R[X_1, \ldots, X_n], \qquad Q_i := Q_{i+1} - G_i \cdot f_i.$$

The case $i = 1$ is simply given by $G_1 = f_1^{-1} \cdot Q_2$. Now, we are going to transform this recurrence rule under the following terms : let β_i be the free A_i–module generated by the monomials in $\mathcal{M}_i$, and $\beta'_i := F_i \otimes_{A_i} B_i$. Let us consider $\pi_i : \beta_i \to B_i$ and $\pi'_i : \beta'_i \to B'_i$ the projections given by :

$$\pi'_i(C_1, \ldots, C_{N_i}) := \sum_{k=1}^{N_i} \bar{C}_k \cdot \bar{b}_k^{(i)} \in B'_i.$$

The following diagram obviously commutes for every $i, 1 \leq i \leq t-1$:

$$\begin{array}{ccccc} & \beta_i & \hookrightarrow & \beta'_i & \\ \pi_i & \downarrow & & \downarrow & \pi'_i \\ & B_i & \hookrightarrow & B'_i & \end{array}$$

The previous division procedure can be performed as follows : We are going to compute for every $i, 2 \leq i \leq t-1$ some elements of the free A_{i-1}–module β_{i-1} :

$$(C_1^{(i)}, \ldots, C_{N_{i-1}}^{(i)}) \in \beta_{i-1}$$

such that

$$G_i = \sum_{k=1}^{N_i} C_k^{(i)} \cdot \bar{b}_k^{(i-1)} \in K[Y_1, \ldots, Y_n].$$

In order to perform this task, let us observe the following facts :
For every $i, 1 \leq i \leq t-1$ let $f, g \in R[Y_1, \ldots, Y_n]$ be polynomials such that $\bar{f} \mid \bar{g}$ in B_i and $\bar{f}$ is not a zero divisor in B_i. Then, for every $a \in K[X_1, \ldots, X_n]$ we have that :

$$\sigma'_i(\bar{g} \cdot \bar{f}^{-1} \cdot \bar{a}) \in A_i.$$

The reason is simply the following : let $q \in K[Y_1, \ldots, Y_n]$ be such that $\bar{g} = \bar{f} \cdot \bar{q}$ in B_i. Then, since $\bar{f}^{-1} \in B'_i$, we have $\bar{f}^{-1} \cdot \bar{g} = \bar{q}$ in B'_i. Finally, $\sigma'_i(\bar{g} \cdot \bar{f}^{-1} \cdot \bar{a}) = \sigma_i(\bar{q} \cdot \bar{a}) \in A_i$. The polynomials $(C_1^{(i)}, \ldots, C_{N_{i-1}}^{(i)}) \in \beta_{i-1}$ are given by $C_j^{(i)} := \sigma'_{i-1}(\bar{a}_k^{(i-1)} \cdot \bar{f}_i^{-1} \cdot \bar{Q}_{i+1}) \in A_{i-1}$. Let us now consider the following sequence of objects :

- for $1 \leq i \leq t-1$ and $1 \leq k \leq N_i$:

$$d_k^{(i)} := \sigma'_i(f_{i+1}^{-1} \cdot a_k^{(i)}) \in K_i,$$

- for $1 \leq i \leq t-1$, $1 \leq k \leq N_i$, $1 \leq l \leq N_j$, $j \geq i-1$,

$$e_{k,l}^{(i,j)} := \sigma'_i(\bar{b}_t^{(j)} \cdot \bar{f}_{j+1} \cdot \bar{f}_{i+1}^{-1} \cdot b_k^{(i)}) \in K_i.$$

We consider now the following matrices and column vectors :

$$E^{(i,j)} := (e_{k,l}^{(i-1,j)})_{\substack{1 \leq k \leq N_{i-1} \\ 1 \leq l \leq N_j}}, \text{ and } D^{(i)} := (d_k^{(i-1)})_{1 \leq k \leq i-1}.$$

Now, suppose that we already computed the polynomials $G_t, \ldots, G_{r+1}$, where :

$$G_j := \sum_{k=1}^{N_{i-1}} C_k^{(j)} \cdot b_k^{(j-1)}$$

for $r+1 \leq j \leq t$ and $C_k^{(j)} \in A_{j-1}$ for $r+1 \leq j \leq t$. For the computation of the coefficients $(C_1^{(r)}, \ldots, C_{N_{r-1}}^{(r)}) \in \beta_{r-1}$ such that the following holds :

$$1 - (G_t f_t + \cdots + G_r f_r) \in (f_1, \ldots, f_{r-1}),$$

we proceed as follows : f_r is not a zero divisor in B_{r-1} and f_r divides the polynomial Q_{r+1}. Let $h_r \in B_{r-1}$ be such that $h_r \cdot \bar{f}_r = \bar{Q}_{r+1}$. Then, for every $k, 1 \leq k \leq N_{r-1}$, we have the following identity :

$$\sigma'_{r-1}(\bar{f}_r^{-1} \cdot \bar{Q}_{r+1} \cdot \bar{a}_k^{(r-1)}) = \sigma_{r-1}(\bar{h}_r \cdot \bar{a}_k^{(r-1)}) \in A_{r-1}.$$

Then, we proceed as follows :

$$\begin{aligned}
\sigma'_{r-1}\left(\bar{f}_r^{-1} \cdot \bar{q}_r \cdot \bar{a}_k^{(r-1)}\right) &= \sigma'_{r-1}\left((\overline{(1 - (g_t f_t + \cdots + g_{r+1} f_{r+1}))} \cdot \bar{f}_r^{-1} \cdot \bar{a}_k^{(r-1)}\right) \\
&= \sigma'_{r-1}\left(\bar{f}_r^{-1} \cdot \bar{a}_k^{(r-1)}\right) - \left(\sum_{i=r+1}^{t} \sigma'_{r-1}\left(\bar{g}_i \cdot \bar{f}_i \cdot \bar{f}_r^{-1} \cdot \bar{a}_k^{(r-1)}\right)\right) \\
&= \sigma'_{r-1}\left(\bar{f}_r^{-1} \cdot \bar{a}_k^{(r-1)}\right) - \left[\sum_{i=r+1}^{t} \sigma'_{r-1}\left(\sum_{t=1}^{N_{i-1}} \bar{C}_t^{(i)} \cdot \bar{b}_t^{(i-1)} \cdot \bar{f}_i \cdot \bar{f}_r^{-1} \cdot \bar{a}_k^{(r-1)}\right)\right] \\
&= d_k^{(r-1)} - \left[\sum_{i=r+1}^{t} \left(\sum_{t=1}^{N_{i-1}} \bar{C}_t^{(i)} \cdot \sigma'_{r-1}\left(\bar{b}_t^{(i-1)} \cdot \bar{f}_i \cdot \bar{f}_r^{-1} \cdot \bar{a}_k^{(r-1)}\right)\right)\right] \\
&= d_k^{(r-1)} - \left[\sum_{i=r+1}^{t} \left(\sum_{t=1}^{N_{i-1}} e_{k,t}^{(r-1,i)} \cdot \bar{C}_r^{(i)}\right)\right].
\end{aligned}$$

In other words, using the matricial language, we obtain for $1 \leq r \leq t-1$ the following linear recurrence to perform the wanted division step. It is well-known that linear recurrences can be inverted by a well-parallelizable procedure, see [20]. Then, the computation of terms given by a linear recurrence can be done by a well-parallelizable procedure.

$$\begin{pmatrix} C_1^{(r)} \\ \vdots \\ C_{N_{r-1}}^{(r)} \end{pmatrix} = D^{(r)} - \left(\sum_{i=r+1}^{t} E^{(r,i)} \cdot \begin{pmatrix} C_1^{(i)} \\ \vdots \\ C_{N_{i-1}}^{(i)} \end{pmatrix}\right).$$

Let us observe that this identity holds in the vector space β'_{r-1} (since the matrices $D^{(r)}$ and $E^{(r,i)}$ have entries in F_i) but that both sides of this identity represent objects belonging to the free A_{r-1}–module β_{r-1}.

Thus, to conclude the proof of Theorem 2 we just have to show how to invert this linear recurrence. However, as in the previous proof of Theorem 1, the presence of intermediate divisions by non–constant polynomials would hide information. This leads to a procedure that combines inversion of linear recurrences together with carrying on denominators. This is what we show below.

Following the recurrence rule, we observe that there are polynomials

$$P_i(Z^{(i)}, \ldots, Z^{(t)}, Z^{(i,i+1)}, \ldots, Z^{i,t)}, Z^{(i+1,i+2)}, \ldots, Z^{(t-1,t)}) \tag{35}$$

such that for every $i, 1 \leq i \leq t-1$,

$$\begin{pmatrix} C_1^{(i)} \\ \vdots \\ C_{N_{i-1}}^{(i)} \end{pmatrix} := P_i(D^{(i)}, \ldots, D^{(t)}, E^{(i,i+1)}, \ldots, E^{(i,t)}, \ldots, E^{(t-1,t)}) \cdot \begin{pmatrix} C_1^{(t)} \\ \vdots \\ C_{N_{t-1}}^{(t)} \end{pmatrix}$$

where $\mathcal{P}_i := P_i(D^{(i)}, \ldots)$ is a matrix with entries in F_{i-1}. These polynomials P_i have coefficients in $\{-1, 0, 1\} \subseteq \mathbb{Z}$ and their monomials are of degree at most t. In fact, only a few monomials occur in this expression, since they are of the form $E^{(i,j_1)} \cdot E^{(j_1,j_2)} \cdots E^{(j_k,j_{k+1})}$ where $i < j_1 < j_2 < \ldots < j_{k+1} < t$ or $E^{(i,j_1)} \cdot E^{(j_1,j_2)} \cdots E^{(j_k,j_{k+1})} \cdot D^{(j_{k+1})}$ also with $i < j_1 < j_2 < \ldots < j_{k+1} < t$.

The obvious procedure that computes first the monomials (in the appropriate order) and then adds the results has non–scalar depth of order $O(\log_2 t)$. However, to multiply two of these matrices we are dealing a total number of multiplications of order $(\max N_i)^{O(1)} \leq (td)^{O(t)}$ which yields an awful upper bound for the size.

To end this proof, we are going to see how these linear recurrences can be computed in low parallel time. Let us observe that for the computation of the matrices $D^{(i)}$ and $E^{(i,j)}$ we have to compute some traces of some polynomials. This can be done using the following identities :

$$d_0^{(i)} := Tr_i'(\bar{J}_i^{-1} \cdot \bar{f}_{i+1}^{-1} \cdot \bar{a}_k^{(i)}) \text{ and } e_{k,l}^{(i,j)} := Tr_i'(\bar{J}_i^{-1} \cdot \bar{b}_t^{(j)} \cdot \bar{f}_{j+1} \cdot \bar{f}_{i+1}^{-1} \cdot \bar{b}_k^{(i)}),$$

where $Tr_i' : B_i' \to F_i$ is the usual trace and J_i is the jacobian determinant of $f_1, \ldots, f_i$ with respect to the variables $Y_1, \ldots, Y_{n-i+1}$. Thus, noting that $\deg a_k^{(i)} \leq t(d-1)$ and $\deg b_k^{(j)} \leq t(d-1)$, we may conclude as in Lemma 21 (i.e. carrying on denominators) that :

There exists a non–scalar straight–line program Γ of size $((td)^t L\delta)^{O(1)}$ and non–scalar depth $O(\log_2 t + \log_2 d + \log_2 L + \log_2 \delta)$ such that Γ computes from the geometric solutions of the varieties $V_1, \ldots, V_{t-1}$ non–zero polynomials $\Theta^{(i)} \in R[Y_1, \ldots, Y_{n-i+1}]$ and the entries in $R[Y_1, \ldots, Y_{n-i+1}]$ of matrices $\mathcal{D}_k^{(i)}$, $\mathcal{E}^{(i,j)}$ such that $D_k^{(i)} = (\Theta^{(i)})^{-1} \cdot \mathcal{D}_k^{(i)}$ and $E^{(i,j)} = (\Theta^{(i)})^{-1} \cdot \mathcal{E}^{(i,j)}$.

Finally, the computation of the polynomials P_i from Equation (35) on page 61 is performed for each polynomial separately. We also compute the respective homogeneous components :

$$P_i := P_{i,0}^* + \cdots + P_{i,t}^*.$$

Thus, defining $\widetilde{\Theta}^{(i)} := \prod_{j=1}^{t} \Theta^{(i)}$, we conclude that for every i there exists a matrix

$$\widetilde{\mathcal{P}}_i \in \mathcal{M}_{N_{t-1}}(R[Y_1, \ldots, Y_{n-i+1}])$$

such that

$$\begin{pmatrix} C_1^{(i)} \\ \vdots \\ C_{N_{i-1}}^{(i)} \end{pmatrix} = (\widetilde{\Theta}^{(i)})^{-1} \cdot \widetilde{\mathcal{P}}_i \cdot \begin{pmatrix} C_1^{(t)} \\ \vdots \\ C_{N_{t-1}}^{(t)} \end{pmatrix}$$

and both $\widetilde{\Theta}^{(i)}$ and the matrices $\widetilde{\mathcal{P}}_i$ can be computed from the geometric solutions of the varieties $V_1, \ldots, V_{t-1}$ by a non–scalar straight–line program of size $((td)^t\delta)L^{O(1)}$, non–scalar depth $O(\log_2 t + \log_2 d + \log_2 \delta + \log_2 L)$ and parameters in $\{-1, 0, 1\}$.

Thus we finally conclude by performing the non–scalar arithmetic operations (that can be done in depth $O(1)$)

$$G_i := (\widetilde{\Theta}^{(i)})^{-1} \cdot (\langle \widetilde{\mathcal{P}}_i \begin{pmatrix} C_1^{(t)} \\ \vdots \\ C_{N_{t-1}}^{(t)} \end{pmatrix}, \begin{pmatrix} b_1^{(i-1)} \\ \vdots \\ b_{N_{i-1}}^{(i-1)} \end{pmatrix} \rangle)$$

where $\langle , \rangle$ denotes the scalar product. Finally, applying the *Vermeidung von Divisionen* technique as in Proposition 20, we obtain the desired statement. ∎

7.2 Applications

This Subsection recompiles the proofs of the Corollaries which were announced at the introduction and which depended on the completion of the proofs for the Theorems 1 and 2.

Complexity bounds - proof of Corollary 3 *Proof.–* The algorithm developed in the sequence of papers [44], [28], [25], and [60] gives an efficient method for the computation of the geometric solutions of all intermediate varieties $V(f_1, \ldots, f_i)$, see Proposition 54. This, together with the method given in Section 6 for the computation of a straight–line program evaluating the polynomials $g_1, \ldots, g_t$ and the integer a yields the proof of Corollary 3. The time complexity of the Turing machine M is an immediate consequence of the size of the straight–line program exhibited in Section 6. ■

Height bounds - proof of Corollary 4 *Proof.–* By Lemma 40 from page 32 we know that a geometric solution of every variety $V(f_1, \ldots, f_i)$ can be computed from the elimination polynomial of $V(f_1, \ldots, f_i)$. Thus, applying Lemma 17 (Composition) from page 18, we may estimate the logarithmic and invariant heights of the polynomials in a geometric solution of $(f_1, \ldots, f_i))$. Now, using the straight–line program stated in Theorem 2 and applying the bounds of Lemmata 15 and 17 from Section 2.3 we obtain the desired bounds for the proof of Corollary 4. ■

Upper bound for π_S: proof of Corollary 7 *Proof.–* The height bound of Corollary 5 for the integer a appearing in the arithmetic Bézout Equality gives $ht(a) \leq (ndL\delta_S)^{O(1)}(ht(\mathcal{F}) + \eta_S + \log_2 s)$. As we can always bound the number of possible prime divisors of a number by its (logarithmic) height, the claim of Corollary 7 follows as an immediate consequence. ■

Lower bound for π_S: proof of Theorem 10 *Proof.–* The following lines give an idea of the proof, a more complete account can be found in [60]). Let us suppose given the system $S = \{f_1, \ldots, f_s\}$, where the polynomials $f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_n]$ are given by a straight–line program of size L and depth ℓ. Let us also suppose, that these polynomials form a reduce regular sequence and let us denote by δ_S the geometric degree and by η_S the height of the system S.

For the proof of Theorem 10, the following results are relevant:

Lemma 66 *Let $x = (x_1, \ldots, x_n)$ be a zero of the system S and let r be a primitive element (in the sense of Subsection 3.4) for $x_1, \ldots, x_n$. Then, there exist $Q_1, \ldots, Q_n \in \mathbb{Z}[X]$ and $a \in \mathbb{Z}$ such that $x_i = Q_i(r)/a$. Let $R \in \mathbb{Z}[X]$ be an irreducible polynomial such that $R(r) = 0$. If R has a root in $\mathbb{F}_p$ and a is not zero modulo p, the system is consistent in $\mathbb{F}_p$.*

Let now $f \in \mathbb{Z}[X]$ be a polynomial of degree d, Δ its discriminant and let $\pi_f(x)$ be the number of primes p such that f has a root modulo p. Based on an effective version of Chebotarev's Density Theorem (which assumes the Generalized Riemann Hypothesis) one can prove:

Lemma 67 ([41]) *There exists a universal constant $c > 0$ such that*

$$\pi_f(x) \geq \frac{1}{d}[\pi(x) - log_2\Delta - cx^{1/2}log_2(\Delta x^d)]$$

Once stated these results we begin the proof of Theorem 10.
We first study the case $s = n$, that is, the zero—dimensional case. In this case we have a primitive element for the variety V defined by S, $u \in \mathbb{Z}[X_1, \ldots, X_n]$, and polynomials $q \in \mathbb{Z}[T]$, $v_j \in \mathbb{Z}[T]$ and $\rho \in \mathbb{Z}$ (multiple of the discriminant of q) such that :

- q is square free and
- $\rho x_j - v_j(u(x_1, \ldots, x_n)) = 0$ for all $(x_1, \ldots, x_n)$ in V.

In order to finish the proof, we remark that by Lemma 66 above we only have to estimate $\pi_f(x)$. To do that, we simply remark that the degree of q is bounded by δ_S and the logarithmic height of its discriminant is bounded by $\delta_S^{O(1)}\eta_S$ by Theorem 41.

For the case $s < n$, we can reduce the situation to the zero–dimensional case by considering the fiber in a point of moderate logarithmic height (see [25] and [60] for more details). ∎

Bounds on $P_S(I)$ - proof of Corollary 8 *Proof.–* Given a bound B on the absolute value of the integer a appearing in the Nullstellensatz we know that a has at most $\log_2 B$ many prime divisors and therefore holds

$$P_S(I) \geq \frac{\#(I) - \log_2 B}{\#(I)}.$$

We apply Lemma 16 to the bounds for L, ℓ established in *iii)* of Corollary 5 to conclude claim *i)* of Corollary 8. Similarly, using the bound for the height of a from Corollary 5 *iv)*, follows claim *ii)*. ∎

Probability - proof of Corollary 9 *Proof.–* Under the hypotheses of Corollary 5, the height of the integer a appearing in the Nullstellensatz is bounded by $|\, a \,| \leq (ndL\delta_S)^{O(1)}(ht(\mathcal{F}) + \eta_S + \log_2 s)$, and therefore a cannot possess any prime divisors of greater height. This already yields the bound given in Corollary 7.

Now, for $m := \max\{c_3' \log_2(ndL\delta_S)), ht(\mathcal{F}) + \eta_s + \log_2 s\}$ holds $|\, a \,| \leq 2^{m2^m}$ which in turn yields claim *ii)* of Corollary 9. Claim *i)* follows as an application of Corollary 8 *i)*. ∎

References

[1] M. Aldaz, J. Heintz, G. Matera, J. L. Montaña, and L. M. Pardo. Time-Space Tradeoffs in algebraic complexity theory. preprint, Universidad de Cantabria, Santander, Spain, 1996.

[2] M. Almeida, L. D'Alfonso, and P. Solernó. On the degrees of bases of free modules over a polynomial ring. *Math. Zeitschrift,* to appear, pp. 1–24, 1998.

[3] M. E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeroes, multiplicities and idempotents for zerodimensional systems. In *Algorithms in Algebraic Geometry and Applications. Proceedings of MEGA'94*, vol. 142 of *Progress in Mathematics*, pp. 1–15. Birkhäuser, 1996.

[4] I. Armendáriz and P. Solernó. On the computation of the radical of polynomial complete intersection ideals. In G. Cohen, H. Giusti, and T. Mora, eds., *Applied Algebra, Algebraic Algorithms and Error Correcting Codes. Proceedings of AAECC-11*, vol. 948 of *LNCS*, pp. 106–119. Springer, 1995.

[5] E. Becker, J. P. Cardinal, M. F. Roy, and Z. Szafraniec. Multivariate Bezoutians, Kronecker symbol and Eisenbud-Levine formula. In *Algorithms in Algebraic Geometry and Applications. Proceedings of MEGA'94*, vol. 142 of *Progress in Mathematics*, pp. 79–104. Birkhäuser, 1996.

[6] C. Berenstein and A. Yger. Effective Bézout identities in $Q[X_1, \ldots, X_n]$. *Acta. Math.*, **vol. 166**:pp. 69–120, 1991.

[7] C. Berenstein and A. Yger. Une Formule de Jacobi et ses conséquences. *Ann. Sci. E.N.S.*, **vol. 24 (4)**:pp. 363–377, 1991.

[8] S. J. Berkowitz. On Computing the determinant in small parallel time using a small number of processors. *Information Processing Letters*, **vol. 18**:pp. 147–150, 1984.

[9] L. Blum, F. Cucker, M. Shub, and S. Smale. Complexity and Real Computation: A Manifesto. Technical Report ICSI-TR-95-042, International Computer Science Institute, Berkeley, CA, August 1995.

[10] L. Blum, F. Cucker, M. Shub, and S. Smale. Real Complexity and Computation. Manuscript, to appear in Springer Verlag, 1997.

[11] A. Borodin, J. von zur Gathen, and J. Hopcroft. Fast parallel matrix and gcd computations. In *Proceedings 23rd. Ann. Symp. FOCS*, pp. 65–71. 1982.

[12] D. W. Brownawell. Bounds for the Degree in the Nullstellensatz. *Annals of Math.*, **vol. 126**:pp. 577–591, 1987.

[13] L. Caniglia, A. Galligo, and J. Heintz. Borne simple exponentielle pour les degrés dans le théorème des zéros sur un corps de charactéristique quelconque. *C. R. Acad. Sci. Paris*, **vol. 307**:pp. 255–258, 1988.

[14] L. Caniglia, A. Galligo, and J. Heintz. Some new effectivity bounds in computational geometry. In T. Mora, ed., *Applied Algebra, Algebraic Algorithms and Error Correcting Codes. Proceedings of AAECC-6*, vol. 357 of *LNCS*, pp. 131–152. Springer, 1989.

[15] L. Caniglia, A. Galligo, and J. Heintz. Equations for the projective closure and effective Nullstellensatz. *Discrete Applied Mathematics*, **vol. 33**:pp. 11–23, 1991.

[16] D. Castro, K. Hägele, J. L. Montaña, and L. M. Pardo. Probabilistic zero test for elimination polynomials. preprint, 21 pages, May 1998.

[17] A. Chistov. Polynomial complexity algorithm for factoring polynomials and constructing components of a variety in subexponential time. *J. of Soviet Mathematics*, **vol. 34**, 1986.

[18] A. L. Chistov. Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic. *Lecture Notes in Computer Science*, **vol. 199**:pp. 63–69, 1985.

[19] S. A. Cook. The complexity of theorem-proving procedures. In *Proceedings of the Third Annual ACM Symposium on Theory of Computing*, pp. 151–158. 1971.

[20] L. Csanky. Fast parallel matrix inversion algorithms. *SIAM Journal of Computing*, **vol. 5 (4)**:pp. 618–623, 1976.

[21] T. W. Dubé. A combinatorial proof of Effective Nullstellensatz. *J. Symb. Comp.*, **vol. 15**:pp. 277–296, 1993.

[22] N. Fitchas and A. Galligo. Nullstellensatz effectif et Conjecture de Serre (Théorème de Quillen-Suslin) pour le Calcul Formel. *Math. Nachr.*, **vol. 149**:pp. 231–253, 1990.

[23] N. Fitchas, M. Giusti, and F. Smietanski. Sur la complexité du théorème des zéros. In J. Guddat, ed., *Approximation and Optimization in the Caribbean II, Proceedings 2nd Int. Conf. on Non-Linear Optimization and Approximation*, vol. 8 of *Approximation and Optimization*, pp. 247–329. Peter Lange Verlag, Frankfurt am Main, 1995.

[24] W. Fulton. *Intersection Theory*. Number 3 in Ergebnisse der Mathematik. Springer, second edition, 1984.

[25] M. Giusti, K. Hägele, J. Heintz, J. E. Morais, J. L. Montaña, and L. M. Pardo. Lower Bounds for Diophantine Approximation. In *Proceedings of MEGA'96*, vol. 117,118, pp. 277–317. Journal of Pure and Applied Algebra, 1997.

[26] M. Giusti and J. Heintz. Algorithmes - disons rapides - pour la décomposition d' une variété algébrique en composantes irréductibles et équidimensionelles. In T. Mora and C. Traverso, eds., *Proceedings of MEGA'90*, vol. 94 of *Progress in Mathematics*, pp. 169–194. Birkhäuser, 1991.

[27] M. Giusti and J. Heintz. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. In D. Eisenbud and L. Robbiano, eds., *Computational Algebraic Geometry and Commutative Algebra*, vol. XXXIV of *Symposia Matematica*, pp. 216–256. Cambridge University Press, 1993.

[28] M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, and L. M. Pardo. Straight–Line Programs In Geometric Elimination Theory. *J. of Pure and App. Algebra*, **vol. 124**:pp. 101–146, 1998.

[29] M. Giusti, J. Heintz, J. E. Morais, and L. M. Pardo. When Polynomial Equation Systems can be solved fast ? In G. Cohen, H. Giusti, and T. Mora, eds., *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings AAECC-11*, vol. 948 of *LNCS*, pp. 205–231. Springer, 1995.

[30] M. Giusti, J. Heintz, J. E. Morais, and L. M. Pardo. Le rôle des structures de données dans les problèmes d'élimination. *C. R. Acad. Sci. Paris*, **vol. 325**:pp. 1223–1228, 1997.

[31] M. Giusti, J. Heintz, and J. Sabia. On the Efficiency of effective Nullstellensätze. *Computational Complexity*, **vol. 3**:pp. 56–95, 1993.

[32] D. Grigoriev. Polynomial factoring over a finite field and solving systems of algebraic equations. *J. of Soviet Mathematics*, **vol. 34**:pp. 1762–1803, 1986.

[33] K. Hägele. *Intrinsic height estimates for the Nullstellensatz*. Ph.D. thesis, Universidad de Cantabria, Santander, Spain, 1998.

[34] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theor. Comput. Sci.*, **vol. 24 (3)**:pp. 239–277, 1983.

[35] J. Heintz. On the computational complexity of polynomials and bilinear mappings. A survey. In *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings of AAECC-5*, vol. 356 of *LNCS*, pp. 269–300. Springer, 1989.

[36] J. Heintz and C. P. Schnorr. Testing Polynomials which are easy to compute. In *Logic and Algorithmic*, vol. 30 of *Monographie de l'Enseignement Mathématique*, pp. 237–254. 1982.

[37] G. Hermann. Die Frage der endlich vielen Schritte in der Theorie de Polynomideale. *Math. Ann.*, **vol. 95**:pp. 736–788, 1926.

[38] O. H. Ibarra and S. Moran. Equivalence of Straight-line Programs. *Journal of the ACM*, **vol. 30**:pp. 217–228, 1983.

[39] B. Iversen. *Generic local structure of the morphisms in Commutative Algebra*, vol. 310 of *LNM*. Springer, 1973.

[40] J. P. Jouanolou. *Théorèmes de Bertini et applications*. Progress in Mathematics. Birkhäuser Verlag, 1983.

[41] P. Koiran. Hilbert's Nullstellensatz Is in the Polynomial Hierarchy. *Journal of Complexity*, **vol. 12 (4)**:pp. 273–286, December 1996.

[42] J. Kollár. Sharp effective Nullstellensatz. *J. of the AMS*, **vol. 1**:pp. 963–975, 1988.

[43] T. Krick and L. M. Pardo. Une approche informatique pour l' approximation diophantienne. *C. R. Acad. Sci. Paris*, **vol. 318 (1)**:pp. 407–412, 1994.

[44] T. Krick and L. M. Pardo. A Computational Method for Diophantine Approximation. In L. González-Vega and T. Recio, eds., *Algorithms in Algebraic Geometry and Applications. Proceedings of MEGA'94*, vol. 143 of *Progress in Mathematics*, pp. 193–254. Birkhäuser Verlag, 1996.

[45] T. Krick, J. Sabia, and P. Solernó. On intrinsic bounds in the Nullstellensatz. *Applicable Algebra in Engineering Communications and Computing (AAECC Journal)*, **vol. 8**:pp. 125–134, 1997.

[46] L. Kronecker. Grundzüge einer arithmetischen Theorie de algebraischen Grössen. *J. reine angew. Math.*, **vol. 92**:pp. 1–122, 1882.

[47] E. Kunz. *Introduction to Commutative Algebra and Algebraic Geometry*. Birkhäuser Verlag, 1985.

[48] E. Kunz. *Kähler Differentials*. Advanced Lectures in Mathematics. Vieweg Verlag, 1986.

[49] T. Y. Lam. *Serre's Conjecture*, vol. 635 of *LNM*. Springer, 1978.

[50] S. Lang. *Fundamentals of Diophantine Geometry*. Springer, 1983.

[51] D. H. Lehmer. Factorization of certain cyclotomic functions. *Ann. of Math.*, **vol. 34 (2)**:pp. 461–479, 1933.

[52] F. S. Macauley. *The Algebraic Theory of Modular Systems*. Cambridge University Press, 1916.

[53] G. Matera. *Sobre la complejidad en espacio y tiempo de la eliminación geométrica*. Ph.D. thesis, Universidad de Buenos Aires, Argentina, 1997.

[54] H. Matsumura. *Commutative Ring Theory*. Cambridge University Press, 1986.

[55] P. J. McCarthy. *Algebraic Extensions of Fields*. Chelsea Publishing Comp., New York, 1976.

[56] H. M. Möller and F. Mora. Upper and lower Bounds for the degree of Groebner Bases. In J. Fitch, ed., *Proceedings of the International Symposium on Symbolic and Algebraic Computation (EUROSAM 84)*, vol. 174 of *LNCS*, pp. 172–183. Springer, Cambridge, UK, July 1984.

[57] J. L. Montaña, J. E. Morais, and L. M. Pardo. Lower Bounds for Arithmetic Networks II: Sum of Betti Numbers. *Applicable Algebra in Engineering Communications and Computing*, **vol. 7**:pp. 41–51, 1996.

[58] J. L. Montaña and L. M. Pardo. Lower bounds for Arithmetic Networks. In *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings of AAECC-4*, pp. 1–24. Springer, 1993.

[59] J. L. Montaña, L. M. Pardo, and T. Recio. The non-scalar Model of Complexity in Computational Geometry. In C. Traverso and T. Mora, eds., *Effective Methods in Algebraic Geometry, Proceedings of MEGA'90*, vol. 94 of *Progress in Mathematics*, pp. 347–361. Birkhäuser, 1991.

[60] J. E. Morais. *Resolución eficaz de sistemas de ecuaciones polinomiales*. Ph.D. thesis, Universidad de Cantabria, Santander, Spain, 1997.

[61] Y. Nesterenko. On algebraic independence of algebraic powers of algebraic numbers. *Math. USSR. Sbornik*, **vol. 51 (2)**:pp. 429–455, 1985.

[62] Y. Nesterenko. On a measure of the algebraic independence of the values of certain functions. *Math. USSR. Sbornik*, **vol. 56 (2)**:pp. 545–567, 1987.

[63] L. M. Pardo. How lower and upper complexity bounds meet in elimination theory. In G. Cohen, H. Giusti, and T. Mora, eds., *Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995)*, vol. 948 of *Lecture Notes in Computer Science*, pp. 33–69. Springer, Berlin, 1995.

[64] P. Philippon. Critères pour l'indépendance algébrique. *Pub. Math. de l'IHES*, **vol. 64**:pp. 5–52, 1986.

[65] P. Philippon. Denominators in Hilbert's Nullstellensatz. *Acta Arith.*, **vol. 58**:pp. 1–25, 1991.

[66] P. Philippon. Sur des hauteurs alternatives, I. *Math. Ann.*, **vol. 289**:pp. 255–283, 1991.

[67] P. Philippon. Sur des hauteurs alternatives, II. *Ann. Inst. Fourier, Grenoble*, **vol. 44 (2)**:pp. 1043–1065, 1994.

[68] P. Philippon. Sur des hauteurs alternatives, III. *J. Math. Pures Appl.*, **vol. 74**:pp. 345–365, 1995.

[69] F. Rossi and W. Spangher. Some effective methods in the openness of loci for Cohen-Macaulay and Gorenstein properties. In T. Mora and C. Traverso, eds., *Proceedings of MEGA'90*, vol. 94 of *Progress in Mathematics*, pp. 441–455. Birkhäuser, 1991.

[70] J. Sabia and P. Solernó. Bounds for Traces in Complete Intersections and Degrees in the Nullstellensatz. *Applicable Algebra in Engineering Communications and Computing (AAECC Journal)*, **vol. 6**:pp. 353–376, 1996.

[71] A. Schönhage. On the power of random access machines. In H. A. Maurer, ed., *Proceedings of the 6th Colloquium on Automata, Languages and Programming*, vol. 71 of *LNCS*, pp. 520–529. Springer, July 1979.

[72] J. T. Schwartz. Probabilistic algorithms for verification of polynomial identities. In *ISSAC '79: Proceedings of Int'l. Symp. on Symbolic and Algebraic Computation*, vol. 72 of *Lecture Notes in Computer Science*. Springer-Verlag, 1979.

[73] M. Shub and S. Smale. Complexity of Bézout's Theorem I: Geometric Aspects. *J. of the AMS*, **vol. 6 (2)**:pp. 459–501, 1993.

[74] M. Shub and S. Smale. Complexity of Bézout's Theorem II: Volumes and Probabilities. In *Proceeding effective methods in Algebraic Geometry*, vol. 109 of *Progress in Mathematics*, pp. 267–285. MEGA '92, Niece, Birkhäuser, 1993.

[75] M. Shub and S. Smale. Complexity of Bézout's Theorem III: Condition number and packing. *J. of Complexity*, **vol. 9**:pp. 4–14, 1993.

[76] M. Sombra. Bounds for the Hilbert function of polynomial ideal and for the degrees in the Nullstellensatz. In *Proceedings of MEGA'96*, vol. 117 & 118, pp. 565–599. North-Holland, 1997.

[77] M. Sombra. *Estimaciones para el teorema de ceros de Hilbert*. Ph.D. thesis, Universidad de Buenos Aires, Argentina, 1998.

[78] M. Sombra. A sparse effective Nullstellensatz. *Adv. Appl. Math.* to appear, 1998.

[79] V. Strassen. Vermeidung von Divisionen. *Crelle J. Reine Angew. Math,*, **vol. 264**:pp. 182–202, 1973.

[80] V. Strassen. Algebraic Complexity Theory. In *Handbook of Theoretical Computer Science*, chapter 11, pp. 634–671. Elsevier, 1990.

[81] B. L. Van der Waerden. *Moderne Algebra I*. Berlin, 1930.

[82] W. Vogel. *Results on Bézout's Theorem*. Tata Institute of Fundamental Research. Springer, 1984.

[83] O. Zariski. *Algebraic Surfaces*. Classics in Mathematics. Springer, 1995.

[84] O. Zariski and P. Samuel. *Commutative Algebra*, vol. 2 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1960.

[85] R. Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings EUROSAM' 79*, number 72 in LNCS, pp. 216–226. Springer, 1979.

[86] R. Zippel. Interpolating Polynomials from their Values. *J. Symbol. Comput.*, **vol. 9**:pp. 147–175, 1990.

[87] R. Zippel. *Effective Polynomial Computation*. ECS 241. Kluwer Academic Publishers, 1993.