Bit-size estimates for triangular sets in positive dimension

Xavier Dahan
Faculty of Mathematics, Kyûshû University
dahan@math.kyushu-u.ac.jp

Abdulilah Kadri
Mathematics Department, The University of Western Ontario
akadri4@uwo.ca

Éric Schost
Computer Science Department, The University of Western Ontario
eschost@uwo.ca

May 23, 2010

Abstract

We give bit-size estimates for the coefficients appearing in triangular sets describing positive-dimensional algebraic sets defined over $\mathbb{Q}$. These estimates are worst case upper bounds; they depend only on the degree and height of the underlying algebraic sets. We illustrate the use of these results in the context of a modular algorithm.

This extends results by the first and last author, which were confined to the case of dimension 0. Our strategy is to get back to dimension 0 by evaluation and interpolation techniques. Even though the main tool (height theory) remains the same, new difficulties arise to control the growth of the coefficients during the interpolation process.

Keywords: triangular set, regular chain, Chow form, height function, bit-size

1 Introduction

It is well known that for algorithms for multivariate polynomials with rational coefficients, or involving parameters, small inputs can generate very large outputs. We will be concerned here with the occurrence of this phenomenon for the solution of polynomial systems.

To circumvent this issue, a natural solution is to find smaller outputs. In dimension 0, if a parametrization of the solutions is required through a “Shape Lemma” output, the Rational Univariate Representation (Alonso et al., 1996; Rouillier, 1999), or Kronecker representation (Giusti et al., 2001), is usually seen to have smaller coefficients than a lexicographic Gröbner basis. It is obtained by multiplying the Gröbner basis elements by a well-chosen polynomial. It turns out that if a “triangular” representation is wanted, a similar trick can be employed, which, in most practical situations, reduces the coefficients size.

While such experimental observations can drive the choice or the discovery of a good data structure, it is desirable to dispose of a theoretical argument to validate its efficiency. Bit-size estimates, like the ones provided in this article for positive dimensional situations, provide this kind of theoretical argument. A second use of this kind of result, which will be illustrated later on, is to help quantify success probabilities of some probabilistic modular algorithms.

Triangular representations. Let k be a field; all fields will have characteristic 0 in this paper. For the moment, let us consider a 0-dimensional algebraic set $V \subset \overline{k}^n$, defined over k, and let $I \subset k[\mathbf{X}] = k[X_1, \ldots, X_n]$ be its defining ideal. Our typical assumption will be the following.

Assumption 1. *For the lexicographic order $X_1 < \cdots < X_n$, the reduced Gröbner basis of the ideal I has the form*

$$\left|\begin{array}{l} T_n(X_1, \ldots, X_n) \\ \quad\vdots \\ T_2(X_1, X_2) \\ T_1(X_1), \end{array}\right.$$

where for $\ell \leq n$, T_ℓ depends only on $X_1, \ldots, X_\ell$ and is monic in X_ℓ.

Following Lazard (1992), we say that the polynomials $(T_1, \ldots, T_n)$ form a *monic triangular set*, or simply a triangular set. This representation is well-suited to many problems (see some examples in (Lazard, 1992; Aubry and Valibouze, 2000; Schost, 2003a,b)), as meaningful information is easily read off on it.

Several algorithmic and complexity questions remain open for this data structure: this paper studies one of them. For V as in Assumption 1, we are interested in the “space complexity” of the representation of V by means of $(T_1, \ldots, T_n)$. For $\ell \leq n$, let d_ℓ be the degree of T_ℓ in X_ℓ and let $V_\ell \subset \overline{k}^\ell$ be the image of V by the projection $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_\ell)$; then, $d_1 \cdots d_\ell$ is the cardinality of V_ℓ.

Representing T_ℓ amounts to specifying at most $d_1 \cdots d_\ell$ elements of k. If k bears no particular structure, we cannot say more in terms of the space complexity of such a representation. New questions arise when k is endowed with a notion of “size”: then, the natural question is to relate the size of the coefficients in T_ℓ to quantities associated to V_ℓ.

This kind of information is useful in its own sake, but is also crucial in the development of algorithms to compute triangular sets (Schost, 2003a; Dahan et al., 2005, 2008), using in particular modular techniques. Several variants exist of such algorithms, most of them being probabilistic: integers are reduced modulo one or several random primes, and free variables are specialized at random values. To analyze the running time or the error probability of these algorithms, *a priori* bounds on the size of the coefficients of $(T_1, \ldots, T_n)$ are necessary (as is the case for modular algorithms in general: already for linear algebra algorithms, or gcd computations, bounds such as e.g. Hadamard's are crucial). An example of such an application is given in the last section of this paper, in the context of a modular algorithm for triangular decomposition.

The previous paper (Dahan and Schost, 2004) gave such space complexity results for the following cases:

- $k = \mathbb{Q}$, in which case we are concerned with the bit-size of coefficients;
- $k = K(\mathbf{Y})$, where K is a field and $\mathbf{Y} = Y_1, \ldots, Y_m$ are indeterminates; in this case we are concerned with the degrees in $\mathbf{Y}$ of the numerators and denominators of the coefficients.

These two cases cover many interesting concrete applications; the latter is typically applied over $K = \mathbb{F}_p$. The goal of this paper is to present an extension of these results to the last important case: polynomials defined over $k = \mathbb{Q}(\mathbf{Y})$. The second item above already covers the degree-related aspects; what is missing is the study of the bit-size of coefficients.

Unfortunately, the techniques of Dahan and Schost (2004) are unable to provide such information. Indeed, they rely on the study of an appropriate family of absolute values on k, together with a suitable notion of *height* for algebraic sets over k: for $k = \mathbb{Q}$, these are the classical p-adic absolute values, plus the Archimedean one, and height measures arithmetic complexity; for $k = K(\mathbf{Y})$, there are the absolute values associated to irreducible polynomials in $K[\mathbf{Y}]$, plus the one associated to the total degree on $K[\mathbf{Y}]$; then, height is a measure of geometric complexity.

Extending this approach to our case would require a family of absolute values that captures the notion of bit-size on $\mathbb{Q}(\mathbf{Y})$. Gauss' lemma implies that p-adic absolute values do extend from $\mathbb{Q}$ to $\mathbb{Q}(\mathbf{Y})$, but the Archimedean one does not. As a result, concretely, it seems unfeasible to re-apply the ideas of Dahan and Schost (2004) here. A different approach will be used, using evaluation and interpolation techniques.

Following Dahan and Schost (2004), it is fruitful to study not only the polynomials $(T_1, \ldots, T_n)$, but a related family of polynomials written $(N_1, \ldots, N_n)$ and defined as follows. Observe that for $\ell \leq n$, $(T_1, \ldots, T_\ell)$ form a reduced Gröbner basis; for a polynomial A in $k[\mathbf{X}]$, $A \bmod \langle T_1, \ldots, T_\ell \rangle$ denotes the normal form of A modulo the Gröbner basis $(T_1, \ldots, T_\ell)$. Let $D_1 = 1$ and $N_1 = T_1$; for $2 \leq \ell \leq n$, we define

$$\begin{aligned} D_\ell &= \prod_{1 \leq i \leq \ell-1} \frac{\partial T_i}{\partial X_i} \mod \langle T_1, \ldots, T_{\ell-1} \rangle, \\ N_\ell &= D_\ell T_\ell \mod \langle T_1, \ldots, T_{\ell-1} \rangle. \end{aligned}$$

Note that D_ℓ is in $k[X_1, \ldots, X_{\ell-1}]$ and N_ℓ in $k[X_1, \ldots, X_{\ell-1}, X_\ell]$, and that D_ℓ is the leading coefficient of N_ℓ in X_ℓ. Our reason to introduce the polynomials $(N_1, \ldots, N_n)$ is that they will feature much better bounds than the polynomials $(T_1, \ldots, T_n)$; we lose no information, since the ideals $\langle T_1, \ldots, T_n \rangle$ and $\langle N_1, \ldots, N_n \rangle$ coincide. Remark that the polynomials $(N_1, \ldots, N_n)$ are not monic, but the leading coefficient D_ℓ of N_ℓ is invertible modulo $\langle N_1, \ldots, N_{\ell-1} \rangle$: as such, $(N_1, \ldots, N_n)$ form a *regular chain* (Aubry et al., 1999).

Main result. After this general introduction, our precise setup will be the following. Consider first the affine space of dimension $m + n$ over $\mathbb{C}$, endowed with coordinates $\mathbf{Y} = Y_1, \ldots, Y_m$ and $\mathbf{X} = X_1, \ldots, X_n$. For $0 \le \ell \le n$, let next Π_ℓ be the projection

$$\begin{array}{cccc} \Pi_\ell : & \mathbb{C}^{m+n} & \to & \mathbb{C}^{m+\ell} \\ & (y_1, \ldots, y_m, x_1, \ldots, x_n) & \mapsto & (y_1, \ldots, y_m, x_1, \ldots, x_\ell), \end{array}$$

so that Π_0 is the projection on the $\mathbf{Y}$-space. Our starting object will be a positive-dimensional algebraic set $\mathscr{V}$ defined over $\mathbb{Q}$; then, the construction of the previous paragraphs will take place over $k = \mathbb{Q}(\mathbf{Y})$.

To measure the complexity of $\mathscr{V}$, we let $d_{\mathscr{V}}$ and $h_{\mathscr{V}}$ be respectively its *degree* and *height*. For the former, we use the classical definition (Bürgisser et al., 1997): under the assumption that $\mathscr{V}$ is equidimensional, this is the generic (and maximal) number of intersection points of $\mathscr{V}$ with a linear space of the complementary dimension. The notion of height is more technical: we give the definition in Section 3.

Let then $\mathscr{I} \subset \mathbb{Q}[\mathbf{Y}, \mathbf{X}]$ be the defining ideal of $\mathscr{V}$ and let $\mathscr{V}^\star \subset \overline{\mathbb{Q}(\mathbf{Y})}^n$ be the zero-set of $\mathscr{I}^\star = \mathscr{I} \cdot \mathbb{Q}(\mathbf{Y})[\mathbf{X}]$. We make the following assumptions:

Assumption 2.

- *The algebraic set $\mathscr{V}$ is defined over $\mathbb{Q}$, equidimensional of dimension m and the image of each irreducible component of $\mathscr{V}$ through Π_0 is dense in $\mathbb{C}^m$.*

- *The former point implies that $\mathscr{V}^\star$ has dimension 0; then, we assume that $\mathscr{V}^\star$ satisfies Assumption 1 over the base field $\mathbb{Q}(\mathbf{Y})$.*

As a consequence, there exist polynomials $(T_1, \ldots, T_n)$ in $\mathbb{Q}(\mathbf{Y})[\mathbf{X}]$ that generate the ideal $\mathscr{I}^\star$; associated to them, we also have the polynomials $(N_1, \ldots, N_n)$ defined above, which are in $\mathbb{Q}(\mathbf{Y})[\mathbf{X}]$ as well. Then, Theorem 1 below gives degree and bit-size bounds for the polynomials $(T_1, \ldots, T_n)$ and $(N_1, \ldots, N_n)$. As was said above, the degree bounds were already in (Dahan and Schost, 2004); the bit-size aspects are new.

In the complexity estimates, we denote by $\mathscr{V}_\ell \subset \mathbb{C}^{m+\ell}$ the Zariski-closure of the image of $\mathscr{V}$ through Π_ℓ, and let $d_{\mathscr{V}_\ell}$ and $h_{\mathscr{V}_\ell}$ be its degree and height. The degree and height of $\mathscr{V}_\ell$ may be smaller than those of $\mathscr{V}$, and cannot be larger (up to small parasite terms in the case of height, see Krick et al. (2001)). Next, for $\ell \le n$, we define the projection

$$\begin{array}{cccc} \pi_\ell : & \overline{\mathbb{Q}(\mathbf{Y})}^n & \to & \overline{\mathbb{Q}(\mathbf{Y})}^\ell \\ & (x_1, \ldots, x_n) & \mapsto & (x_1, \ldots, x_\ell); \end{array}$$

we let $\mathscr{V}_\ell^\star \subset \overline{\mathbb{Q}(\mathbf{Y})}^\ell$ be the image of $\mathscr{V}^\star$ through π_ℓ and let $d_\ell \le d_{\mathscr{V}_\ell}$ be its degree. Note that $\mathscr{V}_\ell^\star$ is obtained from $\mathscr{V}_\ell$ by the same process that gives $\mathscr{V}^\star$ from $\mathscr{V}$.

Finally, in the following theorem, the *height* $h(x)$ of a non-zero integer x denotes the real number $\log|x|$; it is a measure of its bit-length. The height of a non-zero polynomial with integer coefficients is the maximum of the heights of its non-zero coefficients. Recall also that for polynomials in $\mathbb{Z}[\mathbf{Y}]$, gcd's and lcm's are uniquely defined, up to sign.

Theorem 1. *Suppose that $\mathscr{V}$ satisfies Assumption 2. For $1 \le \ell \le n$, let us write N_ℓ as*

$$N_\ell = \sum_{\mathbf{i}} \frac{\gamma_{\mathbf{i},\ell}}{\varphi_{\mathbf{i},\ell}} X_1^{i_1} \cdots X_\ell^{i_\ell} + \frac{\gamma_\ell}{\varphi_\ell} X_\ell^{d_\ell}$$

and T_ℓ as

$$T_\ell = \sum_{\mathbf{i}} \frac{\beta_{\mathbf{i},\ell}}{\alpha_{\mathbf{i},\ell}} X_1^{i_1} \cdots X_\ell^{i_\ell} + X_\ell^{d_\ell},$$

where:

- *all multi-indices $\mathbf{i} = (i_1, \dots, i_\ell)$ satisfy $i_r < d_r$ for $r \le \ell$;*
- *all polynomials $\gamma_{\mathbf{i},\ell}$, $\varphi_{\mathbf{i},\ell}$, γ_ℓ and φ_ℓ, and $\beta_{\mathbf{i},\ell}$, $\alpha_{\mathbf{i},\ell}$, are in $\mathbb{Z}[\mathbf{Y}]$;*
- *in $\mathbb{Z}[\mathbf{Y}]$, the equalities $\gcd(\gamma_{\mathbf{i},\ell}, \varphi_{\mathbf{i},\ell}) = \gcd(\gamma_\ell, \varphi_\ell) = \gcd(\beta_{\mathbf{i},\ell}, \alpha_{\mathbf{i},\ell}) = \pm 1$ hold.*

Then, all polynomials $\gamma_{\mathbf{i},\ell}$ and γ_ℓ, $\varphi_{\mathbf{i},\ell}$ and φ_ℓ, as well as the lcm of all $\varphi_{\mathbf{i},\ell}$ and φ_ℓ, have degree bounded by $d_{\mathscr{V}_\ell}$ and height bounded by

$$\mathcal{H}_\ell \le 2h_{\mathscr{V}_\ell} + \big((4m+2)d_{\mathscr{V}_\ell} + 4m\big)\log(d_{\mathscr{V}_\ell}+1) + \big((10m+16)d_{\mathscr{V}_\ell} + 5\ell + 2m\big)\log(m+\ell+3).$$

All polynomials $\beta_{\mathbf{i},\ell}$ and $\alpha_{\mathbf{i},\ell}$, as well as the lcm of all $\alpha_{\mathbf{i},\ell}$, have degree bounded by $2d_{\mathscr{V}_\ell}^2$ and height bounded by

$$\begin{aligned}\mathcal{H}'_\ell \;\le\; & 4d_{\mathscr{V}_\ell}h_{\mathscr{V}_\ell} + 3d_{\mathscr{V}_\ell}^2 + 4\big((2m+1)d_{\mathscr{V}_\ell}^2 + m(d_{\mathscr{V}_\ell}+1)\big)\log(d_{\mathscr{V}_\ell}+1) \\ & + \big((20m+22)d_{\mathscr{V}_\ell}^2 + 5(d_{\mathscr{V}_\ell}+\ell+m)\big)\log(m+\ell+3).\end{aligned}$$

Comments. The first thing to note is that these bounds are *polynomial* in the degree and height of $\mathscr{V}_\ell$, and are quite similar to those obtained in (Dahan and Schost, 2004) for the 0-dimensional case (with $m = 0$). These results are actually simplified versions of more precise estimates; they were obtained by performing (sometimes crude) simplifications at various stages of the derivation. These simplifications are nevertheless necessary to obtain compact formulas, and the orders of magnitude of the results are unchanged: the bound for N_ℓ is essentially of order $h_{\mathscr{V}_\ell} + d_{\mathscr{V}_\ell}$, whereas that for T_ℓ has order $(h_{\mathscr{V}_\ell} + d_{\mathscr{V}_\ell})d_{\mathscr{V}_\ell}$.

While we do not know about the sharpness of these results, they reflect practical experience: in many cases, the polynomials $(N_1, \dots, N_n)$ have much smaller coefficients than the polynomials $(T_1, \dots, T_n)$; this was already pointed out for 0-dimensional cases in (Alonso et al., 1996; Rouillier, 1999; Dahan and Schost, 2004).

These bounds are intrinsic, in that they do not depend on a given system of generators of $\mathscr{I}$. As such, they behave well under operations such as decomposition, due to the additivity of degree and height of algebraic sets. Of course, if we are given bounds on polynomials defining $\mathscr{V}$, it is possible to rewrite the previous estimates in terms of these bounds, by means of the geometric and arithmetic forms of Bézout's theorem. Suppose for instance that $\mathscr{V}$ is the zero-set of a system of n polynomials of degree at most d, with integer coefficients of height at most h; more generally, since degree and height are additive, we could suppose that $\mathscr{V}$ consists of one or several irreducible components of an algebraic set defined by such a system. The geometric Bézout inequality, and bounds on degrees through projections (Heintz, 1983) gives the inequality $d_{\mathscr{V}_\ell} \leq d^n$ for all ℓ; similar results in an arithmetic context (Krick et al., 2001) show that $h_{\mathscr{V}_\ell} \leq d^n(nh + (4m + 2n + 3)\log(m + n + 1))$ holds for all ℓ. After substitution, this gives

$$\mathcal{H}_\ell = O\big(d^n(nh + mn\log(d) + (m + n)\log(m + n))\big)$$

and

$$\mathcal{H}'_\ell = O\big(d^{2n}(nh + mn\log(d) + (m + n)\log(m + n))\big);$$

here, we write $f(m, n, d, h) = O(g(m, n, d, h))$ if there exists $\lambda > 0$ such that $f(m, n, d, h) \leq \lambda g(m, n, d, h)$ holds for all m, n, d, h. The main point is that the former grows roughly like hd^n, while the latter grows like hd^{2n}.

To our knowledge, no previous result has been published on the specific question of bounds in positive dimension. Gallo and Mishra (1990) give a derivation of degree bounds, which may be extended to give bit-size estimates; these would however be of order $hd^{O(n^2)}$ at best. Besides, such bounds would depend on a set of generators for the ideal $\mathscr{I}$ of $\mathscr{V}$.

As a consequence of our results, for many probabilistic arguments involving say, computations modulo a prime p (as is the case in modular algorithms), choosing p polynomial in the Bézout number is enough to ensure a "reasonable" probability of success. We will illustrate this in the last section of this paper.

Organization of the paper. The paper is organized as follows. We start by recalling known material on Chow forms (Section 2) and height theory (Section 3). The next sections give a specialization property for Chow forms, first in dimension 1 (Section 4), then more generally under Assumption 2 (Section 5). This will enable us to predict suitable denominators for the polynomials $(N_1, \ldots, N_n)$ and $(T_1, \ldots, T_n)$, and give some first height estimates in Section 6; bounds on the numerators are obtained by interpolation in Section 7, completing the proof. Finally, Section 8 illustrates the use of our results by providing a probability analysis of a modular approach to estimate the degrees in $(T_1, \ldots, T_n)$.

Notation.

- If F is a polynomial or a set of polynomials, $Z(F)$ denotes its set of zeros, in either an affine, a projective or a multi-projective space, this being clear from to the context.
- Notation using superscripts such as $\mathbf{U}^i = U_0^i, \ldots, U_n^i$ *does not* denote powers.
- As in the introduction, when speaking of an algebraic set defined over an unspecified field k, we will mainly use the notation V. For an algebraic set defined over $\mathbb{Q}$ and lying

in some space such as $\mathbb{C}^{m+n}$, we will use the notation $\mathscr{V}$; the corresponding algebraic set defined over the rational function field $\mathbb{Q}(\mathbf{Y})$ will be denoted $\mathscr{V}^\star$.

2 Chow forms

We review basic material on the Chow forms of an equidimensional algebraic set. In this section, k is a field of characteristic 0 and $V \subset \overline{k}^n$ is an equidimensional algebraic set defined over k, of dimension r. Let $\mathbf{X} = X_1, \dots, X_n$ be the coordinates in $\overline{k}^n$ and let X_0 be an homogenization variable. For $i = 0, \dots, r$, let $\mathbf{U}^i = U_0^i, \dots, U_n^i$ be new indeterminates, and associate them with the bilinear forms

$$L_i: \ U_0^i X_0 + \cdots + U_n^i X_n.$$

Let then $\overline{V}$ be the projective closure of V in $\mathbb{P}^n(\overline{k})$, and consider the incidence variety

$$W = \overline{V} \cap Z(L_0, \dots, L_r) \subset \overline{V} \times \underbrace{\mathbb{P}^n(\overline{k}) \times \cdots \times \mathbb{P}^n(\overline{k})}_{r+1}.$$

The image of the projection $W \to \mathbb{P}^n(\overline{k}) \times \cdots \times \mathbb{P}^n(\overline{k})$ is a hypersurface. A *Chow form* of V is a multi-homogeneous squarefree polynomial in $\overline{k}[\mathbf{U}^0, \dots, \mathbf{U}^r]$ defining this hypersurface. All Chow forms thus coincide up to a constant (non-zero) multiplicative factor in $\overline{k}$; since V is defined over k, Chow forms with coefficients in k exist. The degree of a Chow form in the group of variables $\mathbf{U}^i$ is the degree of V.

Note also the following fact: given an ideal I of $k[X_1, \dots, X_n]$, a field k' containing k and the extension $I' = I \cdot k'[X_1, \dots, X_n]$, any Chow form of $V = Z(I) \subset \overline{k}^n$ is also a Chow form of $V' = Z(I') \subset \overline{k}'^n$ (because the image of the projection described above is defined over k).

Finally, consider the special case $r = 0$, and let $I \subset k[X_1, \dots, X_n]$ be the defining ideal of V. Then, the Chow forms of V are closely related to the characteristic polynomial of a "generic linear form" modulo I. To be more precise, let $\mathbf{U} = U_0, \dots, U_n$ be the indeterminates of the Chow forms of V (since the dimension r equals 0, we can drop the superscript ^{0} here). Over $\overline{k}$, the Chow forms of V admit the factorization

$$c \prod_{x \in V} (U_0 + U_1 x_1 + \cdots + U_n x_n) \in \overline{k}[\mathbf{U}], \tag{1}$$

where c is in $\overline{k}$, and $x = (x_1, \dots, x_n)$. We will distinguish two particular cases:

- taking $c = 1$ in (1), we obtain what we will call the *monic* Chow form of V (which has coefficients in k);
- in the particular case $k = \mathbb{Q}(\mathbf{Y})$, a *primitive* Chow form is a Chow form in $\mathbb{Z}[\mathbf{Y}, \mathbf{U}] = \mathbb{Z}[\mathbf{Y}][\mathbf{U}] \subset \mathbb{Q}(\mathbf{Y})[\mathbf{U}]$, with content ± 1 (the content is the gcd of the coefficients in $\mathbb{Z}[\mathbf{Y}]$). Primitive Chow forms are unique, up to sign.

3 Absolute values and height

Next, we recall the definitions and properties of absolute values and heights for polynomials and algebraic sets. Our references are (Lang, 1983; McCarthy, 1991; Philippon, 1995; Sombra, 1998; Krick et al., 2001); our presentation follows that of Dahan and Schost (2004), which itself is strongly inspired by Krick et al. (2001). The proofs of all statements given here can be found in these references.

3.1 Absolute values

An *absolute value* v on a field k is a multiplicative map $k \to \mathbb{R}^+$, such that $v(a) = 0$ if and only if $a = 0$, and for all $a, b \in k^2$, we have

$$v(a+b) \leq v(a) + v(b).$$

If the stronger inequality

$$v(a+b) \leq \max(v(a), v(b))$$

holds for all $a, b \in k^2$, v is called *non-Archimedean*, and *Archimedean* otherwise. In any case, we will write $\ell_v(x) = \log(v(x))$, for $x \neq 0$.

A family M_k of absolute values on k verifies the *product formula* if for every $x \in k - \{0\}$, there are only a finite number of v in M_k such that $v(x) \neq 1$, and the equality

$$\prod_{v \in \mathsf{M}_k} v(x) = 1$$

holds. In this case, we denote by NA_k and A_k the non-Archimedean and Archimedean absolute values in M_k, and write $\mathsf{M}_k = (\mathsf{NA}_k, \mathsf{A}_k)$.

Our first example of a valuated field is $k = \mathbb{Q}$. Let $\mathcal{P}$ be the set of prime numbers, so that each x in $\mathbb{Q} - \{0\}$ has the unique factorization

$$x = \pm \prod_{p \in \mathcal{P}} p^{\mathrm{ord}_p(x)}.$$

For each prime p, $x \mapsto v_p(x) = p^{-\mathrm{ord}_p(x)}$ defines a non-Archimedean absolute value. Denoting $x \mapsto v_\infty(x) = |x|$ the usual Archimedean absolute value, we let $\mathsf{M}_\mathbb{Q} = (\{v_p,\ p \in \mathcal{P}\},\ \{v_\infty\})$, so that that $\mathsf{A}_\mathbb{Q} = \{v_\infty\}$. One easily checks that $\mathsf{M}_\mathbb{Q}$ satisfies the product formula.

The second example is $k = K(\mathbf{Y})$, with $\mathbf{Y} = Y_1, \ldots, Y_m$ and K a field. Let $\mathcal{S}$ be a set of irreducible polynomials in $K[\mathbf{Y}]$, such that each x in $K(\mathbf{Y}) - \{0\}$ has the factorization

$$x = c \prod_{S \in \mathcal{S}} S^{\mathrm{ord}_S(x)}, \quad c \in K.$$

Then each S in $\mathcal{S}$ defines a non-Archimedean absolute value $x \mapsto v_S(x) = e^{-\deg(S)\ \mathrm{ord}_S(x)}$. An additional non-Archimedean absolute value is given by $x \mapsto v_{\deg}(x) = e^{\deg(x)}$, where $\deg(x)$

is defined as $\deg(n) - \deg(d)$, with $n, d \in K[\mathbf{Y}]$ and $x = n/d$. We define $\mathsf{M}_{K(\mathbf{Y})} = (\{v_S,\ S \in \mathcal{S}\} \cup \{v_{\deg}\},\ \emptyset)$, so that $\mathsf{A}_{K(\mathbf{Y})}$ is empty. As before, $\mathsf{M}_{K(\mathbf{Y})}$ satisfies the product formula, though we will not use this fact here.

Finally, we can point out that the definition of height of an integer we gave in the introduction fits with the definitions given here. Indeed, in general, the height of a non-zero element x in a field k with absolute value M_k that satisfy the product formula is $h(x) = \sum_{v \in \mathsf{M}_k} \max(0, \ell_v(x))$; we recover the particular case of the introduction for $k = \mathbb{Q}$. In particular, for x in $\mathbb{Z} - \{0\}$, $h(x) = \ell_{v_\infty}(x)$.

3.2 Absolute values of polynomials

We next define absolute values and Mahler measures for polynomials over the field k, and give a few useful inequalities.

Absolute values. If f is a non-zero polynomial with coefficients in k, for any absolute value v on k, we define the *v-adic absolute value* of f as

$$\ell_v(f) = \max_\beta\{\ell_v(f_\beta)\},$$

where f_β are the non-zero coefficients of f. We give here a few obvious consequences of this definition, for situations that will be considered later on. In the first example, k is $\mathbb{Q}$, and we consider polynomials in $\mathbb{Q}[\mathbf{Y}]$.

- For f in $\mathbb{Q}[\mathbf{Y}]$, $\ell_{v_p}(f) \leq 0$ for all primes p if and only if f is in $\mathbb{Z}[\mathbf{Y}]$, and $\ell_{v_p}(f) = 0$ for all primes p if and only if f is in $\mathbb{Z}[\mathbf{Y}]$ and has content ± 1.
- For f in $\mathbb{Z}[\mathbf{Y}]$, $\ell_{v_\infty}(f)$ is the maximum of the heights of the non-zero coefficients of f.

In the next example, the base field k is $\mathbb{Q}(\mathbf{Y})$, and we consider polynomials in $\mathbb{Q}(\mathbf{Y})[\mathbf{X}]$ and the absolute values $\mathsf{M}_{K(\mathbf{Y})} = (\{v_S,\ S \in \mathcal{S}\} \cup \{v_{\deg}\},\ \emptyset)$ mentioned before.

- For f in $\mathbb{Q}(\mathbf{Y})[\mathbf{X}]$, $\ell_{v_S}(f) \leq 0$ for all S in $\mathcal{S}$ if and only if f is in $\mathbb{Q}[\mathbf{Y}][\mathbf{X}]$.
- For f in $\mathbb{Q}[\mathbf{Y}][\mathbf{X}]$, $\ell_{v_{\deg}}(f)$ is the maximum of the degrees of the coefficients of f (which are in $\mathbb{Q}[\mathbf{Y}]$).
- By Gauss' Lemma, for p prime, the p-adic absolute value v_p defined on $\mathbb{Q}$ extend to a non-Archimedean absolute value v_p on $\mathbb{Q}(\mathbf{Y})$. For f in $\mathbb{Q}[\mathbf{Y}][\mathbf{X}]$, $\ell_{v_p}(f) \leq 0$ holds for all primes p if and only if f is actually in $\mathbb{Z}[\mathbf{Y}][\mathbf{X}]$.

Mahler measures. The following discussion is devoted to the case $k = \mathbb{Q}$. In this case, we introduce Mahler measures, which are closely related to Archimedean absolute values, but possess an extra additivity property. If f is in $\mathbb{Q}[\mathbf{X}^1, \ldots, \mathbf{X}^r]$, where each $\mathbf{X}^i$ is a group of n variables, we define the *r, n-Mahler measure* $\mathsf{m}(f, r, n)$ as

$$\mathsf{m}(f, r, n) = \int_{S_n^r} \log|f|\, \mu_n^r,$$

where $S_n \subset \mathbb{C}^n$ is the complex sphere of dimension n, and μ_n is the Haar measure of mass 1 over S_n.

Remark that if f depends on r variables, the $r, 1$-Mahler measure $\mathsf{m}(f, r, 1)$ is the "classical" one, obtained by integration over the product of r unit circles.

Useful inequalities. We conclude by giving basic inequalities for absolute values and Mahler measures. If v is non-Archimedean over a field k, we have (Gauss' lemma)

- $\mathbf{N_1}$ $\ell_v(f_1 f_2) = \ell_v(f_1) + \ell_v(f_2)$ for any polynomials f_1, f_2 in $k[\mathbf{Y}]$.

If $k = \mathbb{Q}$ and $v = v_\infty$ is the Archimedean absolute value on $\mathbb{Q}$, we have:

- $\mathbf{A_1}$ $\ell_{v_\infty}(f) \leq \mathsf{m}(f, r(n+1), 1) + rd \log(n+2)$ if f is a polynomial in r groups of $n+1$ variables, of degree at most d in each group.
- $\mathbf{A_2}$ $\mathsf{m}(f, r(n+1), 1) \leq \mathsf{m}(f, r, n+1) + rd \sum_{i=1}^{n} \frac{1}{2i}$ if f is a polynomial in r groups of $n+1$ variables, of degree at most d in each group.
- $\mathbf{A_3}$ $\ell_{v_\infty}(f_1) + \ell_{v_\infty}(f_2) \leq \ell_{v_\infty}(f_1 f_2) + 4d \log(n+1)$, if f_1 and f_2 are polynomials in n variables of degree at most d.

3.3 Height of algebraic sets

We finally define heights of algebraic sets defined over $\mathbb{Q}$ (though the construction can be extended to any field with a set of absolute values satisfying the product formula). First, we note that as a general rule, we will denote the degree of an algebraic set $\mathscr{V}$ by $d_{\mathscr{V}}$, and its height by $h_{\mathscr{V}}$.

Let thus $\mathscr{V} \subset \mathbb{C}^k$ be an m-equidimensional algebraic set defined over $\mathbb{Q}$ and let $\mathscr{C}$ be a Chow form of $\mathscr{V}$ with coefficients in $\mathbb{Q}$. We use the non-Archimedean absolute values and Mahler measures of $\mathscr{C}$ to define the height of $\mathscr{V}$. Let $\mathsf{M}_{\mathbb{Q}} = (\{v_p,\, p \in \mathcal{P}\},\ \{v_\infty\})$ be the absolute values on $\mathbb{Q}$ introduced before. Then, as said above, we let $d_{\mathscr{V}}$ be the degree of $\mathscr{V}$, and we define its height $h_{\mathscr{V}}$ as

$$h_{\mathscr{V}} = \sum_{p \in \mathcal{P}} \ell_{v_p}(\mathscr{C}) + \mathsf{m}(\mathscr{C}, m+1, k+1) + (m+1) d_{\mathscr{V}} \sum_{i=1}^{k} \frac{1}{2i}.$$

This is well-defined, as a consequence of the product formula for $\mathsf{M}_{\mathbb{Q}}$. Then, the definition extends by additivity to arbitrary algebraic sets.

4 A specialization property

Let k be a field, and let ε and $\mathbf{X} = X_1, \ldots, X_n$ be indeterminates over k. In this section, we work in the affine space $\overline{k}^{n+1}$, taking ε and $\mathbf{X}$ for coordinates, and we let π be the projection

$$\begin{array}{rccc} \pi : & \overline{k}^{n+1} & \to & \overline{k} \\ & (e, x_1, \ldots, x_n) & \mapsto & e. \end{array}$$

Let V be an algebraic set in $\overline{k}^{n+1}$, defined over k. We will show how to relate the Chow forms of the "generic fiber" of π to those of the special fiber above $e = 0$. The results of this section will be used only in Section 5.

We write V as the union $V_0 \cup V_1 \cup V_{\geq 2}$, where:

- V_0 (resp. V_1) is the union of the irreducible components of V of dimension 0 (resp. of dimension 1);
- $V_{\geq 2}$ is the union of the irreducible components of V of dimension at least 2;

remark that any of those can be empty. Let further $I \subset k[\varepsilon, \mathbf{X}]$ be the ideal defining V, let $I^\star$ be the extension of I in $k(\varepsilon)[\mathbf{X}]$ and let $V^\star \subset \overline{k(\varepsilon)}^n$ be the zero-set of $I^\star$. Then, we introduce the following conditions:

$\mathbf{G_1}$: The algebraic set $V^\star$ has dimension 0.

$\mathbf{G_2}$: The fiber $\pi^{-1}(0) \cap V$ has dimension 0.

$\mathbf{G_3}$: The fiber $\pi^{-1}(0) \cap V$ is contained in $V_1 \cup V_{\geq 2}$.

Let $\mathbf{U} = U_0, U_1, \ldots, U_n$ be indeterminates, to be used for Chow forms in dimension 0:

- Since $V^\star$ has dimension 0 by $\mathbf{G_1}$, its Chow forms are homogeneous polynomials in $\overline{k(\varepsilon)}[\mathbf{U}]$.
- Let us denote by W_0 the fiber $\pi^{-1}(0) \cap V$ (the motivation for this notation appears below). Since W_0 has dimension 0 by $\mathbf{G_2}$, its Chow forms are homogeneous polynomials in $\overline{k}[\mathbf{U}]$.

Proposition 1. *Suppose that $\mathbf{G_1}$, $\mathbf{G_2}$ and $\mathbf{G_3}$ hold. Let C be a Chow form of $V^\star$, and suppose that C belongs to the polynomial ring $k[\varepsilon, \mathbf{U}] \subset \overline{k(\varepsilon)}[\mathbf{U}]$. Then any Chow form of W_0 that belongs to $k[\mathbf{U}]$ divides $C(0, \mathbf{U})$ in $k[\mathbf{U}]$.*

Proof. Let $W \subset V_1$ be the reunion of all 1-dimensional components of V whose image by π is dense in $\overline{k}$; we shall actually mainly be interested in W in what follows. We start by the following easy lemma, which justifies our writing W_0 for the fiber $\pi^{-1}(0) \cap V$.

Lemma 1. *The fiber $W_0 = \pi^{-1}(0) \cap V$ is contained in W.*

Proof. Let us write W' for the reunion of all 1-dimensional components of V whose image by π is not dense in $\overline{k}$; then V_1 is the union of W and W'. With this notation, Assumption $\mathbf{G_3}$ asserts that W_0 is contained in $W \cup W' \cup V_{\geq 2}$.

The theorem on the dimension of fibers implies that all non-empty fibers of the restriction of π to either W' or $V_{\geq 2}$ have positive dimension. So, the fact that W_0 has dimension 0 (Assumption $\mathbf{G_2}$) implies that W_0 is contained in W. □

One easily checks that W is defined over k; let then $J \subset k[\varepsilon, \mathbf{X}]$ be its defining ideal, let $J^\star$ be the extension of J in $k(\varepsilon)[\mathbf{X}]$ and let $W^\star$ be the zero-set of $J^\star$. The following lemma shows that the "generic fibers" of π restricted to either V or W coincide.

Lemma 2. *The equality $V^\star = W^\star$ holds.*

Proof. We claim that all components of V that are not in W have a 0-dimensional image through π:

- For the 1-dimensional components, this is true by definition of W'.
- Suppose that a component in $V_{\geq 2}$ has a dense image through π. By the theorem on the dimensions of fibers, all fibers of π on this component have positive dimension. These two points imply that the algebraic set $V^\star$ must have positive dimension as well. This contradicts Assumption $\mathbf{G_1}$.

Thus, we can write the equality $I = J \cap J'$, where J' contains a non-zero polynomial in $k[\varepsilon]$. Then, the extension of J' to $k(\varepsilon)[\mathbf{X}]$ is the ideal $\langle 1 \rangle$, so that $I^\star = J^\star$; this proves the statement. $\square$

By Lemma 2, the Chow forms of $V^\star$ and $W^\star$ coincide; they belong to $\overline{k(\varepsilon)}[\mathbf{U}]$. Let thus C be a Chow form of $W^\star$ that belongs to the polynomial ring $k[\varepsilon, \mathbf{U}] \subset \overline{k(\varepsilon)}[\mathbf{U}]$. We will now establish the proposition, that is, prove that any Chow form of W_0 that belongs to $k[\mathbf{U}]$ divides $C(0, \mathbf{U})$ in $k[\mathbf{U}]$.

The proof is inspired by that of Sabia and Solernó (1995, Prop. 1). We first extend the coefficient field k, by adjoining to it the indeterminates $U_1, \ldots, U_n$; after this scalar extension, objects that were previously defined over k inherit the same denomination, but using $\mathfrak{fraktur}$ face: letting $\mathfrak{K}$ be the rational function field $k(U_1, \ldots, U_n)$, we thus define the following objects:

- $\mathfrak{J}$ is the extension of J in $\mathfrak{K}[\varepsilon, \mathbf{X}]$ and $\mathfrak{W}$ is its zero-set.

  Still denoting by π the projection on the first coordinate axis, we note that $\mathfrak{W}$ inherits the geometric properties of W: it has pure dimension 1, and the restriction of π to all its irreducible components is dominant.
- $\mathfrak{J}^\star$ is the extension of $\mathfrak{J} \subset \mathfrak{K}[\varepsilon, \mathbf{X}]$ in $\mathfrak{K}(\varepsilon)[\mathbf{X}]$. This is a 0-dimensional ideal.
- $\mathfrak{W}_0$ is the fiber $\pi^{-1}(0) \cap \mathfrak{W}$. Since W_0 has dimension 0, $\mathfrak{W}_0$ has dimension 0 as well.

The core of the proof is Lemma 3 below. Recall that $C \in k[\varepsilon, \mathbf{U}]$ is a Chow form of $W^\star$; we will see C in $\mathfrak{K}[\varepsilon, U_0]$, with $\mathfrak{K} = k(U_1, \ldots, U_n)$. We also introduce the map

$$\begin{array}{rccc} \varphi : & \mathfrak{W} & \to & \overline{\mathfrak{K}}^2 \\ & (e, x_1, \ldots, x_n) & \mapsto & (e, -U_1 x_1 - \cdots - U_n x_n). \end{array}$$

Lemma 3. *Seen in $\mathfrak{K}[\varepsilon, U_0]$, C vanishes on the image of φ.*

Proof. The closure of the image of φ has dimension 1; we let B be a squarefree polynomial in $\mathfrak{K}[\varepsilon, U_0]$ that defines this hypersurface. Note that B does not admit any non-constant factor in $\mathfrak{K}[\varepsilon]$, since all components of $\mathfrak{W}$ have a dense image through π. Our goal is to show that B divides C in $\mathfrak{K}[\varepsilon, U_0]$.

Let us see C in $\mathfrak{K}[\varepsilon][U_0]$ and let $c \in \mathfrak{K}[\varepsilon]$ be its leading coefficient. Since C is a Chow form of $W^\star$, Proposition 4.2.7 in (Cox et al., 1998) shows that C/c is the characteristic polynomial of the multiplication by $-U_1X_1 - \cdots - U_nX_n$ modulo $\mathfrak{J}^\star$.

On the other hand, Proposition 1 in (Schost, 2003b) shows that B/b is also the characteristic polynomial of the multiplication by $-U_1X_1 - \cdots - U_nX_n$ modulo $\mathfrak{J}^\star$, where $b \in \mathfrak{K}[\varepsilon]$ is the leading coefficient of B seen in $\mathfrak{K}[\varepsilon][U_0]$. We deduce from these considerations the equality $Bc = Cb$ in $\mathfrak{K}[\varepsilon, U_0]$; since B admits no factor in $\mathfrak{K}[\varepsilon]$, b divides c in $\mathfrak{K}[\varepsilon]$, which proves our claim. ☐

Specializing ε at 0, we deduce that $C(0, \mathbf{U}) \in \mathfrak{K}[U_0]$ vanishes on the image of the map

$$\begin{array}{rccc} \varphi_0 : & \mathfrak{W}_0 & \to & \overline{\mathfrak{K}} \\ & (x_1, \ldots, x_n) & \mapsto & -U_1x_1 - \cdots - U_nx_n. \end{array}$$

Hence, it admits the polynomial $\prod_{x \in \mathfrak{W}_0}(U_0 + U_1x_1 + \cdots + U_nx_n)$ as a factor. Note that this last polynomial is the monic Chow form of W_0; note also that the division takes place in $k[\mathbf{U}]$, since $C(0, \mathbf{U})$ and this Chow form are in $k[\mathbf{U}]$, and the Chow form is monic in U_0. Since all Chow forms of W_0 differ by a constant factor in $\overline{k}$, this concludes the proof of Proposition 1. ☐

Assumptions $\mathbf{G_1}$ and $\mathbf{G_2}$ will be easy to ensure; to conclude, we give sufficient conditions that ensure that $\mathbf{G_3}$ holds.

Lemma 4. *Let $I' \subset k[\varepsilon, \mathbf{X}]$ be an ideal such that $V = Z(I')$ and suppose that there exist $F_1, \ldots, F_n$ and Δ in $k[\varepsilon, \mathbf{X}]$ such that:*

- *the inclusions $\Delta I' \subset \langle F_1, \ldots, F_n \rangle \subset I'$ hold;*
- *$\Delta(0, \mathbf{X})$ is in $k - \{0\}$.*

Then V satisfies $\mathbf{G_3}$.

Proof. Let V' be the Zariski closure of $V - Z(\Delta)$: each irreducible component of V' is thus an irreducible component of V. Our assumptions imply that V' coincides with the Zariski closure of $Z(F_1, \ldots, F_n) - Z(\Delta)$. By Krull's theorem, all irreducible components of the zero-set $Z(F_1 \ldots, F_n)$ have dimension at least 1, so it is also the case for V'. To summarize, each irreducible component of V' is a positive-dimensional irreducible component of V, so that V' is contained in $V_1 \cup V_{\geq 2}$.

Now, since $\Delta(0, \mathbf{X})$ is in $k - \{0\}$, the fiber $\pi^{-1}(0) \cap V$ does not meet $Z(\Delta)$, so it is contained in V'. This proves that V satisfies Assumption $\mathbf{G_3}$. ☐

5 Chow forms for the generic solutions

We consider now an m-equidimensional algebraic set $\mathscr{V} \subset \mathbb{C}^{m+n}$ that satisfies Assumption 2. As in the introduction, we write the ambient coordinates as $\mathbf{Y}, \mathbf{X}$, with $\mathbf{Y} = Y_1, \ldots, Y_m$ and $\mathbf{X} = X_1, \ldots, X_n$, and we recall that Π_0 is the projection $\mathbb{C}^{m+n} \to \mathbb{C}^m$. We let $\mathscr{I}$ be the ideal defining $\mathscr{V}$, let $\mathscr{I}^\star$ be the extended ideal $\mathscr{I} \cdot \mathbb{Q}(\mathbf{Y})[\mathbf{X}]$ and let $\mathscr{V}^\star$ be the zero-set of $\mathscr{I}^\star$. In this section, we show how to obtain a Chow form of $\mathscr{V}^\star$ starting from a Chow form of $\mathscr{V}$.

The Chow forms of $\mathscr{V}$ are polynomials in $(m+1)(m+n+1)$ variables, which we write as $\mathbf{U}^i = U_0^i, \ldots, U_{m+n}^i$, for $i = 0, \ldots, m$. It will be helpful to have the following matrix notation for these indeterminates:

$$\mathbf{U}_{(0)} = \begin{bmatrix} U_0^0 \\ \vdots \\ U_0^m \end{bmatrix}, \mathbf{U}_{(\mathbf{Y})} = \begin{bmatrix} U_1^0 & \ldots & U_m^0 \\ \vdots & & \vdots \\ U_1^m & \ldots & U_m^m \end{bmatrix}, \ \mathbf{U}_{(\mathbf{X})} = \begin{bmatrix} U_{m+1}^0 & \ldots & U_{m+n}^0 \\ \vdots & & \vdots \\ U_{m+1}^m & \ldots & U_{m+n}^m \end{bmatrix}.$$

This choice of variables corresponds to seeing these Chow forms as polynomials defining the projection on $\mathbb{P}^{m+n}(\mathbb{C}) \times \cdots \times \mathbb{P}^{m+n}(\mathbb{C})$ of the incidence variety

$$\overline{\mathscr{V}} \cap Z(L_0, \ldots, L_m) \subset \overline{\mathscr{V}} \times \underbrace{\mathbb{P}^{m+n}(\mathbb{C}) \times \cdots \times \mathbb{P}^{m+n}(\mathbb{C})}_{m+1},$$

where $\overline{\mathscr{V}}$ is the projective closure of $\mathscr{V}$, where for all $0 \leq i \leq m$, L_i is the bilinear form

$$U_0^i T_0 + U_1^i Y_1 + \cdots + U_m^i Y_m + U_{m+1}^i X_1 + \cdots + U_{m+n}^i X_n,$$

and where T_0 is an homogenization variable. We will denote the Chow forms of $\mathscr{V}$ by $\mathscr{C}$.

Assumption 2 implies that $\mathscr{V}^\star \subset \overline{\mathbb{Q}(\mathbf{Y})}^n$ has dimension 0, so we write $\mathbf{U} = U_0, \ldots, U_n$ for the indeterminates of the Chow forms of $\mathscr{V}^\star$. These Chow forms are in $\overline{\mathbb{Q}(\mathbf{Y})}[\mathbf{U}]$; however, we will be interested in those belonging to the subring $\mathbb{Z}[\mathbf{Y}, \mathbf{U}]$ of $\overline{\mathbb{Q}(\mathbf{Y})}[\mathbf{U}]$.

Krick et al. (2001) answer our question under an additional assumption. Instead of requiring the restriction of Π_0 to $\mathscr{V}$ to be dominant, their result requires the following stronger assumption:

Assumption 3. *The restriction of Π_0 to $\mathscr{V}$ is finite, of degree the degree of $\mathscr{V}$.*

Then, the following relation holds (Krick et al., 2001, Lemma 2.14).

Proposition 2. *Let $\mathscr{C} \in \mathbb{Z}[\mathbf{U}^0, \ldots, \mathbf{U}^m]$ be a Chow form of $\mathscr{V}$ and let $\mathscr{C}^\star \in \mathbb{Z}[\mathbf{Y}, \mathbf{U}]$ be the polynomial obtained by performing the following substitution in $\mathscr{C}$:*

$$\mathbf{U}_{(0)} \leftarrow \begin{bmatrix} U_0 \\ Y_1 \\ \vdots \\ Y_m \end{bmatrix}, \ \mathbf{U}_{(\mathbf{Y})} \leftarrow \begin{bmatrix} 0 & \ldots & 0 \\ -1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & -1 \end{bmatrix}, \ \mathbf{U}_{(\mathbf{X})} \leftarrow \begin{bmatrix} U_1 & \ldots & U_n \\ 0 & \ldots & 0 \\ \vdots & & \vdots \\ 0 & \ldots & 0 \end{bmatrix}.$$

If $\mathscr{V}$ satisfies Assumption 3, then, seen in $\overline{\mathbb{Q}(\mathbf{Y})}[\mathbf{U}]$, $\mathscr{C}^\star$ is a Chow form of $\mathscr{V}^\star$; in particular, it is non-zero.

In our more general setting, one can still perform this substitution, but the result might be zero. For instance, the algebraic set $\mathscr{V}$ defined by the system in $\mathbb{Q}[Y_1, Y_2, X_1, X_2]$

$$X_1 + 1 + Y_1 X_2 = 0, \quad X_2 + Y_2 X_1 = 0$$

satisfies Assumption 2 but not Assumption 3. Indeed, since

$$\langle X_1 + 1 + Y_1 X_2, X_2 + Y_2 X_1 \rangle \cap \mathbb{Q}[Y_1, Y_2] = \langle 0 \rangle,$$

the projection of $\mathscr{V}$ on the (Y_1, Y_2)-space is dense, and the associated triangular set in $\mathbb{Q}(Y_1, Y_2)[X_1, X_2]$ is $T_1(X_1) = X_1 + 1/(1 - Y_1 Y_2)$ and $T_2(X_1, X_2) = X_2 + Y_2 X_1$; this gives Assumption 2. To see why Assumption 3 is not verified by this example, note that for any $(y_1, y_2) \in \mathbb{C}^2$ with $y_1 y_2 \neq 1$, the fiber $\Pi_0^{-1}(y_1, y_2)$ has cardinality 1 (whereas $\mathscr{V}$ has degree 4); if $y_1 y_2 = 1$, the fiber is empty. As it turns out, the Chow forms of $\mathscr{V}$ are polynomials in 15 variables, having 6648 monomials, and performing the substitution of Proposition 2 in them gives zero.

The following theorem shows how to bypass this difficulty, by providing a suitable multiple of a Chow form of $\mathscr{V}^\star$. To this effect, we need to introduce a new indeterminate ε.

Theorem 2. *Let $\mathscr{C} \in \mathbb{Z}[\mathbf{U}^0, \dots, \mathbf{U}^m]$ be a Chow form of $\mathscr{V}$ and let $\mathscr{C}_\varepsilon \in \mathbb{Z}[\mathbf{Y}, \mathbf{U}, \mathbf{U}^1, \dots, \mathbf{U}^m, \varepsilon]$ be the polynomial obtained by performing the following substitution in $\mathscr{C}$:*

$$\mathbf{U}_{(0)} \leftarrow \begin{bmatrix} U_0 \\ Y_1 \\ \vdots \\ Y_m \end{bmatrix}, \quad \mathbf{U}_{(\mathbf{Y})} \leftarrow \begin{bmatrix} 0 & \dots & 0 \\ -1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & -1 \end{bmatrix}, \quad \mathbf{U}_{(\mathbf{X})} \leftarrow \begin{bmatrix} U_1 & \dots & U_n \\ \varepsilon U^1_{m+1} & \dots & \varepsilon U^1_{m+n} \\ \vdots & & \vdots \\ \varepsilon U^m_{m+1} & \dots & \varepsilon U^m_{m+n} \end{bmatrix}.$$

Then, $\mathscr{C}_\varepsilon$ is not zero. Let $\mathscr{C}_0 \in \mathbb{Z}[\mathbf{Y}, \mathbf{U}, \mathbf{U}^1 \dots, \mathbf{U}^m]$ be the coefficient of lowest degree in ε of $\mathscr{C}_\varepsilon$, and let finally $\mathscr{C}^\star \in \mathbb{Z}[\mathbf{Y}, \mathbf{U}]$ be a primitive Chow form of $\mathscr{V}^\star$. Then $\mathscr{C}^\star$ divides $\mathscr{C}_0$ in $\mathbb{Z}[\mathbf{Y}, \mathbf{U}, \mathbf{U}^1, \dots, \mathbf{U}^m]$.

Ingredients used in the proof. The proof will occupy the remainder of this section. Let us start by explaining the ingredients of it. We will apply a generic change of variables, to get back under Assumption 3; introducing the matrix of this change of variables will require to work over a purely transcendental extension of $\mathbb{Q}$.

- In the first step of the proof, we will work over the field $\mathbb{L} = \mathbb{Q}(\mathbf{T}^1, \dots, \mathbf{T}^m, \varepsilon)$, where $\mathbf{T}^i = T^i_1, \dots, T^i_n$ are new indeterminates; we will use $\mathbf{T}^1, \dots, \mathbf{T}^m$ and ε to perform our change of variables.

- In the last step of the proof, we let $\varepsilon \to 0$, by working over the coefficient fields $\mathbb{K} = \mathbb{Q}(\mathbf{T}^1, \dots, \mathbf{T}^m, \mathbf{Y})$ and $\mathbb{M} = \mathbb{Q}(\mathbf{T}^1, \dots, \mathbf{T}^m, \varepsilon, \mathbf{Y})$, so that $\mathbb{M} = \mathbb{K}(\varepsilon) = \mathbb{L}(\mathbf{Y})$. The connection will be done using the results of Section 4.

This lattice of fields is represented in the following diagram:

$$\begin{array}{ccccc} & & \mathbb{L} = \mathbb{Q}(\mathbf{T}^1, \dots, \mathbf{T}^m, \varepsilon) & & \\ & \nearrow & & \searrow & \\ \mathbb{Q} & & & & \mathbb{M} = \mathbb{Q}(\mathbf{T}^1, \dots, \mathbf{T}^m, \varepsilon, \mathbf{Y}) = \mathbb{K}(\varepsilon) = \mathbb{L}(\mathbf{Y}). \\ & \searrow & & \nearrow & \\ & & \mathbb{K} = \mathbb{Q}(\mathbf{T}^1, \dots, \mathbf{T}^m, \mathbf{Y}) & & \end{array}$$

5.1 Application of a generic change of variables

First, we work over $\mathbb{L} = \mathbb{Q}(\mathbf{T}^1, \dots, \mathbf{T}^m, \varepsilon)$. To recover Assumption 3, we define the following new coordinates for $\overline{\mathbb{L}}^{m+n}$:

$$\begin{bmatrix} \widetilde{X}_1 \\ \vdots \\ \widetilde{X}_n \end{bmatrix} = \begin{bmatrix} X_1 \\ \vdots \\ X_n \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} \widetilde{Y}_1 \\ \vdots \\ \widetilde{Y}_m \end{bmatrix} = \begin{bmatrix} Y_1 \\ \vdots \\ Y_m \end{bmatrix} + \begin{bmatrix} \varepsilon T_1^1 & \dots & \varepsilon T_n^1 \\ \vdots & & \vdots \\ \varepsilon T_1^m & \dots & \varepsilon T_n^m \end{bmatrix} \begin{bmatrix} X_1 \\ \vdots \\ X_n \end{bmatrix}. \qquad (2)$$

In all that follows, we write for short $\widetilde{\mathbf{Y}} = \widetilde{Y}_1, \dots, \widetilde{Y}_m$ and $\widetilde{\mathbf{X}} = \widetilde{X}_1, \dots, \widetilde{X}_n$. Then, we define the ideal $\mathscr{J}$ as

$$\mathscr{J} = \langle\, F(\widetilde{\mathbf{Y}}, \widetilde{\mathbf{X}}) \mid F \in \mathscr{I} \,\rangle \quad \subset \quad \mathbb{L}[\mathbf{Y}, \mathbf{X}],$$

and we let $\mathscr{W} \subset \overline{\mathbb{L}}^{m+n}$ be the zero-set of $\mathscr{J}$. Note that $\mathscr{W}$ is equidimensional of dimension m, and has the same degree as $\mathscr{V}$.

Since $\mathscr{W}$ is in generic coordinates, we will apply Proposition 2 to obtain a Chow form of its "generic solutions". Recall the definition $\mathbb{M} = \mathbb{L}(\mathbf{Y})$; we let $\mathscr{J}^\star$ be the extension of $\mathscr{J}$ in the polynomial ring $\mathbb{L}(\mathbf{Y})[\mathbf{X}] = \mathbb{M}[\mathbf{X}]$, and denote by $\mathscr{W}^\star$ its set of solutions. Then, the first step of the proof of Theorem 2 is the following.

Proposition 3. *The algebraic set $\mathscr{W}^\star$ has dimension 0. Let further $\mathscr{C} \in \mathbb{Z}[\mathbf{U}^0, \dots, \mathbf{U}^m]$ be a Chow form of $\mathscr{V}$, and let $\mathscr{C}^\star$ be the polynomial in $\mathbb{Z}[\mathbf{Y}, \mathbf{U}, \mathbf{T}^1, \dots, \mathbf{T}^m, \varepsilon]$ obtained by performing the following substitution in $\mathscr{C}$:*

$$\mathbf{U}_{(0)} \leftarrow \begin{bmatrix} U_0 \\ Y_1 \\ \vdots \\ Y_m \end{bmatrix}, \quad \mathbf{U}_{(\mathbf{Y})} \leftarrow \begin{bmatrix} 0 & \dots & 0 \\ -1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & -1 \end{bmatrix}, \quad \mathbf{U}_{(\mathbf{X})} \leftarrow \begin{bmatrix} U_1 & \dots & U_n \\ \varepsilon T_1^1 & \dots & \varepsilon T_n^1 \\ \vdots & & \vdots \\ \varepsilon T_1^m & \dots & \varepsilon T_n^m \end{bmatrix}.$$

Then, seen in $\mathbb{M}[\mathbf{U}]$, $\mathscr{C}^\star$ is a Chow form of $\mathscr{W}^\star$; in particular, it is non-zero.

This subsection is devoted to give a proof of this proposition. The key element is the following lemma.

Lemma 5. *The algebraic set $\mathscr{W}$ satisfies Assumption 3; in particular, $\mathscr{W}^\star$ has dimension 0.*

Proof. Let $d_{\mathscr{V}}$ be the degree of $\mathscr{V}$. By definition of the degree, there exists a Zariski-dense subset Γ of $\mathbb{C}^{m(m+n+1)}$ such that for all choices of $(u_0^i, \ldots, u_{m+n}^i)_{1 \le i \le m}$ in Γ, the algebraic set

$$\mathscr{V} \cap Z(\{u_0^i + u_1^i Y_1 + \cdots + u_m^i Y_m + u_{m+1}^i X_1 + \cdots + u_{m+n}^i X_n\}_{1 \le i \le m}) \tag{3}$$

has dimension 0 and cardinality $d_{\mathscr{V}}$, and furthermore the determinant

$$\begin{vmatrix} u_1^1 & \ldots & u_m^1 \\ \vdots & & \vdots \\ u_1^m & \ldots & u_m^m \end{vmatrix}$$

is non-zero. Thus, there exists

$$\begin{bmatrix} u_0^1 \\ \vdots \\ u_0^m \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} u_1^1 & \ldots & u_m^1 \\ \vdots & & \vdots \\ u_1^m & \ldots & u_m^m \end{bmatrix} \tag{4}$$

in $\mathbb{Q}^{m(m+1)}$ and an open dense subset Γ' of $\mathbb{C}^{mn}$ such that for all

$$\begin{bmatrix} u_{m+1}^1 & \ldots & u_{m+n}^1 \\ \vdots & & \vdots \\ u_{m+1}^m & \ldots & u_{m+n}^m \end{bmatrix}$$

in Γ', the former property holds. We keep the quantities of (4) fixed, and we define $y_1, \ldots, y_m$ by

$$\begin{bmatrix} y_1 \\ \vdots \\ y_m \end{bmatrix} = - \begin{bmatrix} u_1^1 & \ldots & u_m^1 \\ \vdots & & \vdots \\ u_1^m & \ldots & u_m^m \end{bmatrix}^{-1} \begin{bmatrix} u_0^1 \\ \vdots \\ u_0^m \end{bmatrix}.$$

Besides, we let $\Lambda \subset \mathbb{C}^{mn}$ be the image of Γ' through the map

$$\begin{bmatrix} u_{m+1}^1 & \ldots & u_{m+n}^1 \\ \vdots & & \vdots \\ u_{m+1}^m & \ldots & u_{m+n}^m \end{bmatrix} \mapsto - \begin{bmatrix} u_1^1 & \ldots & u_m^1 \\ \vdots & & \vdots \\ u_1^m & \ldots & u_m^m \end{bmatrix}^{-1} \begin{bmatrix} u_{m+1}^1 & \ldots & u_{m+n}^1 \\ \vdots & & \vdots \\ u_{m+1}^m & \ldots & u_{m+n}^m \end{bmatrix};$$

so that Λ is dense in $\mathbb{C}^{mn}$. For any choice of $(\mathbf{t}^i = (t_1^i, \ldots, t_n^i))_{1 \le i \le m}$ in Λ, the algebraic set

$$\mathscr{V} \cap Z(\{Y_i - t_1^i X_1 - \cdots - t_n^i X_n - y_i\}_{1 \le i \le m}) \ \subset \ \mathbb{C}^{m+n}$$

has dimension 0 and cardinality $d_{\mathscr{V}}$. Let finally $\Lambda' \subset \mathbb{C}^{mn+1}$ be the preimage of Λ by the surjective map $(\mathbf{t}^1, \ldots, \mathbf{t}^m, e) \mapsto (e\mathbf{t}^1, \ldots, e\mathbf{t}^m)$, where $e\mathbf{t}^i = (et_1^i, \ldots, et_n^i)$. Then, Λ' is dense in $\mathbb{C}^{mn+1}$ and for all $(\mathbf{t}^1, \ldots, \mathbf{t}^m, e)$ in Λ', the algebraic set

$$\mathscr{V} \cap Z(\{Y_i - et_1^i X_1 - \cdots - et_n^i X_n - y_i\}_{1 \le i \le m}) \ \subset \ \mathbb{C}^{m+n}$$

has dimension 0 and cardinality $d_{\mathscr{V}}$. Since this property holds for $(\mathbf{t}^1, \dots, \mathbf{t}^m, e)$ in a dense subset of $\mathbb{C}^{mn+1}$, we deduce from (Heintz, 1983, Prop. 1) that the algebraic set defined over $\mathbb{L} = \mathbb{Q}(\mathbf{T}^1, \dots, \mathbf{T}^m, \varepsilon)$ by

$$\mathscr{V} \cap Z(\{Y_i - \varepsilon T_1^i X_1 - \dots - \varepsilon T_n^i X_n - y_i\}_{1 \le i \le m}) \subset \overline{\mathbb{L}}^{m+n}$$

has dimension 0 and cardinality $d_{\mathscr{V}}$. But this algebraic set is isomorphic through the change of variables $\mathbf{Y} \leftrightarrow \widetilde{\mathbf{Y}}$ to

$$\mathscr{W} \cap Z(\{Y_i - y_i\}_{1 \le i \le m}) \subset \overline{\mathbb{L}}^{m+n},$$

which is the fiber $\Pi_0^{-1}(y_1, \dots, y_m) \cap \mathscr{W}$.

To summarize, $\mathscr{W}$ is an m-equidimensional algebraic set, and the fiber $\Pi_0^{-1}(y_1, \dots, y_m) \cap \mathscr{W}$ has a cardinality equal to the degree of $\mathscr{W}$. The first point of (Krick et al., 2001, Lemma 2.14) implies that under these conditions, $\mathscr{W}$ satisfies Assumption 3. □

We can now conclude the proof of Proposition 3. If $\mathscr{C}$ is a Chow form of $\mathscr{V} = Z(\mathscr{I})$, since $\mathbb{L} = \mathbb{Q}(\mathbf{T}^1, \dots, \mathbf{T}^m, \varepsilon)$, $\mathscr{C}$ is also a Chow form of the algebraic set defined by the extension of $\mathscr{I}$ in $\mathbb{L}[\mathbf{Y}, \mathbf{X}]$ (we mentioned this fact in Section 2). Since $\mathscr{W}$ is obtained by applying a linear change of variables to this algebraic set, we can deduce a Chow form of $\mathscr{W}$ by changing the variables in $\mathscr{C}$: Let $\widetilde{\mathbf{U}}_{(\mathbf{X})}$ be the matrix

$$\begin{bmatrix} U_{m+1}^0 & \dots & U_{m+n}^0 \\ \vdots & & \vdots \\ U_{m+1}^m & \dots & U_{m+n}^m \end{bmatrix} - \begin{bmatrix} U_1^0 & \dots & U_m^0 \\ \vdots & & \vdots \\ U_1^m & \dots & U_m^m \end{bmatrix} \begin{bmatrix} \varepsilon T_1^1 & \dots & \varepsilon T_n^1 \\ \vdots & & \vdots \\ \varepsilon T_1^m & \dots & \varepsilon T_n^m \end{bmatrix};$$

then $\mathscr{C}(\mathbf{U}_{(0)}, \mathbf{U}_{(\mathbf{Y})}, \widetilde{\mathbf{U}}_{(\mathbf{X})})$ is a Chow form of $\mathscr{W}$. Now, we apply Proposition 2 to $\mathscr{W}$, which is legitimate by the previous lemma; this gives the announced result.

5.2 Setup for the specialization $\varepsilon = 0$

The final part of the proof consists in letting $\varepsilon = 0$ in the previous result; this will be done in the next subsection, by applying the results of Section 4. The purpose of this subsection is to prove that the necessary assumptions hold. We work here using $\mathbb{K} = \mathbb{Q}(\mathbf{T}^1, \dots, \mathbf{T}^m, \mathbf{Y})$ as our base field. Using the notation of Equations (2), we define the ideal $\mathscr{L}$ as

$$\mathscr{L} = \langle\ F(\widetilde{\mathbf{Y}}, \widetilde{\mathbf{X}}) \mid F \in \mathscr{I}\ \rangle \ \subset \mathbb{K}[\varepsilon, \mathbf{X}].$$

Let $\mathscr{Z} \subset \overline{\mathbb{K}}^{n+1}$ be the zero-set of $\mathscr{L}$. As in Section 4, we write π for the projection map $(e, x_1, \dots, x_n) \mapsto e$; our purpose is to establish the following proposition.

Proposition 4. *The algebraic set $\mathscr{Z}$ satisfies Assumptions $\mathbf{G_1}$, $\mathbf{G_2}$ and $\mathbf{G_3}$ of Section 4.*

Remark that there exist polynomials $F_1, \dots, F_n$ in $\mathbb{Q}[\mathbf{Y}, \mathbf{X}]$ that generate the extended ideal $\mathscr{I} \cdot \mathbb{Q}(\mathbf{Y})[\mathbf{X}]$, since this ideal is 0-dimensional (actually, we can take the polynomials $T_1, \dots, T_n$, whose existence is guaranteed by Assumption 2, and clear their denominators). We will first relate the ideals $\mathscr{L}$ and $\langle F_1(\widetilde{\mathbf{Y}}, \widetilde{\mathbf{X}}), \dots, F_n(\widetilde{\mathbf{Y}}, \widetilde{\mathbf{X}})\rangle$ in $\mathbb{K}[\varepsilon, \mathbf{X}]$.

Lemma 6. *There exists* $\Delta \in \mathbb{K}[\varepsilon, \mathbf{X}]$ *such that:*

- *the inclusions* $\Delta \mathscr{L} \subset \langle F_1(\widetilde{\mathbf{Y}}, \widetilde{\mathbf{X}}), \ldots, F_n(\widetilde{\mathbf{Y}}, \widetilde{\mathbf{X}}) \rangle \subset \mathscr{L}$ *hold;*
- $\Delta(0, \mathbf{X})$ *is in* $\mathbb{Q}[\mathbf{Y}] \subset \mathbb{K}$ *and is non-zero.*

Proof. Let $f_1, \ldots, f_s \in \mathbb{Q}[\mathbf{Y}, \mathbf{X}]$ be generators of $\mathscr{I}$. By construction, all polynomials F_j, for $j = 1, \ldots, n$, can be expressed through equalities of the form

$$F_j = \sum_{i=1}^{s} h_{i,j} f_i,$$

for some $h_{i,j}$ in $\mathbb{Q}(\mathbf{Y})[\mathbf{X}]$. Clearing denominators, these equalities can be rewritten as

$$\gamma_j F_j = \sum_{i=1}^{s} H_{i,j} f_i,$$

for some coefficients $H_{i,j}$ in $\mathbb{Q}[\mathbf{Y}, \mathbf{X}]$ and γ_j in $\mathbb{Q}[\mathbf{Y}]$. Assumption 2 on $\mathscr{V}$ then implies that F_j itself belongs to the ideal $\mathscr{I}$; the rightmost inclusion of the first point follows, after applying the change of variable in (2).

Conversely, each polynomial f_i belongs to the ideal $\mathscr{I} \cdot \mathbb{Q}(\mathbf{Y})[\mathbf{X}]$, so that for $i = 1, \ldots, s$, there is an equality of the form

$$f_i = \sum_{j=1}^{n} a_{i,j} F_j,$$

for some $a_{i,j}$ in $\mathbb{Q}(\mathbf{Y})[\mathbf{X}]$. Clearing denominators, we can rewrite this equality as

$$\delta_i f_i = \sum_{j=1}^{n} A_{i,j} F_j,$$

for some $A_{i,j}$ in $\mathbb{Q}[\mathbf{Y}, \mathbf{X}]$ and δ_i non-zero in $\mathbb{Q}[\mathbf{Y}]$. Taking the least common multiple of all δ_i, we finally obtain expressions of the form

$$\delta f_i = \sum_{j=1}^{n} B_{i,j} F_j,$$

for some $B_{i,j}$ in $\mathbb{Q}[\mathbf{Y}, \mathbf{X}]$ and δ in $\mathbb{Q}[\mathbf{Y}]$. Define $\Delta = \delta(\widetilde{\mathbf{Y}}) \in \mathbb{K}[\varepsilon, \mathbf{X}]$, and note that $\Delta(0, \mathbf{X}) = \delta \in \mathbb{Q}[\mathbf{Y}]$. Then, we deduce the equalities

$$\Delta\, f_i(\widetilde{\mathbf{Y}}, \widetilde{\mathbf{X}}) = \sum_{j=1}^{n} B_{i,j}(\widetilde{\mathbf{Y}}, \widetilde{\mathbf{X}}) F_j(\widetilde{\mathbf{Y}}, \widetilde{\mathbf{X}}),$$

so that

$$\Delta\, f_i(\widetilde{\mathbf{Y}}, \widetilde{\mathbf{X}}) \in \langle F_1(\widetilde{\mathbf{Y}}, \widetilde{\mathbf{X}}), \ldots, F_n(\widetilde{\mathbf{Y}}, \widetilde{\mathbf{X}}) \rangle$$

for all i; this finishes the proof. ∎

We can then conclude the proof of Proposition 4.

- The extension of $\mathscr{L} \subset \mathbb{K}[\varepsilon, \mathbf{X}]$ in $\mathbb{K}(\varepsilon)[\mathbf{X}] = \mathbb{M}[\mathbf{X}]$ is the ideal $\langle F(\widetilde{\mathbf{Y}}, \widetilde{\mathbf{X}}) \mid F \in \mathscr{I} \rangle$ of $\mathbb{M}[\mathbf{X}]$; it is thus the ideal $\mathscr{J}^\star$ defined in the previous subsection. This ideal has dimension 0, so that $\mathscr{Z}$ satisfies $\mathbf{G_1}$.

- The fiber $\pi^{-1}(0) \cap \mathscr{Z}$ is obtained by adding $\varepsilon = 0$ to the defining equations of $\mathscr{Z}$; it is thus defined by the ideal $\mathscr{I} \cdot \mathbb{K}[\mathbf{X}]$. Since $\mathbb{K}$ is built by adjoining new transcendentals to $\mathbb{Q}(\mathbf{Y})$, and since $\mathscr{I} \cdot \mathbb{Q}(\mathbf{Y})[\mathbf{X}]$ has dimension 0, $\pi^{-1}(0) \cap \mathscr{Z}$ has dimension 0. Thus, $\mathscr{Z}$ satisfies $\mathbf{G_2}$.

- Lemmas 4 and 6 establish that $\mathscr{Z}$ satisfies $\mathbf{G_3}$.

5.3 Conclusion

We will now conclude the proof of Theorem 2. Let $\mathscr{C} \in \mathbb{Z}[\mathbf{U}^0, \dots, \mathbf{U}^m]$ be a Chow form of $\mathscr{V}$, and let $\mathscr{C}_\varepsilon \in \mathbb{Z}[\mathbf{Y}, \mathbf{U}, \mathbf{T}^1, \dots, \mathbf{T}^m, \varepsilon]$ be the polynomial obtained by performing the following substitution in $\mathscr{C}$:

$$\mathbf{U}_{(0)} \leftarrow \begin{bmatrix} U_0 \\ Y_1 \\ \vdots \\ Y_m \end{bmatrix}, \quad \mathbf{U}_{(\mathbf{Y})} \leftarrow \begin{bmatrix} 0 & \dots & 0 \\ -1 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & -1 \end{bmatrix}, \quad \mathbf{U}_{(\mathbf{X})} \leftarrow \begin{bmatrix} U_1 & \dots & U_n \\ \varepsilon T_1^1 & \dots & \varepsilon T_n^1 \\ \vdots & & \vdots \\ \varepsilon T_1^m & \dots & \varepsilon T_n^m \end{bmatrix}.$$

Then, by Proposition 3, seen in $\mathbb{M}[\mathbf{U}]$, $\mathscr{C}_\varepsilon$ is a Chow form of $\mathscr{W}^\star$ (and so, is non-zero). Besides, if d is the valuation of $\mathscr{C}_\varepsilon$ in ε, then $\mathscr{C}'_\varepsilon = \mathscr{C}_\varepsilon / \varepsilon^d$ is also a Chow form of $\mathscr{W}^\star$, since ε belongs to the base field $\mathbb{M}$.

Let now $\mathscr{C}_0 \in \mathbb{Z}[\mathbf{Y}, \mathbf{U}, \mathbf{T}^1, \dots, \mathbf{T}^m]$ be the coefficient of lowest degree in ε of $\mathscr{C}_\varepsilon$; it is thus obtained by letting $\varepsilon = 0$ in $\mathscr{C}'_\varepsilon$. Recall that the extension of $\mathscr{L}$ to $\mathbb{M}[\mathbf{X}]$ is the defining ideal $\mathscr{J}^\star$ of $\mathscr{W}^\star$. Besides, by Proposition 4, $\mathscr{Z} = Z(\mathscr{L})$ satisfies Assumptions $\mathbf{G_1}$, $\mathbf{G_2}$ and $\mathbf{G_3}$ of Proposition 1. We deduce from that proposition that any Chow form of the fiber $\pi^{-1}(0) \cap \mathscr{Z}$ divides $\mathscr{C}_0$ in $\mathbb{K}[\mathbf{U}]$.

As mentioned in the proof of Proposition 4, the fiber $\pi^{-1}(0) \cap \mathscr{Z}$ is defined by the extension of $\mathscr{I} \cdot \mathbb{Q}(\mathbf{Y})[\mathbf{X}]$ in $\mathbb{K}[\mathbf{X}]$. Let thus $\mathscr{C}^\star \in \mathbb{Q}(\mathbf{Y})[\mathbf{U}]$ be a Chow form of $\mathscr{I} \cdot \mathbb{Q}(\mathbf{Y})[\mathbf{X}]$. By the former remark, $\mathscr{C}^\star$ is a Chow form of $\mathscr{I} \cdot \mathbb{K}[\mathbf{X}]$, so it divides $\mathscr{C}_0$ in $\mathbb{K}[\mathbf{U}] = \mathbb{Q}(\mathbf{Y}, \mathbf{T}^1, \dots, \mathbf{T}^m)[\mathbf{U}]$. If we additionally impose that $\mathscr{C}^\star$ is a *primitive* Chow form, so that in particular it belongs to $\mathbb{Z}[\mathbf{Y}, \mathbf{U}]$, then one deduces that $\mathscr{C}^\star$ divides $\mathscr{C}_0$ in $\mathbb{Z}[\mathbf{Y}, \mathbf{T}^1, \dots, \mathbf{T}^m, \mathbf{U}]$. This finishes the proof, up to formally replacing the indeterminates $\mathbf{T}^i$ by the indeterminates $\mathbf{U}^i$ appearing in the statement of Theorem 2.

6 Predicting a denominator

We continue with the notation of the previous section, and study the polynomials $(N_1, \dots, N_n)$ and $(T_1, \dots, T_n)$ of $\mathbb{Q}(\mathbf{Y})[\mathbf{X}]$, that were defined in the introduction. We reuse some notation from the introduction, such as the degree $d_{\mathscr{V}}$ and the height $h_{\mathscr{V}}$ of $\mathscr{V}$, and the degrees $(d_1, \ldots, d_n)$ of the polynomials $(T_1, \ldots, T_n)$. The notation of Section 3 is in use as well. We will use the constant

$$\mathsf{G}_n \quad = \quad 1 + 2\sum\nolimits_{i \le n-1}(d_i - 1)$$

Because $d_1 \cdots d_n \le d_{\mathscr{V}}$, one easily deduces the upper bound $\mathsf{G}_n \le 2d_{\mathscr{V}}$.

A first goal in this section is to predict suitable "common denominators" for the polynomials $(N_1, \ldots, N_n)$. We also wish to do the same for the polynomials $(T_1, \ldots, T_n)$, but this is not as straightforward; for this reason, we are going to introduce a slightly modified version of $(T_1, \ldots, T_n)$, which will be more handy. For $i = 1, \ldots, n$, let us define the iterated resultant

$$e_i = \mathrm{res}(\cdots \mathrm{res}(\frac{\partial T_i}{\partial X_i}, T_i, X_i), \cdots, T_1, X_1) \in \mathbb{Q}(\mathbf{Y}),$$

so that for instance e_1 is the discriminant of T_1. We define the polynomials $\widetilde{T}_1, \ldots, \widetilde{T}_n$ by $\widetilde{T}_\ell = e_1 \cdots e_{\ell-1} T_\ell$ for $\ell \le n$. As it turns, these polynomials are easier to handle than the polynomials T_ℓ, and the bit-length information we wish to obtain for T_ℓ can easily be recovered from $\widetilde{T}_\ell$.

The Chow forms of $\mathscr{V}^\star$ are polynomials in $\mathbb{Q}(\mathbf{Y})[\mathbf{U}]$, where $\mathbf{U} = U_0, \ldots, U_n$ are new indeterminates. We will especially be interested in a *primitive* Chow form of $\mathscr{V}^\star$; recall that it is unique, up to sign. Informally, the denominator we seek will be the leading coefficient of one of these primitive Chow forms. Formally, choosing one the two possible signs, we let $\mathscr{C}^\star \in \mathbb{Z}[\mathbf{Y}, \mathbf{U}]$ be a primitive Chow form of $\mathscr{V}^\star$ and we let $a_n \in \mathbb{Z}[\mathbf{Y}]$ be the coefficient of $U_0^{d_n}$ in $\mathscr{C}^\star$.

Proposition 5. *The following holds:*

- $a_n \neq 0$;
- $\ell_{v_\infty}(a_n) \le h_{\mathscr{V}} + 5(m+1)d_{\mathscr{V}} \log(m+n+2)$;
- $\deg(a_n) \le d_{\mathscr{V}}$;
- $a_n N_n$ *is in* $\mathbb{Z}[\mathbf{Y}, \mathbf{X}]$, *with* $\deg(a_n N_n, \mathbf{Y}) \le d_{\mathscr{V}}$;
- $a_n^{\mathsf{G}_n} \widetilde{T}_n$ *is in* $\mathbb{Z}[\mathbf{Y}, \mathbf{X}]$, *with* $\deg(a_n^{\mathsf{G}_n} \widetilde{T}_n, \mathbf{Y}) \le \mathsf{G}_n d_{\mathscr{V}}$.

The first point is obvious: since $\mathscr{V}^\star$ has dimension 0, Equation (1) shows that the coefficient of $U_0^{d_n}$ in $\mathscr{C}^\star$ is non-zero. Then, Subsection 6.1 will prove the degree and height estimates for a_n; Subsection 6.2 will prove the last assertions by means of valuation estimates.

Finally, remark that in Proposition 5, we deal only with N_n and $\widetilde{T}_n$. However, this result implies analogue results for all N_ℓ and $\widetilde{T}_\ell$, by replacing $\mathscr{V}$ by $\mathscr{V}_\ell$ and $\mathscr{V}^\star$ by $\mathscr{V}_\ell^\star$.

6.1 Degree and height bounds for the primitive Chow form

To prove the second and third points of Proposition 5, we actually prove a similar estimate for the whole primitive Chow form $\mathscr{C}^\star$ of $\mathscr{V}^\star$.

Proposition 6. *The primitive Chow form* $\mathscr{C}^\star$ *of* $\mathscr{V}^\star$ *satisfies* $\deg(\mathscr{C}^\star, \mathbf{Y}) \leq d_{\mathscr{V}}$ *and* $\ell_{v_\infty}(\mathscr{C}^\star) \leq h_{\mathscr{V}} + 5(m+1)d_{\mathscr{V}} \log(m+n+2)$.

First, we recall from (Schost, 2003b, Lemma 3) that a primitive Chow form of $\mathscr{V}^\star$ has degree in $\mathbf{Y}$ at most $d_{\mathscr{V}}$: this handles the claimed degree bound. To deal with the height aspect, we need a Chow form of the positive-dimensional algebraic set $\mathscr{V}$ with good height properties.

Lemma 7. *The algebraic set* $\mathscr{V}$ *admits a Chow form* $\mathscr{C}$ *in* $\mathbb{Z}[\mathbf{U}^0, \ldots, \mathbf{U}^m]$ *with* $\ell_{v_\infty}(\mathscr{C}) \leq h_{\mathscr{V}} + (m+1)d_{\mathscr{V}} \log(m+n+2)$.

Proof. Let $\mathscr{C} \in \mathbb{Z}[\mathbf{U}^0, \ldots, \mathbf{U}^m]$ be a Chow form of $\mathscr{V}$ with integer coefficients and content 1. Let $\mathsf{M}_{\mathbb{Q}} = (\{v_p,\, p \in \mathcal{P}\},\ \{v_\infty\})$ be the set of absolute values over $\mathbb{Q}$ introduced in Subsection 3.1. Then, for every non-Archimedean valuation v_p in $\mathsf{M}_{\mathbb{Q}}$, $\ell_{v_p}(\mathscr{C}) = 0$. The definition of the height of $\mathscr{V}$ implies that we have

$$h_{\mathscr{V}} = \mathsf{m}(\mathscr{C}, m+1, m+n+1) + (m+1)d_{\mathscr{V}} \sum_{i=1}^{m+n} \frac{1}{2i}.$$

Using Inequalities $\mathbf{A_1}$ and $\mathbf{A_2}$ of Subsection 3.2, we conclude that $\ell_{v_\infty}(\mathscr{C}) \leq h_{\mathscr{V}} + (m+1)d_{\mathscr{V}} \log(m+n+2)$. □

We can now conclude the proof of Proposition 6, using the specialization property seen in the previous section. Let $\mathscr{C} \in \mathbb{Z}[\mathbf{U}^0, \ldots, \mathbf{U}^m]$ be a Chow form of $\mathscr{V}$ as in the previous lemma. Following Theorem 2, we rewrite the indeterminates $\mathbf{U}^0, \ldots, \mathbf{U}^m$ of $\mathscr{C}$ as

$$\mathbf{U}_{(0)} = \begin{bmatrix} U_0^0 \\ \vdots \\ U_0^m \end{bmatrix}, \mathbf{U}_{(\mathbf{Y})} = \begin{bmatrix} U_1^0 & \ldots & U_m^0 \\ \vdots & & \vdots \\ U_1^m & \ldots & U_m^m \end{bmatrix},\ \mathbf{U}_{(\mathbf{X})} = \begin{bmatrix} U_{m+1}^0 & \cdots & U_{m+n}^0 \\ \vdots & & \vdots \\ U_{m+1}^m & \cdots & U_{m+n}^m \end{bmatrix};$$

then, we let $\mathscr{C}_\varepsilon \in \mathbb{Z}[\mathbf{Y}, \mathbf{U}, \mathbf{U}^1, \ldots, \mathbf{U}^m, \varepsilon]$ be the polynomial obtained by performing the following substitution in $\mathscr{C}$:

$$\mathbf{U}_{(0)} \leftarrow \begin{bmatrix} U_0 \\ Y_1 \\ \vdots \\ Y_m \end{bmatrix},\quad \mathbf{U}_{(\mathbf{Y})} \leftarrow \begin{bmatrix} 0 & \ldots & 0 \\ -1 & \ldots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \ldots & -1 \end{bmatrix},\quad \mathbf{U}_{(\mathbf{X})} \leftarrow \begin{bmatrix} U_1 & \ldots & U_n \\ \varepsilon U_{m+1}^1 & \cdots & \varepsilon U_{m+n}^1 \\ \vdots & & \vdots \\ \varepsilon U_{m+1}^m & \ldots & \varepsilon U_{m+n}^m \end{bmatrix};$$

Theorem 2 shows that this polynomial is non-zero. Let finally $\mathscr{C}_0 \in \mathbb{Z}[\mathbf{Y}, \mathbf{U}, \mathbf{U}^1 \ldots, \mathbf{U}^m]$ be the coefficient of lowest degree in ε of $\mathscr{C}_\varepsilon$. Then, Theorem 2 shows that $\mathscr{C}^\star$ divides $\mathscr{C}_0$ in $\mathbb{Z}[\mathbf{Y}, \mathbf{U}, \mathbf{U}^1, \ldots, \mathbf{U}^m]$.

If we rewrite $\mathscr{C}_0$ as a polynomial in variables $\mathbf{U}^1 \dots, \mathbf{U}^m$ with coefficients in $\mathbb{Z}[\mathbf{Y}, \mathbf{U}]$, this implies that $\mathscr{C}^\star$ divides one of these coefficients, say $\mathscr{C}_{0,0}$, in $\mathbb{Z}[\mathbf{Y}, \mathbf{U}]$, with $\mathscr{C}_{0,0} \neq 0$.

The polynomial $\mathscr{C}_{0,0}$ is in $\mathbb{Z}[\mathbf{Y}, \mathbf{U}]$ and satisfies $\ell_{v_\infty}(\mathscr{C}_{0,0}) \leq h_{\mathscr{V}} + (m+1)d_{\mathscr{V}} \log(m+n+2)$, since all its coefficients are coefficients of $\mathscr{C}$. Besides, it has total degree at most $(m+1)d_{\mathscr{V}}$. Since $\mathscr{C}_{0,0}/\mathscr{C}^\star$ has integer coefficients, we deduce that $\ell_{v_\infty}(\mathscr{C}_{0,0}/\mathscr{C}^\star) \geq 0$; then, $\mathbf{A_3}$ implies that $\ell_{v_\infty}(\mathscr{C}^\star) \leq \ell_{v_\infty}(\mathscr{C}_{0,0}) + 4(m+1)d_{\mathscr{V}} \log(m+n+2)$, which yields

$$\ell_{v_\infty}(\mathscr{C}^\star) \leq h_{\mathscr{V}} + 5(m+1)d_{\mathscr{V}} \log(m+n+2).$$

6.2 Valuation estimates

We prove the missing statements of Proposition 5. The conclusion of the proof uses valuation estimates; the key lemma is the following.

Lemma 8. *For any non-Archimedean absolute value v on $\mathbb{Q}(\mathbf{Y})$, the inequalities*

$$\ell_v(a_n N_n) \leq \ell_v(\mathscr{C}^\star) \quad \textit{and} \quad \ell_v(a_n^{\mathsf{G}_n} \widetilde{T}_n) \leq \mathsf{G}_n \ell_v(\mathscr{C}^\star)$$

hold.

Proof. We let here $\widetilde{\mathscr{C}^\star} \in \mathbb{Q}(\mathbf{Y})[\mathbf{U}]$ be the *monic* Chow form of $\mathscr{V}^\star$, so that the primitive Chow form $\mathscr{C}^\star$ and its leading term a_n satisfy $\mathscr{C}^\star = a_n \widetilde{\mathscr{C}^\star}$. Lemma 5 in (Dahan and Schost, 2004) establishes the inequalities

$$h_v(N_n) \leq h_v(\widetilde{\mathscr{C}^\star}) \quad \text{and} \quad h_v(\widetilde{T}_n) \leq \mathsf{G}_n h_v(\widetilde{\mathscr{C}^\star}),$$

with $h_v(f) = \max(\ell_v(f), 0)$ for any polynomial f. Since on one hand ℓ_v is always bounded from above by h_v, and since on the other hand $h_v(\widetilde{\mathscr{C}^\star}) = \ell_v(\widetilde{\mathscr{C}^\star})$ (because this polynomial has a coefficient equal to 1), we deduce the alternative form

$$\ell_v(N_n) \leq \ell_v(\widetilde{\mathscr{C}^\star}) \quad \text{and} \quad \ell_v(\widetilde{T}_n) \leq \mathsf{G}_n \ell_v(\widetilde{\mathscr{C}^\star}).$$

Since $a_n \widetilde{\mathscr{C}^\star} = \mathscr{C}^\star$, using $\mathbf{N_1}$, we deduce

$$\ell_v(a_n N_n) = \ell_v(a_n) + \ell_v(N_n) \leq \ell_v(a_n) + \ell_v(\widetilde{\mathscr{C}^\star}) = \ell_v(\mathscr{C}^\star)$$

and

$$\ell_v(a_n^{\mathsf{G}_n} \widetilde{T}_n) = \ell_v(a_n^{\mathsf{G}_n}) + \ell_v(\widetilde{T}_n) = \mathsf{G}_n \ell_v(a_n) + \ell_v(\widetilde{T}_n) \leq \mathsf{G}_n \ell_v(a_n) + \mathsf{G}_n \ell_v(\widetilde{\mathscr{C}^\star}) = \mathsf{G}_n \ell_v(\mathscr{C}^\star).$$

Thus, all inequalities are proved. □

Let V be the set of all absolute values on $\mathbb{Q}(\mathbf{Y})$ either of the form v_S for S irreducible in $\mathbb{Q}[\mathbf{Y}]$, or of the form v_p, for p a prime. By the discussion in Subsection 3.2, for f in $\mathbb{Q}(\mathbf{Y})[\mathbf{X}]$, $v(f) \leq 0$ holds for all v in V if and only if f is in $\mathbb{Z}[\mathbf{Y}][\mathbf{X}] = \mathbb{Z}[\mathbf{Y}, \mathbf{X}]$.

Since $\mathscr{C}^\star$ is in $\mathbb{Z}[\mathbf{Y},\mathbf{X}]$, we have that $\ell_v(\mathscr{C}^\star) \le 0$ for all v in V. By the previous lemma, we obtain

$$\ell_v(a_n N_n) \le 0 \quad \text{and} \quad \ell_v(a_n^{\mathsf{G}_n} \widetilde{T}_n) \le 0,$$

so that $a_n N_n$ and $a_n^{\mathsf{G}_n} \widetilde{T}_n$ are in $\mathbb{Z}[\mathbf{X},\mathbf{Y}]$. To conclude the proof of Proposition 5, recall from Proposition 6 that $\deg(\mathscr{C}^\star, \mathbf{Y}) \le d_{\mathscr{V}}$, which can be restated as $\ell_{v_{\deg}}(\mathscr{C}^\star) \le d_{\mathscr{V}}$, where $v_{\deg}$ is the non-Archimedean absolute value introduced in Subsection 3.1; this implies $\mathsf{G}_n \ell_{v_{\deg}}(\mathscr{C}^\star) \le \mathsf{G}_n d_{\mathscr{V}}$.

Applying the former lemma to the absolute value $v_{\deg}$, we thus prove the last two assertions of Proposition 5, finishing its proof.

7 Proof of the main theorem

We finally prove Theorem 1 using interpolation techniques. The results of (Dahan and Schost, 2004) enable us to give height bounds for specializations of $(N_1, \dots, N_n)$ and $(\widetilde{T}_1, \dots, \widetilde{T}_n)$. The results of the previous section then make it possible to predict a denominator for the coefficients of $(N_1, \dots, N_n)$ and $(\widetilde{T}_1, \dots, \widetilde{T}_n)$, so that polynomial interpolation of the numerators is sufficient.

We focus only on N_n and $\widetilde{T}_n$, since extending the results to all $(N_1, \dots, N_n)$ and $(\widetilde{T}_1, \dots, \widetilde{T}_n)$ is straightforward. All the notation introduced in the previous section is still in use in this section.

7.1 Norm estimates for interpolation

First, we give norm estimates for interpolation at integer points. For any integer $M > 0$, we denote by Γ_M the set of integers

$$\Gamma_M = \{1, \dots, M\}.$$

Let us fix M and another integer $L \le M$. We will use subsets of Γ_M^m of cardinality L^m to perform evaluation and interpolation. To control the norm growth through interpolation at these subsets in the multivariate case, the following "univariate" lemma will be useful.

Lemma 9. *Let Λ be a subset of Γ_M of cardinality L and let $\mathbf{V}$ be the $L \times L$ Vandermonde matrix built on Λ. Let $\mathbf{a} = (a_1, \dots, a_L)$ be in $\mathbb{Q}^L$, with $\ell_{v_\infty}(a_i) \le A$ for all i, and let $(b_1, \dots, b_L) = \mathbf{V}^{-1}\mathbf{a}$. Then the inequality $\ell_{v_\infty}(b_i) \le A + L\log(M+1) + \log(L)$ holds for all i.*

Proof. Let $\mathbf{W}$ be the inverse of $\mathbf{V}$. The upper bound given in (Higham, 2002, Eq. (22.3)) shows that all entries $w_{i,j}$ of $\mathbf{W}$ satisfy $|w_{i,j}| = v_\infty(w_{i,j}) \le (M+1)^L$. Since all entries of $\mathbf{a}$ satisfy $v_\infty(a_i) \le e^A$, we deduce that all b_i satisfy $v_\infty(b_i) \le L(M+1)^L e^A$. Taking logarithms finishes the proof. □

In the multivariate case, we rely on the notion of *equiprojectable* set (Aubry and Valibouze, 2000), which we recall here, adding a few extra constraints to facilitate norm estimates later on. Let us define a sequence $\Lambda_1, \Lambda_2, \ldots$ of subsets of $\Gamma_M, \Gamma_M^2, \ldots$ through the following process:

- Λ_1 is a subset of Γ_M of cardinality L;
- for $i \geq 1$, assuming that Λ_i has been defined, we take Λ_{i+1} of the form

$$\Lambda_{i+1} = \cup_{\mathbf{y} \in \Lambda_i} \ \big(\mathbf{y} \times \Lambda_{i,\mathbf{y}}\big),$$

  where each $\Lambda_{i,\mathbf{y}}$ is a subset of Γ_M of cardinality L.

Then, we say that $\Lambda \subset \Gamma_M^m$ is an (M, L)-*equiprojectable set* if it arises as the mth element Λ_m of a sequence $\Lambda_1, \ldots, \Lambda_m$ constructed as above. Observe that such a set has cardinality L^m.

Let $\mathbb{Q}[\mathbf{Y}]_L$ be the subspace of $\mathbb{Q}[\mathbf{Y}]$ consisting of all polynomials of degree less than L in each variable $Y_1, \ldots, Y_m$; thus, $\mathbb{Q}[\mathbf{Y}]_L$ has dimension L^m. Associated to an (M, L)-equiprojectable set $\Lambda \subset \Gamma_M^m$, we set up the evaluation operator

$$\begin{array}{rccc} ev_\Lambda : & \mathbb{Q}[\mathbf{Y}]_L & \mapsto & \mathbb{Q}^{L^m} \\ & f & \mapsto & [f(\mathbf{y})]_{\mathbf{y} \in \Lambda}. \end{array}$$

We let $\mathbf{M}_\Lambda$ be the matrix of this map, where we use the canonical monomial basis for $\mathbb{Q}[\mathbf{Y}]_L$.

Proposition 7. *The following holds:*

- *The map ev_Λ is invertible.*
- *Let $\mathbf{a}$ be in $\mathbb{Q}^{L^m}$, with $\ell_{v_\infty}(a_i) \leq A$ for each entry a_i of $\mathbf{a}$, and let $\mathbf{b} = \mathbf{M}_\Lambda^{-1}\mathbf{a}$. Then the inequality $\ell_{v_\infty}(b_i) \leq A + mL\log(M+1) + m\log(L)$ holds for each entry b_i of $\mathbf{b}$.*

Proof. To evaluate a polynomial $f \in \mathbb{Q}[\mathbf{Y}]$ at Λ, we first see it as a polynomial in $\mathbb{Q}[Y_1][Y_2, \ldots, Y_m]$ and evaluate all its coefficients at Λ_1. We obtain L polynomials $\{f_\mathbf{y},\ \mathbf{y} \in \Lambda_1\}$ in $\mathbb{Q}[Y_2, \ldots, Y_m]$, and we proceed recursively to evaluate each $f_\mathbf{y}$. This implies that the matrix $\mathbf{M}_\Lambda$ factors as $\mathbf{M}_\Lambda = \mathbf{M}_m \cdots \mathbf{M}_1$, where, up to permutation of the rows and columns, $\mathbf{M}_i$ is a block diagonal matrix, whose blocks are Vandermonde matrices of size L built on the sets $\Lambda_{i,\mathbf{y}}$ (each of them being repeated L^{m-i} times).

Thus, $\mathbf{M}$ is invertible, of inverse $\mathbf{M}$ given by $\mathbf{M}_1^{-1} \cdots \mathbf{M}_m^{-1}$. The second point is now a direct consequence of Lemma 9. □

7.2 Good specializations

We return to the study of an algebraic set $\mathscr{V} \subset \mathbb{C}^{m+n}$ satisfying Assumption 2; we discuss here the "good" and "bad" specialization values for the polynomials $(T_1, \ldots, T_n)$ and $(N_1, \ldots, N_n)$.

For $\mathbf{y} = (y_1, \ldots, y_m)$ in $\mathbb{C}^m$ and F in $\mathbb{Q}(\mathbf{Y})[\mathbf{X}]$, we denote by $F_\mathbf{y}$ the specialized polynomial $F(\mathbf{y}, \mathbf{X})$, assuming that the denominator of no coefficient of F vanishes at $\mathbf{y}$. We denote by $\mathscr{V}_\mathbf{y}$ the fiber of the projection $\Pi_0 : \mathbb{C}^{m+n} \to \mathbb{C}^m$ restricted to $\mathscr{V}$, that is, the algebraic set

$$\mathscr{V}_\mathbf{y} = \mathscr{V} \cap Z(Y_1 - y_1, \ldots, Y_m - y_m) \ \subset \ \mathbb{C}^{m+n}.$$

Finally, we say that $\mathbf{y}$ is a *good specialization* if the following holds:

- the denominator of no coefficient in $(T_1, \dots, T_n)$ vanishes at $\mathbf{y}$, so that all polynomials $T_{i,\mathbf{y}} = T_i(\mathbf{y}, \mathbf{X})$ are well-defined;
- the monic triangular set $(Y_1 - y_1, \dots, Y_m - y_m, T_{1,\mathbf{y}}, \dots, T_{n,\mathbf{y}})$ is the Gröbner basis of the defining ideal of $\mathscr{V}_{\mathbf{y}}$, for the lexicographic order $Y_1 < \cdots < Y_m < X_1 < \cdots < X_n$.

The following proposition shows that for any L, there exist (M, L)-equiprojectable sets where all points are good specializations, if we choose M large enough.

Proposition 8. *For any positive integer L, there exists an (M, L)-equiprojectable set Λ such that all points in Λ are good specializations, with $M = (3nd_{\mathscr{V}} + n^2)d_{\mathscr{V}} + L$.*

Proof. Theorem 2 in (Schost, 2003a) shows that there exists a non-zero polynomial $\Delta \in \mathbb{Z}[\mathbf{Y}]$ of degree at most $M_0 = (3nd_{\mathscr{V}} + n^2)d_{\mathscr{V}}$ such that any $\mathbf{y} \in \mathbb{C}^m$ with $\Delta(\mathbf{y}) \neq 0$ is a good specialization; in what follows, we take $M = M_0 + L$.

We are going to use this to construct a sequence $\Lambda_1, \Lambda_2, \dots, \Lambda_m$ of (M, L)-equiprojectable sets in $\Gamma_M, \Gamma_M^2, \dots, \Gamma_M^m$, and we will take $\Lambda = \Lambda_m$. We will impose the following property for $i \leq m$:

($\mathbf{P}_i$) for all $\mathbf{y} = (y_1, \dots, y_i)$ in Λ_i, the polynomial $\Delta(y_1, \dots, y_i, Y_{i+1}, \dots, Y_m)$ is not identically zero.

The proof is by induction.

- For $i = 1$, remark that there exist at most M_0 values y_1 such that $\Delta(y_1, Y_2, \dots, Y_m)$ vanishes identically, so that there exists a subset Λ_1 of Γ_M of cardinality L that satisfies $\mathbf{P}_1$.
- For $1 \leq i < m$, assume that a subset Λ_i satisfying $\mathbf{P}_i$ has been defined. Thus, for $\mathbf{y} = (y_1, \dots, y_i)$ in Λ_i, the polynomial $\Delta(y_1, \dots, y_i, Y_{i+1}, \dots, Y_m)$ is not identically zero. Consequently, there exist at most M_0 values y_{i+1} such that $\Delta(y_1, \dots, y_i, y_{i+1}, Y_{i+2}, \dots, Y_m)$ vanishes identically. Thus, there exists a subset $\Lambda_{i,\mathbf{y}}$ of Γ_M of cardinality L such that $\Delta(y_1, \dots, y_i, y_{i+1}, Y_{i+2}, \dots, Y_m)$ vanishes identically for no element y_{i+1} in $\Lambda_{i,\mathbf{y}}$. Defining $\Lambda_{i+1} = \cup_{\mathbf{y} \in \Lambda_i} (\mathbf{y} \times \Lambda_{i,\mathbf{y}})$, we see that this set satisfies $\mathbf{P}_{i+1}$.

Taking $i = m$ shows that $\Lambda = \Lambda_m$ satisfies our requests. □

7.3 Norm estimates at good specializations

We continue with estimates for good specializations of the polynomials $a_n N_n$ and $a_n^{\mathsf{G}_n} \widetilde{T}_n$. In addition to the constant $\mathsf{G}_n = 1 + 2\sum_{i \leq n-1}(d_i - 1)$ defined in the previous section, we will also use the following quantities:

$$\begin{aligned} \mathsf{H}_n &= 5\log(n+3)\sum_{i \leq n} d_i \\ \mathsf{I}_n &= \mathsf{H}_n + 3\log(2)\sum_{i \leq n-1} d_i(d_i - 1). \end{aligned}$$

One verifies that these constants satisfy the following upper bounds:

$$\begin{aligned} \mathsf{H}_n &\leq 5\log(n+3)(d_{\mathscr{V}}+n) \\ \mathsf{I}_n &\leq 3d_{\mathscr{V}}^2 + 5\log(n+3)(d_{\mathscr{V}}+n). \end{aligned}$$

Considering only the dependency in $(d_{\mathscr{V}}, h_{\mathscr{V}})$, the following proposition gives a bound linear in $(d_{\mathscr{V}} + h_{\mathscr{V}})$ for the specialization of $a_n N_n$; the bound for $a_n^{\mathsf{G}_n}\widetilde{T}_n$ is quadratic.

Proposition 9. *Let $\mathbf{y} = (y_1, \ldots, y_m) \in \mathbb{Z}^m$ be a good specialization, such that all entries y_i satisfies $\ell_{v_\infty}(y_i) \leq M$. Then, the polynomials $a_{n,\mathbf{y}}N_{n,\mathbf{y}}$ and $a_{n,\mathbf{y}}^{\mathsf{G}_n}\widetilde{T}_{n,\mathbf{y}}$ are well-defined, and they satisfy*

$$\begin{aligned} \ell_{v_\infty}(a_{n,\mathbf{y}}N_{n,\mathbf{y}}) &\leq 2h_{\mathscr{V}} + (6m+5)d_{\mathscr{V}}\log(m+n+2) + (m+1)d_{\mathscr{V}}\log(M) + m\log(d_{\mathscr{V}}+1) \\ &\quad +\mathsf{H}_n, \\ \ell_{v_\infty}(a_{n,\mathbf{y}}^{\mathsf{G}_n}\widetilde{T}_{n,\mathbf{y}}) &\leq \mathsf{G}_n\big[2h_{\mathscr{V}} + (6m+5)d_{\mathscr{V}}\log(m+n+2) + (m+1)d_{\mathscr{V}}\log(M) \\ &\quad +m\log(d_{\mathscr{V}}+1)\big] + \mathsf{I}_n. \end{aligned}$$

Proof. If $\mathbf{y}$ is a good specialization, then the monic triangular set $(T_{1,\mathbf{y}}, \ldots, T_{n,\mathbf{y}})$ is well-defined and generates a radical ideal. As a consequence,

$$\begin{aligned} D_n &= \prod_{1\leq i\leq n-1} \frac{\partial T_i}{\partial X_i} \mod \langle T_1, \ldots, T_{n-1}\rangle \\ \text{and}\quad e_n &= \prod_{1\leq i\leq n-1} \mathrm{res}(\cdots \mathrm{res}(\frac{\partial T_i}{\partial X_i}, T_i, X_i), \cdots, T_1, X_1) \end{aligned}$$

can be specialized at $\mathbf{y}$. Since $N_n = D_n T_n \mod \langle T_1, \ldots, T_{n-1}\rangle$ and $\widetilde{T}_n = e_n T_n$, this establishes our first claim.

Let next $\widetilde{\mathscr{C}}_{\mathbf{y}}$ be the monic Chow form of $\mathscr{V}_{\mathbf{y}}$ (this is a polynomial in $m+n+1$ variables) and let $d_{\mathscr{V}_{\mathbf{y}}}$ be its degree. The height $h_{\mathscr{V}_{\mathbf{y}}}$ of $\mathscr{V}_{\mathbf{y}}$ is

$$h_{\mathscr{V}_{\mathbf{y}}} = \sum_{p\in\mathcal{P}} \ell_{v_p}(\widetilde{\mathscr{C}}_{\mathbf{y}}) + \mathsf{m}(\widetilde{\mathscr{C}}_{\mathbf{y}}, 1, m+n+1) + d_{\mathscr{V}_{\mathbf{y}}} \sum_{i=1}^{m+n} \frac{1}{2i}.$$

Since $\widetilde{\mathscr{C}}_{\mathbf{y}}$ has a coefficient equal to 1, for every non-Archimedean absolute value v_p we have $\ell_{v_p}(\widetilde{\mathscr{C}}_{\mathbf{y}}) \geq 0$. Thus, we get the inequality

$$\mathsf{m}(\widetilde{\mathscr{C}}_{\mathbf{y}}, 1, m+n+1) + d_{\mathscr{V}_{\mathbf{y}}} \sum_{i=1}^{m+n} \frac{1}{2i} \leq h_{\mathscr{V}_{\mathbf{y}}}.$$

Let further $v_{\mathbf{y}} \subset \mathbb{C}^n$ be the 0-dimensional algebraic set obtained by projecting $\mathscr{V}_{\mathbf{y}}$ on the $\mathbf{X}$-space, and let $\widetilde{c}_{\mathbf{y}}$ be its monic Chow form. Thus, $\widetilde{c}_{\mathbf{y}}$ is obtained by setting all variables corresponding to $Y_1, \ldots, Y_m$ to 0 in $\widetilde{\mathscr{C}}_{\mathbf{y}}$.

Because $\mathbf{y}$ is a good specialization, applying Lemma 5 in (Dahan and Schost, 2004) to $v_{\mathbf{y}}$ and $\widetilde{c}_{\mathbf{y}}$ gives the following upper bounds:

$$\begin{aligned} \ell_{v_\infty}(N_{n,\mathbf{y}}) &\leq \mathsf{m}(\widetilde{c}_{\mathbf{y}}, n+1, 1) + \mathsf{H}_n \\ \ell_{v_\infty}(\widetilde{T}_{n,\mathbf{y}}) &\leq \mathsf{G}_n \mathsf{m}(\widetilde{c}_{\mathbf{y}}, n+1, 1) + \mathsf{I}_n, \end{aligned}$$

which imply, since $a_{n,\mathbf{y}}$ is actually in $\mathbb{Z}$,

$$\begin{aligned} \ell_{v_\infty}(a_{n,\mathbf{y}} N_{n,\mathbf{y}}) &\leq \ell_{v_\infty}(a_{n,\mathbf{y}}) + \mathsf{m}(\widetilde{c}_{\mathbf{y}}, n+1, 1) + \mathsf{H}_n \\ \text{and} \quad \ell_{v_\infty}(a_{n,\mathbf{y}}^{\mathsf{G}_n} \widetilde{T}_{n,\mathbf{y}}) &\leq \mathsf{G}_n \ell_{v_\infty}(a_{n,\mathbf{y}}) + \mathsf{G}_n \mathsf{m}(\widetilde{c}_{\mathbf{y}}, n+1, 1) + \mathsf{I}_n. \end{aligned}$$

Because $\widetilde{c}_{\mathbf{y}}$ is obtained by specializing indeterminates at 0 in $\widetilde{\mathscr{C}}_{\mathbf{y}}$, we deduce as in (Krick et al., 2001) that $\mathsf{m}(\widetilde{c}_{\mathbf{y}}, n+1, 1) \leq \mathsf{m}(\widetilde{\mathscr{C}}_{\mathbf{y}}, m+n+1, 1)$. Using inequality $\mathbf{A}_2$, we deduce further

$$\begin{aligned} \ell_{v_\infty}(a_{n,\mathbf{y}} N_{n,\mathbf{y}}) &\leq \ell_{v_\infty}(a_{n,\mathbf{y}}) + \mathsf{m}(\widetilde{\mathscr{C}}_{\mathbf{y}}, 1, m+n+1) + d_{\mathscr{V}_{\mathbf{y}}} \sum_{i=1}^{m+n} \frac{1}{2i} + \mathsf{H}_n \\ &\leq \ell_{v_\infty}(a_{n,\mathbf{y}}) + h_{\mathscr{V}_{\mathbf{y}}} + \mathsf{H}_n \end{aligned} \tag{5}$$

and similarly

$$\ell_{v_\infty}(a_{n,\mathbf{y}}^{\mathsf{G}_n} \widetilde{T}_{n,\mathbf{y}}) \leq \mathsf{G}_n \ell_{v_\infty}(a_{n,\mathbf{y}}) + \mathsf{G}_n h_{\mathscr{V}_{\mathbf{y}}} + \mathsf{I}_n. \tag{6}$$

Next, we give upper bounds on $\ell_{v_\infty}(a_{n,\mathbf{y}})$ and on $h_{\mathscr{V}_{\mathbf{y}}}$. We start with $\ell_{v_\infty}(a_{n,\mathbf{y}}) = \ell_{v_\infty}(a_n(\mathbf{y}))$. Recall from Proposition 5 that a_n is a polynomial with integer coefficients, of total degree bounded by $d_{\mathscr{V}}$ and with

$$\ell_{v_\infty}(a_n) \leq h_{\mathscr{V}} + 5(m+1) d_{\mathscr{V}} \log(m+n+2).$$

Since all y_i are integers of absolute value bounded by M, we deduce that

$$\ell_{v_\infty}(a_{n,\mathbf{y}}) \leq \ell_{v_\infty}(a_n) + d_{\mathscr{V}} \log(M) + m \log(1 + d_{\mathscr{V}}).$$

The previous bound on $\ell_{v_\infty}(a_n)$ gives

$$\ell_{v_\infty}(a_{n,\mathbf{y}}) \leq h_{\mathscr{V}} + 5(m+1) d_{\mathscr{V}} \log(m+n+2) + d_{\mathscr{V}} \log(M) + m \log(1 + d_{\mathscr{V}}).$$

Next, we need to control $h_{\mathscr{V}_{\mathbf{y}}}$, with

$$\mathscr{V}_{\mathbf{y}} = \mathscr{V} \cap Z(Y_1 - y_1, \dots, Y_m - y_m).$$

All polynomials $Y_i - y_i$ have degree 1 and satisfy $\ell_{v_\infty}(Y_i - y_i) \leq \log(M)$. Using the arithmetic Bézout inequality given in Corollary 2.11 of Krick et al. (2001), we obtain the upper bound

$$h_{\mathscr{V}_{\mathbf{y}}} \leq h_{\mathscr{V}} + m d_{\mathscr{V}} \log(M) + m d_{\mathscr{V}} \log(m+n+1).$$

Using the bounds on $\ell_{v_\infty}(a_{n,\mathbf{y}})$ and $h_{\mathscr{V}_{\mathbf{y}}}$, Equations (5) and (6) give our result after a quick simplification. □

7.4 Conclusion by interpolation

Finally, we obtain the requested bounds on N_n and T_n using interpolation at suitable equiprojectable sets.

The degree bounds are already in (Dahan and Schost, 2004), and also follow from Proposition 5. They state that, if we see $a_n N_n$ in $\mathbb{Z}[\mathbf{Y}][\mathbf{X}]$, each coefficient of this polynomial is in $\mathbb{Z}[\mathbf{Y}]_{L_1}$, with $L_1 = d_{\mathscr{V}} + 1$. Similarly, each coefficient of $a_n^{\mathsf{G}_n} \widetilde{T}_n$ is in $\mathbb{Z}[\mathbf{Y}]_{L_2}$, with $L_2 = \mathsf{G}_n d_{\mathscr{V}} + 1$. Let thus

$$M_1 = (3nd_{\mathscr{V}} + n^2)d_{\mathscr{V}} + L_1 \quad \text{and} \quad M_2 = (3nd_{\mathscr{V}} + n^2)d_{\mathscr{V}} + L_2.$$

For $i = 1, 2$, by Proposition 8, there exists an (M_i, L_i)-equiprojectable set Λ_i such that all points in Λ_i are good specializations. Hence, we will interpolate the coefficients of $a_n N_n$ at Λ_1 and those of $a_n^{\mathsf{G}_n} \widetilde{T}_n$ at Λ_2, and deduce the height bounds on N_n and T_n given in Theorem 1. As was said before, replacing $\mathscr{V}$ by its projection $\mathscr{V}_\ell$ gives the analogue bounds for *all* polynomials $(N_1, \ldots, N_n)$ and $(T_1, \ldots, T_n)$.

Bound on N_n. Write $a_n N_n$ as

$$a_n N_n = \sum_{\mathbf{i}} g_{\mathbf{i},n} X_1^{i_1} \cdots X_n^{i_n} + g_n X_n^{d_n},$$

where all multi-indices $\mathbf{i} = (i_1, \ldots, i_n)$ satisfy $i_\ell < d_\ell$ for $\ell \leq n$, and all coefficients $g_{\mathbf{i},n}$ and g_n are in $\mathbb{Z}[\mathbf{Y}]$. Proposition 9 shows that for $\mathbf{y}$ in Λ_1, we have the inequality

$$\ell_{v_\infty}(a_{n,\mathbf{y}} N_{n,\mathbf{y}}) \leq 2h_{\mathscr{V}} + (6m+5)d_{\mathscr{V}} \log(m+n+2) + (m+1)d_{\mathscr{V}} \log(M_1) + m \log(d_{\mathscr{V}}+1) + \mathsf{H}_n.$$

Applying Proposition 7 to interpolate each $g_{\mathbf{i},n}$ and g_n, we deduce that they all satisfy

$$\begin{aligned} \ell_{v_\infty}(g_{\mathbf{i},n}),\ \ell_{v_\infty}(g_n) \leq\ & 2h_{\mathscr{V}} + (6m+5)d_{\mathscr{V}} \log(m+n+2) + (m+1)d_{\mathscr{V}} \log(M_1) \\ & + m \log(d_{\mathscr{V}}+1) + \mathsf{H}_n + mL_1 \log(M_1+1) + m \log(L_1). \end{aligned}$$

To simplify this expression, we use the definition $L_1 = d_{\mathscr{V}} + 1$ and the upper bounds

$$\mathsf{H}_n \leq 5 \log(n+3)(d_{\mathscr{V}} + n), \quad n+3 \leq m+n+3, \quad m+n+2 \leq m+n+3.$$

After a few simplifications, we obtain that $\ell_{v_\infty}(g_{\mathbf{i},n})$ and $\ell_{v_\infty}(g_n)$ both admit the upper bound

$$2h_{\mathscr{V}} + 2m \log(d_{\mathscr{V}}+1) + \big((6m+10)d_{\mathscr{V}} + 5n\big) \log(m+n+3) + \big((2m+1)d_{\mathscr{V}} + m\big) \log(M_1+1).$$

We continue by remarking that we have the inequality

$$M_1 + 1 \leq (m+n+3)^2 (d_{\mathscr{V}}+1)^2,$$

which gives

$$\ell_{v_\infty}(g_{\mathbf{i},n}),\ \ell_{v_\infty}(g_n) \leq 2h_{\mathscr{V}} + \big((4m+2)d_{\mathscr{V}} + 4m\big) \log(d_{\mathscr{V}}+1) + \big((10m+12)d_{\mathscr{V}} + 5n + 2m\big) \log(m+n+3).$$

Note that $\ell_{v_\infty}(a_n)$ satisfies the same upper bound, in view of Proposition 5. To conclude, we write N_n as

$$N_n = \sum_{\mathbf{i}} \frac{g_{\mathbf{i},n}}{a_n} X_1^{i_1} \cdots X_n^{i_n} + \frac{g_n}{a_n} X_n^{d_n}.$$

After clearing common factors in the coefficients $g_{\mathbf{i},n}/a_n$ and g_n/a_n, the logarithmic absolute value can increase by at most $4d_{\mathscr{V}} \log(m+1)$ (by $\mathbf{A_3}$), since we have seen that all polynomials involved have degree at most $d_{\mathscr{V}}$. We let $\gamma_{\mathbf{i},n}/\varphi_{\mathbf{i},n}$ and γ_n/φ_n be the reduced forms $g_{\mathbf{i},n}/a_n$ and g_n/a_n, that is, obtained after clearing all common factors in $\mathbb{Z}[\mathbf{Y}]$. This gives the height-related statement in the first point of Theorem 1; the claim of the lcm of all $\varphi_{\mathbf{i},n}$ and φ_n follows, since this lcm divides a_n.

Bound on T_n. Similarly, for $\mathbf{y}$ in Λ_2, we have (from Proposition 9)

$$\ell_{v_\infty}(a_{n,\mathbf{y}}^{\mathsf{G}_n} \widetilde{T}_{n,\mathbf{y}}) \leq \mathsf{G}_n\big(2h_{\mathscr{V}} + (6m+5)d_{\mathscr{V}} \log(m+n+2) + (m+1)d_{\mathscr{V}} \log(M_2) + m\log(d_{\mathscr{V}}+1)\big) + \mathsf{l}_n.$$

Proceeding for $a_n^{\mathsf{G}_n} \widetilde{T}_n$ as we did for $a_n N_n$, we first write

$$a_n^{\mathsf{G}_n} \widetilde{T}_n = \sum_{\mathbf{i}} b_{\mathbf{i},n} X_1^{i_1} \cdots X_n^{i_n} + b_n X_n^{d_n},$$

where all multi-indices $\mathbf{i} = (i_1, \dots, i_n)$ satisfy $i_\ell < d_\ell$ for $\ell \leq n$, and all coefficients $b_{\mathbf{i}_n}$ and b_n are in $\mathbb{Z}[\mathbf{Y}]$. This time, we obtain after interpolation

$$\begin{aligned} \ell_{v_\infty}(b_{\mathbf{i},n}),\ \ell_{v_\infty}(b_n) \ \leq\ & \mathsf{G}_n\big[2h_{\mathscr{V}} + (6m+5)d_{\mathscr{V}} \log(m+n+2) + (m+1)d_{\mathscr{V}} \log(M_2) \\ & + m\log(d_{\mathscr{V}}+1)\big] + \mathsf{l}_n + mL_2 \log(M_2+1) + m\log(L_2). \end{aligned}$$

Now, we use the upper bounds

$$\mathsf{G}_n \leq 2d_{\mathscr{V}}, \quad \mathsf{l}_n \leq 3d_{\mathscr{V}}^2 + 5\log(m+n+3)(d_{\mathscr{V}}+n), \quad L_2 \leq 2d_{\mathscr{V}}^2+1, \quad M_2+1 \leq 2(m+n+3)^2(d_{\mathscr{V}}+1)^2,$$

and $\log(L_2) \leq 1 + 2\log(d_{\mathscr{V}}+1)$. We obtain the following upper bound on $\ell_{v_\infty}(b_{\mathbf{i},n})$ and $\ell_{v_\infty}(b_n)$:

$$\begin{aligned} \ell_{v_\infty}(b_{\mathbf{i},n}), \quad \ell_{v_\infty}(b_n) \ \leq\ & 4d_{\mathscr{V}} h_{\mathscr{V}} + 3d_{\mathscr{V}}^2 + m + 2\big((4m+2)d_{\mathscr{V}}^2 + md_{\mathscr{V}} + 2m\big)\log(d_{\mathscr{V}}+1) \\ & + \big((20m+14)d_{\mathscr{V}}^2 + 5d_{\mathscr{V}} + 5n + 2m\big)\log(m+n+3). \end{aligned}$$

To obtain bounds on T_n itself, we recall that this polynomial is monic in X_n; thus, it is enough to divide $a_n^{\mathsf{G}_n} \widetilde{T}_n$ by its leading coefficient b_n to recover T_n. As in the previous case, clearing common factors may induce a growth in logarithmic absolute value, this time by at most $4\mathsf{G}_n d_{\mathscr{V}} \log(m+1) \leq 8d_{\mathscr{V}}^2 \log(m+1)$ (since all polynomials involved have degree at most $\mathsf{G}_n d_{\mathscr{V}}$ by Proposition 5). Taking this into account gives the estimate

$$\begin{aligned} & 4d_{\mathscr{V}} h_{\mathscr{V}} + 3d_{\mathscr{V}}^2 + m + 2\big((4m+2)d_{\mathscr{V}}^2 + md_{\mathscr{V}} + 2m\big)\log(d_{\mathscr{V}}+1) \\ & + \big((20m+22)d_{\mathscr{V}}^2 + 5d_{\mathscr{V}} + 5n + 2m\big)\log(m+n+3). \end{aligned}$$

The second point in Theorem 1 follows after a few quick simplifications.

8 Application

To conclude, we give details of an application of our results. We work under our usual notation, and we suppose that we are given a system $(f_1, \dots, f_n)$ in $\mathbb{Z}[\mathbf{Y}, \mathbf{X}]$, such that $\mathscr{V} = Z(f_1, \dots, f_n)$, and such that the Jacobian determinant J of $(f_1, \dots, f_n)$ with respect to $(X_1, \dots, X_n)$ does not vanish identically on any irreducible component of $\mathscr{V}$. As a consequence, $\mathscr{V}$ satisfies the first condition of Assumption 2; we will actually suppose that $\mathscr{V}$ satisfies the second condition as well.

These assumptions are satisfied if for instance $\mathscr{V}$ is the graph of a dominant polynomial mapping $\mathbb{C}^n \to \mathbb{C}^n$, with f_i of the form $Y_i - \varphi_i(\mathbf{X})$. More generally, we can make a few remarks on the strength of these assumptions.

- If we did not make our assumption on the Jacobian determinant, it would still be possible to restrict the study to the components of $\mathscr{V}$ where J does not vanish identically, by adjoining the polynomial $1 - SJ$ to the system $(f_1, \dots, f_n)$, where S is a new variable.

- The second condition of Assumption 2 is stronger. If we are not in a situation where we can guarantee it (as on the example above), the proper solution will be to replace the discussion below by a more general one that takes into account the *equiprojectable decomposition* of $\mathscr{V}^\star$ (Dahan et al., 2005). We do not consider this here.

Under our assumptions, the question we study here is the following. To compute either $(T_1, \dots, T_n)$ or $(N_1, \dots, N_n)$, it is useful to know in advance their degrees in the variables $\mathbf{Y}$ (exactly, not only upper bounds, as in Dahan and Schost (2004)): for instance, it can help determine how far we proceed in a Newton-Hensel lifting process.

A natural solution is to use modular techniques, that is, to determine the degrees after reduction modulo a prime p: indeed, for all p, except a finite number, the degrees obtained by solving the system modulo p will coincide with those obtained over $\mathbb{Q}$. The obvious question is then, how large to choose p to ensure that this is indeed the case, with a high enough probability? Before giving our answer, we remark that in practice, one should as well reduce to the case $m = 1$ by restricting to a random line in the $\mathbf{Y}$-space; we will not analyze this aspect, as the proof techniques are quite similar to what we show here.

For a prime p, and a polynomial f in $\mathbb{Q}(\mathbf{Y})[\mathbf{X}]$, we denote by f_p the polynomial in $\mathbb{F}_p(\mathbf{Y})[\mathbf{X}]$ obtained by reducing all coefficients of f modulo p, assuming the denominator of no coefficient of f vanishes modulo p. Besides, for f in either $\mathbb{Q}(\mathbf{Y})[\mathbf{X}]$, or $\mathbb{F}_p(\mathbf{Y})[\mathbf{X}]$, we let $\delta(f)$ be the maximum of the quantities $\deg(a) + \deg(b)$, for any coefficient a/b of f, with $\gcd(a, b) = 1$. Our question here will be to estimate $(\delta(T_1), \dots, \delta(T_n))$.

The main result of this section is the following proposition; it takes the form of a big-Oh estimate but the proof gives explicit results. Remark that we choose to measure the size of p using quantities that can be read off on the system of generators $(f_1, \dots, f_n)$, since this is the input usually available in practice.

Proposition 10. *Suppose that $(f_1, \ldots, f_n)$ have height bounded by h and degrees bounded by d. Then, there exists a non-zero integer A of height*

$$\mathcal{H}_A = O((m+n)^2 n^5 d^{4n+4}(nh + (m+n)^2 \log(d))),$$

such that, for any prime p, if $A \bmod p \neq 0$, the following holds:

- *all polynomials $(T_{1,p}, \ldots, T_{n,p})$ are well-defined;*
- *the ideal $\langle T_{1,p}, \ldots, T_{n,p}\rangle$ is radical and coincides with the ideal $\langle f_{1,p}, \ldots, f_{n,p}\rangle$ in $\mathbb{F}_p(\mathbf{Y})[\mathbf{X}]$;*
- *for all $\ell \leq n$, the equality $\delta(T_\ell) = \delta(T_{\ell,p})$ holds.*

In other words, if $A \bmod p \neq 0$, by solving the system $(f_{1,p}, \ldots, f_{n,p})$ in $\mathbb{F}_p(\mathbf{Y})[\mathbf{X}]$ by means of the polynomials $(T_{1,p}, \ldots, T_{n,p})$, we can read off the quantities $(\delta(T_1), \ldots, \delta(T_n))$. Note that the bound on $\mathcal{H}_A$ is polynomial in the Bézout number; we believe that this is hardly avoidable (as long as we express it using n, d, h), though the exponent 4 may not be optimal.

The last part of this section will be devoted to prove this proposition; first, we give an estimate on the random determination of a "good prime" p, whose proof is a consequence of (von zur Gathen and Gerhard, 1999, Th. 18.10(i)).

Proposition 11. *One can compute in time $(n \log(mdh))^{O(1)}$ an integer p such that $6\mathcal{H}_A \leq p \leq 12\mathcal{H}_A$, and, with probability at least $1/2$, p is prime and does not divide A.*

Remark that for p as above, arithmetic operations in $\mathbb{F}_p$ can be done in $(n \log(mdh))^{O(1)}$ bit operations. For a concrete example, suppose that $m = 1$, $n = 12$, that $f_1, \ldots, f_{12}$ have height bounded by $h = 20$ and degrees bounded by $d = 3$: this is already quite a large example, since the Bézout number is 531441. In this case, evaluating explicitly all bounds involved in the former results shows that we would compute modulo primes of about 124 bits: this is routinely done in a system such as Magma (Bosma et al., 1997).

We now prove Proposition 10; we start by constructing explicitly the integer A. For $\ell \leq n$, recall that we wrote in Theorem 1

$$T_\ell = \sum_{\mathbf{i}} \frac{\beta_{\mathbf{i},\ell}}{\alpha_{\mathbf{i},\ell}} X_1^{i_1} \cdots X_\ell^{i_\ell} + X_\ell^{d_\ell}.$$

- For $\ell \leq n$, we first let $A_{0,\ell}$ be any non-zero coefficient of one of the polynomials $\alpha_{\mathbf{i},\ell}$, and take $A_0 = A_{0,1} \cdots A_{0,n}$.
- By assumption, the Zariski-closure of $\Pi_0(Z(f_1, \ldots, f_n, J))$ is not dense, so it is contained in a hypersurface. Thus, there exists a non-zero polynomial $H \in \mathbb{Z}[\mathbf{Y}]$ such that $Z(H) \subset \mathbb{C}^m$ contains $\Pi_0(Z(f_1, \ldots, f_n, J))$. We let A_1 be any non-zero coefficient of such a polynomial H.

- Let S be a new variable; then by construction, the ideal $\langle 1 - SH, f_1, \ldots, f_n, J\rangle \subset \mathbb{Q}[\mathbf{Y}, \mathbf{X}, S]$ is the trivial ideal $\langle 1\rangle$. We let A_2 be a non-zero integer that belongs to the ideal generated by $(1 - SH, f_1, \ldots, f_n, J)$ in $\mathbb{Z}[\mathbf{Y}, \mathbf{X}, S]$.

- For $\ell \le n$, let g_ℓ/h_ℓ be a coefficient of T_ℓ that maximizes the sum $\deg(\beta_{\mathbf{i},\ell}) + \deg(\alpha_{\mathbf{i},\ell})$. We let $A_{3,\ell}$ be a non-zero integer such that if $A_{3,\ell} \bmod p \neq 0$, g_ℓ and h_ℓ remain coprime modulo p, and their degrees do not drop modulo p. Theorem 7.5 in (Geddes et al., 1992) shows the existence of a non-zero integer $a_{3,\ell}$ that satisfies the first requirement; we take for $A_{3,\ell}$ the product of $a_{3,\ell}$ by one coefficient of highest degree in g_ℓ and one in h_ℓ. As before, we take $A_3 = A_{3,1} \cdots A_{3,n}$.

We then let $A = A_0A_1A_2A_3$, and we first show that this choice of A satisfies our requirements.

Lemma 10. *For any prime p, if $A \bmod p \neq 0$, the conclusions of Proposition 10 hold.*

Proof. Let us fix p, and let us write $\mathscr{V}^\star = Z(f_1, \ldots, f_n) \subset \overline{\mathbb{Q}(\mathbf{Y})}^n$ and $\mathscr{V}_p^\star = Z(f_{1,p}, \ldots, f_{n,p}) \subset \overline{\mathbb{F}_p(\mathbf{Y})}^n$. If $A \bmod p \neq 0$, $A_0 \bmod p \neq 0$, so all polynomials $(T_{1,p}, \ldots, T_{n,p})$ are well-defined and still form a Gröbner basis. Since $(T_1, \ldots, T_n)$ reduce $(f_1, \ldots, f_n)$ to zero in $\mathbb{Q}(\mathbf{Y})[\mathbf{X}]$, the reduction relation can be specialized modulo p, as it involves no new denominator. We deduce that the zero-set $Z(T_{1,p}, \ldots, T_{n,p}) \subset \overline{\mathbb{F}_p(\mathbf{Y})}^n$ is contained in $\mathscr{V}_p^\star$.

If $A \bmod p \neq 0$, we also have $A_1 \bmod p \neq 0$ and $A_2 \bmod p \neq 0$; as a consequence, $H \bmod p \neq 0$ and thus the ideal $\langle f_{1,p}, \ldots, f_{n,p}, J_p\rangle \subset \mathbb{F}_p(\mathbf{Y})[\mathbf{X}]$ is the trivial ideal. This implies that $\mathscr{V}_p^\star$ is finite, by the Jacobian criterion, since the Jacobian determinant J_p vanishes nowhere on $\mathscr{V}_p^\star$. Besides, we also obtain that the roots of $\langle f_{1,p}, \ldots, f_{n,p}\rangle$ have multiplicity 1; the claims in the previous paragraph show that this is the case for $\langle T_{1,p}, \ldots, T_{n,p}\rangle$ as well. Thus, to obtain the second point, it suffices to prove that $|Z(T_{1,p}, \ldots, T_{n,p})| = |\mathscr{V}_p^\star|$.

First, we prove the inequality $|\mathscr{V}_p^\star| \le |\mathscr{V}^\star|$. Let $\mathbf{y} = (y_1, \ldots, y_m) \in \overline{\mathbb{F}_p}^m$ be such that J vanishes nowhere on the fiber $\mathscr{V}_{\mathbf{y}} = Z(f_{1,p}(\mathbf{y}, \mathbf{X}), \ldots, f_{n,p}(\mathbf{y}, \mathbf{X})) \subset \overline{\mathbb{F}_p}^n$, and such that $|\mathscr{V}_{\mathbf{y}}| = |\mathscr{V}_p^\star|$; such an $\mathbf{y}$ exists, by (Heintz, 1983, Prop. 1) (therein, the author assumes that the extension $\overline{\mathbb{F}_p}(\mathbf{Y}) \to \overline{\mathbb{F}_p}(\mathbf{Y})[\mathbf{X}]/\langle f_{1,p}, \ldots, f_{n,p}\rangle$ be separable: this is the case here by the Jacobian criterion). Let $\mathbb{F}_q$ be a finite extension of $\mathbb{F}_p$ that contains all coordinates of all points in $\mathscr{V}_{\mathbf{y}}$. Then, using Newton iteration modulo powers of $\langle p, Y_1 - y_1, \ldots, Y_m - y_m\rangle$, all points in $\mathscr{V}_{\mathbf{y}}$ can be lifted to solutions of $(f_1, \ldots, f_n)$ in $\mathbb{Z}_q[[\mathbf{Y} - \mathbf{y}]]$, where $\mathbb{Z}_q$ is a finite integral extension of $\mathbb{Z}_p$. Since $\mathbb{Z}_q[[\mathbf{Y} - \mathbf{y}]]$ contains $\mathbb{Z}[\mathbf{Y}]$, the number of solutions of $(f_1, \ldots, f_n)$ in an algebraic closure of the fraction field of $\mathbb{Z}_q[[\mathbf{Y} - \mathbf{y}]]$ is $|\mathscr{V}^\star|$. As a consequence, the cardinality of $\mathscr{V}_p^\star$, which equals that of $\mathscr{V}_{\mathbf{y}}$, is at most that of $\mathscr{V}^\star$, as claimed.

Let $d_1, \ldots, d_n$ be the degrees of $T_1, \ldots, T_n$ in respectively $X_1, \ldots, X_n$. In view of the inclusion proved above, we deduce the inequalities

$$d_1 \cdots d_n = |Z(T_{1,p}, \ldots, T_{n,p})| \le |\mathscr{V}_p^\star| \le |\mathscr{V}^\star| = d_1 \cdots d_n.$$

As said before, this establishes the second point of the proposition.

It remains to deal with the last point. If $A_3 \bmod p \neq 0$, then for all $\ell \le n$, $A_{3,\ell} \bmod p \neq 0$; the definition we adopted for $A_{3,\ell}$ ensures that in this case, g_ℓ and h_ℓ remain coprime and keep the same degree modulo p, as needed. $\square$

It remains to estimate $h(A) = h(A_0) + h(A_1) + h(A_2) + h(A_3)$. Combining the results of the next paragraphs finishes the proof of Proposition 10.

Height of A_0. By construction, using the notation of Theorem 1, we have $h(A_0) \leq \mathcal{H}'_1 + \cdots + \mathcal{H}'_n$, with for all ℓ

$$\mathcal{H}'_\ell = O\big(d^{2n}(nh + mn\log(d) + (m+n)\log(m+n))\big).$$

In particular, we have

$$h(A_0) = O\big(d^{2n}(n^2h + mn^2\log(d) + n(m+n)\log(m+n))\big).$$

Height of A_1. Next, we estimate the degree and height of the polynomial H. Let $\mathscr{V}' = Z(f_1, \ldots, f_n, J)$; if $\mathscr{V}'$ is empty, we take $H = 1$ and we are done. Otherwise, we get $\dim(\mathscr{V}') \leq m-1$. By Bézout's theorem, the degree $d_{\mathscr{V}'}$ of $\mathscr{V}'$ is bounded from above by nd^{n+1}. Further, note that $h(J) \leq h'$, with $h' = n(h + \log(nd) + d\log(n+1))$, in view of the discussion following (Krick et al., 2001, Lemma 1.2). Applying twice the arithmetic Bézout theorem (in the form of (Krick et al., 2001, Coro. 2.11)), first to bound the height of $\mathscr{V}$ and then of $\mathscr{V}'$, we deduce the inequality

$$h_{\mathscr{V}'} \leq nd^{n+1}(nh + h' + (m+2n+1)\log(m+n+1))$$

and thus

$$h_{\mathscr{V}'} \leq nd^{n+1}(2nh + n\log(nd) + nd\log(n+1) + (m+2n+1)\log(m+n+1)).$$

Let us decompose $\mathscr{V}'$ into its irreducible components $\mathscr{V}'_1, \ldots, \mathscr{V}'_K$. For each such component $\mathscr{V}'_k$, there exists a subset $\mathbf{Y}_k$ of $Y_1, \ldots, Y_m$ such that the Zariski-closure of the projection of $\mathscr{V}'$ on the $\mathbf{Y}_k$-space is a hypersurface.

Fix $k \leq K$, let φ_k be the corresponding projection, and let $\mathscr{W}_k$ be the Zariski-closure of $\varphi_k(\mathscr{V}'_k)$. The degree of $\mathscr{W}_k$ is at most that of $\mathscr{V}'_k$; by (Krick et al., 2001, Lemma 2.6), the height of $\mathscr{W}_k$ is at most $h_{\mathscr{V}'_k} + 3md_{\mathscr{V}'_k}\log(n+m+1)$. As a consequence, using the remarks on (Philippon, 1995, p. 347), we deduce that there exists a non-zero polynomial $H_k \in \mathbb{Z}[\mathbf{Y}_k]$ of degree at most $d_{\mathscr{V}'_k}$ and height at most $h_{\mathscr{V}'_k} + d_{\mathscr{V}'_k}(3m\log(n+m+1)+2)$ that defines $\mathscr{W}_k$.

We can take $H = H_1 \cdots H_K$. The degree of H is bounded by $d_{\mathscr{V}'}$; using (Krick et al., 2001, Lemma 1.2.1.b), we see that its height is bounded by

$$h'' = nd^{n+1}(2nh + (4m+2n+2)\log(m+n+1) + n\log(nd) + nd\log(n+1) + 2).$$

We deduce in particular

$$h(A_1) = O(nd^{n+1}(nh + nd\log(n) + (m+n)\log(m+n))).$$

Height of A_2. We are going to apply a suitable version of the arithmetic Nullstellensatz (Krick et al., 2001, Th. 2). We would also like to mention the recent work of Jelonek (2005): it gives finer estimates for the degrees of polynomials in the effective Nullstellensatz, and it might be possible to derive also better height estimates with his technique. We will not pursue this here.

The polynomials $(1-SH, J, f_1, \ldots, f_n)$ have degrees at most $(d'', d', d, \ldots, d)$, with $d' = nd$ and $d'' = nd^{n+1} + 1$; their heights are bounded by $(h'', h', h, \ldots, h)$, with h' and h'' as above. Definition 4.7 in (Krick et al., 2001) associates to such a system of equations a *degree* δ and a *height* η; Theorem 2 in (Krick et al., 2001) then shows that we can take

$$h(A_2) \leq (m+n+2)^2 d''(2\eta + (h'' + \log(n+2))\delta + 21(m+n+2)^2 d''\delta \log(d''+1)). \quad (7)$$

The quantities δ and η satisfy the following inequalities. Let Γ be the set of $(n+2) \times (n+2)$ integer matrices with coefficients of height at most $\nu = 2(m+n+2)\log(d''+1)$. To a matrix $\mathbf{A}$ in Γ, associate the polynomials

$$g_{\mathbf{A},i} = A_{i,1}(1 - SH) + A_{i,2}J + A_{i,3}f_1 + \cdots + A_{i,n+2}f_n, \quad 1 \leq i \leq n+2$$

and the algebraic set $\mathscr{W}_{\mathbf{A}} = Z(g_{\mathbf{A},1}, \ldots, g_{\mathbf{A},n+2})$. Then $\delta \leq \max_{\mathbf{A}\in\Gamma} d_{\mathscr{W}_{\mathbf{A}}}$ and $\eta \leq \max_{\mathbf{A}\in\Gamma} h_{\mathscr{W}_{\mathbf{A}}}$.

To give good estimates on these quantities, we perform linear combinations of the equations $g_{\mathbf{A},i}$ to partially triangulate them, by eliminating $1 - SH$ from all equations except the first one and J from all equations except the first two ones. As in the proof of (Krick et al., 2001, Lemma 4.8), for any $\mathbf{A} \in \Gamma$, the ideal $\langle g_{\mathbf{A},1}, \ldots, g_{\mathbf{A},n+2}\rangle$ is equal to the ideal $\langle g^\star_{\mathbf{A},1}, \ldots, g^\star_{\mathbf{A},n+2}\rangle$ with the shape just described:

- $g^\star_{\mathbf{A},1} = A^\star_{1,1}(1 - SH) + A^\star_{1,2}J + A^\star_{1,3}f_1 + \cdots + A^\star_{1,n+2}f_n$,
- $g^\star_{\mathbf{A},2} = A^\star_{2,2}J + A^\star_{2,3}f_1 + \cdots + A^\star_{2,n+2}f_n$,
- $g^\star_{\mathbf{A},i} = A^\star_{i,3}f_1 + \cdots + A^\star_{i,n+2}f_n$ for $i \geq 3$.

Besides, one can take the coefficients $A^\star_{1,j}$ as entries of $\mathbf{A}$, the coefficients $A^\star_{2,j}$ as minors of $\mathbf{A}$ of size 2, and the coefficients $A^\star_{i,j}$ as minors of $\mathbf{A}$ of size 3, for $i \geq 3$. This implies that we have

- $\deg(g^\star_{\mathbf{A},1}) \leq d''$ and $h(g^\star_{\mathbf{A},1}) \leq \ell'' = h'' + \nu + \log(n+2)$;
- $\deg(g^\star_{\mathbf{A},2}) \leq d'$ and $h(g^\star_{\mathbf{A},2}) \leq \ell' = h' + 2\nu + \log(2) + \log(n+2)$;
- $\deg(g^\star_{\mathbf{A},i}) \leq d$ and $h(g^\star_{\mathbf{A},i}) \leq \ell = h + 3\nu + \log(6) + \log(n+2)$ for $i \geq 3$.

It follows that $\delta \leq d^n d' d'' = n^2 d^{2n+2} + nd^{n+1}$, as showed in (Krick et al., 2001, Lemma 4.8). The estimate we obtain on η is finer than the one in that lemma, though: we apply a first time the arithmetic Bézout theorem (Krick et al., 2001, Coro. 2.11), to obtain a bound on the height of $Z(g^\star_{\mathbf{A},3}, \ldots, g^\star_{\mathbf{A},n+2})$, then intersect it with $Z(g^\star_{\mathbf{A},2})$ and $Z(g^\star_{\mathbf{A},1})$. This results in the inequality

$$\eta \leq d^n\big(d''d'((n+2)\ell + (m+2n+3)\log(m+n+2)) + \ell'd'' + \ell''d'\big),$$

from which a bound on $h(A_2)$ follows by means of (7). All formulas given in this paragraph yield explicit bounds; however, after a few simplifications, we find the big-Oh estimate

$$h(A_2) = O((m+n)^2 n^5 d^{4n+4}(nh + (m+n)^2 \log(d))).$$

Height of A_3. Let us fix $\ell \leq n$. The corollary to Theorem 7.5 in (Geddes et al., 1992) shows that the integer $a_{3,\ell}$ has height at most $2d^{2n}m(\mathcal{H}'_\ell + m\log(2d^{2n}+1))$; the height bound of $A_{3,\ell}$ follows by adding $2\mathcal{H}'_\ell$. This leads to an upper bound on $h(A_3)$ by summing for $\ell = 1, \ldots, n$; we obtain

$$h(A_3) = O\big(d^{4n}(mnh + m^2 n \log(d) + m(m+n)\log(m+n))\big).$$

Acknowledgments We acknowledge the support of NSERC, the Canada Research Chairs Program and MITACS; and of the Japanese Society for the Promotion of Science (Global-COE program "Maths-for-Industry").

References

M. E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeroes, multiplicities and idempotents for zerodimensional systems. In *MEGA'94*, volume 142 of *Progress in Mathematics*, pages 1–15. Birkhäuser, 1996.

P. Aubry and A. Valibouze. Using Galois ideals for computing relative resolvents. *J. of Symbolic computation*, 30(6):635–651, 2000.

P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *J. of Symbolic Computation*, 28(1,2):45–124, 1999.

W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symb. Comp.*, 24(3-4):235–265, 1997.

P. Bürgisser, M. Clausen, and A. Shokrollahi. *Algebraic complexity theory*. Springer, 1997.

D. Cox, J. Little, and D. O'Shea. *Using algebraic geometry*. Graduate Texts in Mathematics. Springer-Verlag, 1998.

X. Dahan and É. Schost. Sharp estimates for triangular sets. In *ISSAC'04*, pages 103–110. ACM, 2004.

X. Dahan, M. Moreno Maza, É. Schost, W. Wu, and Y. Xie. Lifting techniques for triangular decompositions. In *ISSAC'05*, pages 108–115. ACM, 2005.

X. Dahan, X. Jin, M. Moreno Maza, and É. Schost. Change of order for regular chains in positive dimension. *Theoretical Computer Science*, 392(1–3):37–65, 2008.

G. Gallo and B. Mishra. Efficient algorithms and bounds for Wu-Ritt characteristic sets. In T. Mora and C. Traverso, editors, *Progress in Math.*, volume 94, pages 235–248. Proceedings MEGA'90, Birkhäuser, 1990.

K. O. Geddes, S. R. Czapor, and G. Labahn. *Algorithms for computer algebra*. Kluwer Academic Publishers, Boston, MA, 1992.

M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *J. of Complexity*, 17(2):154–211, 2001.

J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theoret. Comput. Sci.*, 24(3):239–277, 1983.

N. Higham. *Accuracy and stability of numerical algorithms, 2nd ed.* SIAM, 2002.

Z. Jelonek. On the effective Nullstellensatz. *Inventiones Mathematicae*, 162(1):1–17, 2005.

T. Krick, L. M. Pardo, and M. Sombra. Sharp estimates for the arithmetic Nullstellensatz. *Duke Math. Journal*, 109:521–598, 2001.

S. Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983.

D. Lazard. Solving zero-dimensional algebraic systems. *J. Symb. Comput.*, 13:147–160, 1992.

P. J. McCarthy. *Algebraic extensions of fields*. Dover, New York, 1991.

P. Philippon. Sur des hauteurs alternatives III. *J. Math. Pures Appl.*, 74(4):345–365, 1995.

F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Applicable Algebra in Engineering, Communication and Computing*, 9(5):433–461, 1999.

J. Sabia and P. Solernó. Bounds for traces in complete intersections and degrees in the Nullstellensatz. *Appl. Algebra Engrg. Comm. Comput.*, 6(6):353–376, 1995.

É. Schost. Complexity results for triangular sets. *J. Symb. Comput.*, 36(3-4):555–594, 2003a.

É. Schost. Computing parametric geometric resolutions. *Appl. Algebra Engrg. Comm. Comput.*, 13(5):349–393, 2003b.

M. Sombra. *Estimaciones para el teorema de ceros de Hilbert*. PhD thesis, Universidad de Buenos Aires, 1998.

J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, New York, NY, USA, 1999.