EFFECTIVE BOUNDS FOR POLYNOMIAL SYSTEMS DEFINED OVER THE RATIONALS

TERESA KRICK

Dedicated to my advisor, Joos Heintz, 27 October 1945–3 October 2024

1. Introduction

This course aims to present some material that illustrates the kind of estimates we can obtain in effective algebraic geometry, for affine polynomial equation systems defined over the rational numbers $\mathbb{Q}$. I'll consider the case where polynomials are assumed to be given in *dense representation*: a polynomial f in n variables is described by an a priori bound d for its *degree* and the array of its $\binom{d+n}{n} \leq (n+1)^d$ coefficients (zero-coefficients as well as non-zero ones), and when it has integer coefficients, a bound h for their *heights*, i.e. their bit sizes. The accent here is put on describing degree and height bounds for polynomials and polynomial identities arising when solving some classical problems, not on the algorithms to obtain them. Bounds are interesting per se as a complexity measure, but are also useful to know in advance when performing any algorithm or to certify results obtained by numerical algorithms. Although the estimates look somehow coarse, I preferred to present them in detail instead of adopting the $\mathcal{O}$ notation, to show that the bounds are precise with definite universal constants.
Since this is a short course, and wishing to stay at an understandable level, I'll only focus here on systems on equations defining a finite (possibly empty) number of solutions in $\mathbb{C}^n$: a friendly introductory reference that presents this setting is the famous book by Cox, Little and O'Shea [CLO2015, Ch.4 & 5]. Needless to say, there are in the literature many more results and extensions of what I am presenting here, obtained by a huge community, in multiple different settings and directions:

- Algorithms,
- for positive dimension systems of equations as well,
- in the projective, multiprojective, sparse (with its different meanings), toric settings,
- with their corresponding encodings and measures of the data, including the *straight-line program* encoding.

This is just a first step to give some flavor of problems that one can consider, and what is done or can be done in effective algebraic geometry over the rationals. I apologize for the biased choice of references and to the people who has done all the work I am not citing.

Last but not least, I want to express my deep gratitude to the organizers of the Journées Nationales de Calcul Formel 2025 for inviting me to present this course and give me the opportunity to revisit all this material.

2. Setting and notations

In all what follows, $\boldsymbol{x} = \{x_1, \ldots, x_n\}$, a set of n variables, and

$$f_1, \ldots, f_s \in \mathbb{C}[\boldsymbol{x}] = \mathbb{C}[x_1, \ldots, x_n]$$

are s polynomials such that the the (affine) algebraic variety

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

is finite: either empty or finite of cardinality ≥ 1.
In terms of the ideal $I = (f_1, \ldots, f_s) \subset \mathbb{C}[\boldsymbol{x}]$, by the Nullstellensatz (see Section 5),

$$V = \emptyset \iff I = \mathbb{C}[\boldsymbol{x}],$$

while when V is finite and non-empty, we say that I is a *zero-dimensional ideal*, which is equivalent to the fact that the $\mathbb{C}$-vector space $\mathbb{C}[\boldsymbol{x}]/I$ is of finite dimension ≥ 1.

We set $\deg(V) := \#(V)$ and $D := \dim_{\mathbb{C}} \big(\mathbb{C}[\boldsymbol{x}]/I\big)$.

For zero-dimensional ideals, we necessarily have that $s \geq n$ since k polynomials in $\mathbb{C}[\boldsymbol{x}]$ define a variety, which –if not empty– is of dimension at least $n - k$.

We will soon consider the case when the variety V is defined over the rational numbers $\mathbb{Q}$, i.e. we take $f_1, \ldots, f_s \in \mathbb{Q}[\boldsymbol{x}]$, or even simpler, in $\mathbb{Z}[\boldsymbol{x}]$, that is, with integer coefficients, and $I = (f_1 \ldots, f_s) \subset \mathbb{Q}[\boldsymbol{x}]$. We observe that the dimension D remains the same when considering the quotient rings $\mathbb{Q}[\boldsymbol{x}]/I$ or $\mathbb{C}[\boldsymbol{x}]/I$, where $I \subset \mathbb{Q}[\boldsymbol{x}]$ or $\mathbb{C}[\boldsymbol{x}]$ accordingly.

By definition, the (logarithmic) *height* $\mathrm{h}(f)$ of any (non-zero) polynomial f with integer coefficients, in any number of variables, is the logarithm of the maximum of the absolute values of its coefficients, which are all integer. This notion essentially coincides with the maximum bitsize of all the coefficients and is the second measure of the input polynomials that we will use in this text, in addition to the degrees of these polynomials and their number of variables.

3. The Bézout inequality

The Bézout inequality we are going to use all along is an affine version of the Bézout theorem in projective varieties over algebraically closed fields.

Theorem 3.1. (Bézout inequality)
Let $f_1, \ldots, f_s \in \mathbb{C}[\boldsymbol{x}]$ define a zero-dimensional variety $V \subset \mathbb{C}^n$.
If $f_1, \ldots, f_s \in \mathbb{C}[\boldsymbol{x}]$ are ordered such that $d_j := \deg(f_j)$ for $1 \leq j \leq s$ satisfy

$$d := d_1 \geq d_2 \geq \cdots \geq d_s,$$

then

$$\deg(V) \leq d_1 \cdots d_{n-1} d_s \leq d^{n-1} d_s \leq d^n.$$

For example, taking $d, h \in \mathbb{N}$, for

$$V_1 = V_{\mathbb{C}}(x_1^d - 1, \ldots, x_n^d - 1),$$

we have $V_1 = \{(\varepsilon_1, \ldots, \varepsilon_n) \in \mathbb{C}^n : \varepsilon_1^d = \cdots = \varepsilon_n^d = 1\}$ with $\deg(V_1) = d^n$, while for

$$V_2 = V_{\mathbb{C}}(x_1 - 2^h, x_2 - x_1^d, \ldots, x_n - x_{n-1}^d), \tag{1}$$

we have $V_2 = \{(2^h, 2^{dh}, \ldots, 2^{d^{n-1}h})\}$ with $\deg(V_2) = 1 < d^{n-1}$.

This seemingly lighter version cannot be directly deduced from the classical Bézout theorem since there are zero-dimensional systems that have a finite number of common zeros in $\mathbb{C}^n$ but an infinite number when taking their zeros at infinity; consider for instance the polynomials

$$f_1 = xy, f_2 = xz, f_3 = x - 1$$

which satisfy that $V = \{(1, 0, 0)\}$, although if one homogenizes the polynomials with a first variable, then there are infinite projective zeros

$$(1 : 1 : 0 : 0) \cup (0 : 0 : 0 : 1) \cup \{(0 : 0 : 1 : z) \, : \, z \in \mathbb{C}\}.$$

A pioneering reference for it is Joos Heintz' PhD thesis, published in [Hei1983], where it is shown that if $V, W \subset \mathbb{C}^n$ are arbitrary affine algebraic varieties, then

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

Here $\deg(V)$ is the (geometric) *degree* of the variety V, which for an irreducible variety of dimension r is the maximum finite number of points that one can obtain when intersecting the variety with $n-r$ affine hyperplanes: For an arbitrary variety the degree is defined as the sum of the degrees of its irreducible components; for a hypersurface $V = V(g)$ defined by a squarefree polynomial g, we have $\deg(V) = \deg(g)$; and for a zero-dimensional variety V, $\deg(V) = \#V$. Another proof counting multiplicities can also be found in [MaWh1983, Ch.2, Cor.].

Bézout inequality proves to be very useful in Computer Algebra, because it doesn't make any assumption on the polynomials, neither the way they intersect (no consideration of *genericity* is needed) nor their number: it is enough to consider the smallest degree polynomial and the $n-1$ highest degree polynomials, since one can show that there exist "upper triangular" linear combinations of the input polynomials $f_1, \ldots, f_s$ of the form

$$\left\{ \begin{array}{lcl} q_1 & = & f_s \\ q_2 & = & a_{2,1}f_1 + \cdots + a_{2,n-1}f_{n-1} + \cdots + a_{2,s-1}f_{s-1} \\ \vdots & & \ddots \\ q_n & = & a_{n,n-1}f_{n-1} + \cdots + a_{n,s-1}f_{s-1}, \end{array} \right.$$

for $a_{i,j} \in \mathbb{C}$, such that $\dim\big(V(q_1, \ldots, q_k)\big) = n - k$ and therefore, $V(q_1, \ldots, q_n)$, which obviously contains V, is finite, see for instance [CGH1989, Proof of Thm.14]).

Note that it is not true that there always exist n such linear combinations $q_1, \ldots, q_n$ so that $V(q_1, \ldots, q_n) = V$, as shows the very simple example $(x^3 - x, x^2 - 2x) \subset \mathbb{C}[x]$.

4. An Arithmetic Bézout inequality

The *(logarithmic) height* $\mathrm{h}(V)$ of the zero-dimensional variety V is a parameter that somehow measures the size of the points in V. This is part of a more general theory of heights of varieties. I won't use the most sophisticated definition of height, but rather a notion introduced by Patrice Philippon in [Phi1995] that will be sufficient for our purposes and is defined through the *Chow form* of V. A general presentation of the Chow form can be found in [Sha1974, Sec.I.6.5] and for the connection with the height of a variety I follow [KPS2001, Sec.1].

From now on, $f_1,\dots,f_s \in \mathbb{Z}[\boldsymbol{x}]$. In that case, denoting $\boldsymbol{\zeta} = (\zeta_1,\dots,\zeta_n)$ for $\boldsymbol{\zeta} \in V$, the polynomial

$$\prod_{\boldsymbol{\zeta}\in V} (U_0 + \zeta_1 U_1 + \cdots + \zeta_n U_n)$$

happens to belong to $\mathbb{Q}[\boldsymbol{U}] := \mathbb{Q}[U_0, U_1, \dots, U_n]$ and we can choose $c \in \mathbb{N}$ such that

$$\mathrm{Ch}_V(\boldsymbol{U}) := c \prod_{\boldsymbol{\zeta}\in V} (U_0 + \zeta_1 U_1 + \cdots + \zeta_n U_n) \ \in \mathbb{Z}[\boldsymbol{U}] \tag{2}$$

is a primitive polynomial in $\mathbb{Z}[\boldsymbol{U}]$: this is the (primitive) Chow form of the zero-dimensional variety V. It is an homogeneous polynomial of degree $\deg(V)$, which satisfies that for any $\boldsymbol{u} \in \mathbb{C}^{n+1}$,

$$\begin{aligned} \mathrm{Ch}_V(\boldsymbol{u}) = 0 &\iff u_0 + \zeta_1 u_1 + \cdots + \zeta_n u_n = 0 \text{ for some } \boldsymbol{\zeta} \in V \\ &\iff \exists\, \boldsymbol{\zeta} \in V : \ \boldsymbol{\zeta} \text{ belongs to the hyperplane } \{u_1 x_1 + \cdots + u_n x_n = -u_0\}. \end{aligned}$$

The Chow form of the variety characterizes the variety in the sense that different varieties have different Chow forms, and one can recover the variety from its Chow form.

The *(Philippon-)height* $\mathrm{h}(V)$ is defined through a specific Mahler measure $m(\mathrm{Ch}_V; S_{n+1})$ of the Chow form Ch_V and satisfies the following properties

$$\sum_{\boldsymbol{\zeta}\in V} \log(\|(1,\boldsymbol{\zeta})\|_2) \le \mathrm{h}(V); \tag{3}$$

$$|\mathrm{h}(V) - \mathrm{h}(\mathrm{Ch}_V)| \le 3\log(n+1)\deg(V). \tag{4}$$

Moreover, Corollary 2.11 in [KPS2001] applied to a hypersurface directly implies that we can obtain an arithmetic Bézout inequality that distinguishes the degree and height of one of the polynomials with respect to the others:

Theorem 4.1. (An Arithmetic Bézout inequality)
Let $f_1,\dots,f_s \in \mathbb{Z}[\boldsymbol{x}]$ define a zero-dimensional variety $V \subset \mathbb{C}^n$.
Set $d_j := \deg(f_j)$, $h_j := \mathrm{h}(f_j)$ for $1 \le j \le s$. Assume that $d := d_1 \ge d_2 \ge \cdots \ge d_{s-1}$ (with no condition with respect to d_s), and set $h := \max\{h_1,\dots,h_{s-1}\}$. Then

$$\begin{aligned} \mathrm{h}(V) &\le \Big(\frac{h_s}{d_s} + (n-1)\frac{h}{d_{n-1}} + 2n\log(n+1)\Big) d_1 \cdots d_{n-1} d_s \\ &\le d^{n-1}h_s + (n-1)d^{n-2}d_s h + 2n\log(n+1)d^{n-1}d_s. \end{aligned}$$

Inequality (3) above and the Arithmetic Bézout inequality directly imply the following upper bound for the coordinates of any root $\boldsymbol{\zeta} = (\zeta_1,\dots,\zeta_n) \in V$: For $d_s \le d$ and $h_s \le h$ we get

$$\log(|\zeta_i|) \le n d^{n-1}h + 2n\log(n+1)d^n, \quad 1 \le i \le n. \tag{5}$$

It also shows that the arithmetic Bézout bound is quite sharp in terms of the height dependence since for instance for the variety $V_2 = \{\boldsymbol{\zeta}\}$ defined in (1) above, we have $\mathrm{h}(\zeta_n) = d^{n-1}h$ while the estimate in Theorem 4.1 gives

$$\mathrm{h}(V_2) \le d^{n-1}h + 2n\log(n+1)d^{n-1}.$$

Bound (5) for the coordinates implies in turn an upper bound for the value of any complex polynomial $p \in \mathbb{C}[\boldsymbol{x}]$ at a root of our zero-dimensional variety V defined over $\mathbb{Q}$:

Corollary 4.2. (Upper bounds on the roots)
Let $f_1, \dots, f_s \in \mathbb{Z}[\boldsymbol{x}]$ define a zero-dimensional variety $V \subset \mathbb{C}^n$, with $\deg(f_j) \leq d$ and $\mathrm{h}(f_j) \leq h$ for $1 \leq j \leq s$. Let $p \in \mathbb{Z}[\boldsymbol{x}]$ and set $d_p := \deg(p)$ and h_p for the maximum of the absolute value of the logarithm of all non-zero coefficients of p. Then

$$\log(|p(\boldsymbol{\zeta})|) \leq h_p + nd^{n-1}d_p h + 3n\log(n+1)d^n d_p.$$

Proof. Let $p = \sum_{|\alpha| \leq d_p} a_\alpha \boldsymbol{x}^\alpha$, which has $\binom{d_p+n}{n} \leq (d_p+1)^n$ coefficients. Then, by the bound for the coordinates (5) we have

$$\log(|\zeta_1|^{\alpha_1} \cdots |\zeta_n|^{\alpha_n}) \leq nd^{n-1}d_p h + 2n\log(n+1)d^n d_p,$$

and therefore considering the multiplication by $|a_\alpha|$ and adding up the $(d_p+1)^n$ terms we obtain

$$\begin{aligned}\log(|p(\boldsymbol{\zeta})|) &\leq h_p + nd^{n-1}d_p h + 2n\log(n+1)d^n d_p + n\log(d_p+1)\\ &\leq h_p + nd^{n-1}d_p h + 3n\log(n+1)d^n d_p.\end{aligned}$$

□

But more interestingly, we also obtain lower bounds for the non-zero coordinates of the roots in V, and also for the separation of the roots, which extend the bounds for univariate integer polynomials that appear for example in the beautiful book by Maurice Mignotte [Mig1992], and agree with those that can be found in the literature ([Can1987], [Yap2000, Thm.45, Cor.49], [EMT2020, Cor.9]), with the advantage that we don't need to assume that we have exactly n equations that determine the zero-dimensional variety, or that the system is still zero-dimensional if one considers zeros at infinity. The following is [BKM2024, Lem.4.2 & Lem.4.10], where we can drop the assumption that $\mathrm{h}(p) \leq h$ or $\deg(p) \geq d$ due to the application of the more precise Proposition 4.1. (The upper bounds are not as sharp as in the previous corollary, but I include them anyway for symmetry.)

Proposition 4.3. (Lower and separation bounds on the roots)
Let $f_1, \dots, f_s \in \mathbb{Z}[\boldsymbol{x}]$ define a zero-dimensional variety $V \subset \mathbb{C}^n$, with $\deg(f_j) \leq d$ and $\mathrm{h}(f_j) \leq h$ for $1 \leq j \leq s$. Let $p \in \mathbb{Z}[\boldsymbol{x}]$ and set $d_p := \deg(p)$ and $h_p := \mathrm{h}(p)$. Then, for every $\boldsymbol{\zeta}, \boldsymbol{\xi} \in V$ we have

1. $\big|\log(|p(\boldsymbol{\zeta})|)\big| \leq d^n h_p + 2nd^{n-1}d_p h + 4(n+1)\log(n+2)d^n d_p$ *if* $p(\boldsymbol{\zeta}) \neq 0$;
2. $\big|\log(|p(\boldsymbol{\zeta}) - p(\boldsymbol{\xi})|)\big| \leq d^{2n} h_p + 4nd^{2n-1}d_p h + 4(2n+1)\log(2n+2)d^{2n}d_p$ *if* $p(\boldsymbol{\zeta}) \neq p(\boldsymbol{\xi})$.

In particular, for each $\boldsymbol{\zeta} = (\zeta_1, \dots, \zeta_n), \boldsymbol{\xi} = (\xi_1, \dots, \xi_n) \in V$ and i s.t. $\zeta_i \neq 0$ or $\zeta_i \neq \xi_i$, we have

1. $\big|\log(|\zeta_i|)\big| \leq 2nd^{n-1}h + 4(n+1)\log(n+2)d^n$,
2. $\big|\log(|\zeta_i - \xi_i|)\big| \leq 4nd^{2n-1}h + 4(2n+1)\log(2n+2)d^{2n}$.

Proof. To prove Item (1), we apply the arithmetic Bézout inequality together with Inequality (3) above to the zero-dimensional ideals in $n+1$ variables

$$J_1 = \big(f_1(\boldsymbol{x}), \dots, f_s(\boldsymbol{x}), x_{n+1} - p(\boldsymbol{x})\big) \quad \text{and} \quad J_2 = \big(f_1(\boldsymbol{x}), \dots, f_s(\boldsymbol{x}), 1 - x_{n+1}p(\boldsymbol{x})\big).$$

Since $V_{\mathbb{C}}(J_1) = \{(\boldsymbol{\zeta}, p(\boldsymbol{\zeta})) : \boldsymbol{\zeta} \in V\}$ and $V_{\mathbb{C}}(J_2) = \{(\boldsymbol{\zeta}, 1/p(\boldsymbol{\zeta})) : \boldsymbol{\zeta} \in V, p(\boldsymbol{\zeta}) \neq 0\}$ we deduce

$$\log(|p(\boldsymbol{\zeta})|) \leq \sum_{\boldsymbol{\zeta} \in V} \log(\|(1, \boldsymbol{\zeta}, p(\boldsymbol{\zeta}))\|_2) \leq d^n h_p + nd^{n-1}d_p h + 2(n+1)\log(n+2)d^n d_p.$$

Similarly,

$$\log\Big(\Big|\frac{1}{p(\boldsymbol{\zeta})}\Big|\Big) \le \sum_{\boldsymbol{\zeta}\in V} \log(\|(1,\boldsymbol{\zeta},\frac{1}{p(\zeta)})\|_2)$$
$$\le d^n h_p + nd^{n-1}(d_p+1)h + 2(n+1)\log(n+2)d^n(d_p+1)$$

implies that $\log(|p(\boldsymbol{\zeta})|) \ge -\big(d^n h_p + 2nd^{n-1}d_p h + 4(n+1)\log(n+2)d^n d_p\big)$.
To prove Item (2), we apply Item (1) to the zero-dimensional ideal in $2n$ variables

$$J = (f_1(\boldsymbol{x}),\dots,f_s(\boldsymbol{x}),f_1(\boldsymbol{y}),\dots,f_s(\boldsymbol{y})) \subset \mathbb{C}[\boldsymbol{x},\boldsymbol{y}]$$

and the polynomial $p(\boldsymbol{x}) - p(\boldsymbol{y})$ of degree d_p and height h_p.
We then obtain the bounds for the coordinates and the separation of the roots applying this to the polynomials $p = x_i$ and $p = x_i - y_i$ respectively, of degree 1 and height 0. □

These general lower bound for the coordinates of the roots are again essentially optimal as shows the following example presented in [Can1987]:

$$V_3 = V_{\mathbb{C}}(2^h x_1 - 1, x_2 - x_1^d, \dots, x_n - x_{n-1}^d)$$

where the unique root $\boldsymbol{\zeta} = (1/2^h,\dots,1/2^{d^{n-1}h})$ satisfies $\log(\zeta_n) = -d^{n-1}h$ while the lower bound in Proposition 4.3 gives

$$\log(\zeta_n) \ge -(2nd^{n-1}h + 4(n+1)\log(n+2)d^n).$$

They are also quite tight for the separation of the roots, according to the multivariate Mignotte-type example developed in [EMT2020, Sec.4].

Finally, applying more carefully the inequality $\sum_{\boldsymbol{\zeta}\in V} \log(\|(1,\boldsymbol{\zeta})\|_2) \le \mathrm{h}(V)$ to subsets of roots, these statements can be adapted to obtain more general estimates for sums of upper, lower and separations bounds for the roots.

5. An arithmetic Nullstellensatz

The Nullstellensatz (NSS) is a cornerstone of algebraic geometry, that first appeared in a complete form in Hilbert's work. These are its two forms, known as *weak NSS* and *strong NSS*, which are in fact equivalent:

Theorem 5.1. (The Nullstellensatz)
Let $I \subset \mathbb{C}[\boldsymbol{x}]$ be an ideal. Then,

(1) *Weak NSS:* $V_{\mathbb{C}}(I) = \emptyset \iff 1 \in I$;

(2) *Strong NSS:* $I(V_{\mathbb{C}}(I)) = \sqrt{I}$.

(Here $\sqrt{I} := \{f \in \mathbb{C}[\boldsymbol{x}] : \exists\, N \in \mathbb{N} \text{ s.t. } f^N \in I\}$) is the *radical* of the ideal I, and given a set $X \subset \mathbb{C}^n$, $I(X) := \{f \in \mathbb{C}[\boldsymbol{x}] \text{ s.t. } f(\boldsymbol{\zeta}) = 0,\ \forall\, \boldsymbol{\zeta} \in X\}$ is the *vanishing ideal* of the set X.

Both statements are quite well known in the univariate case but do not readily generalize to the multivariate case since there is no Euclidean division algorithm in $k[\boldsymbol{x}]$ for $n \ge 2$. For both statements, the $\Leftarrow$ and $\supseteq$ direction are obvious, and (2) also easily implies (1). The passage of (1) to (2) is usually done trough the famous *Rabinowicz' trick*. There are several proofs for the (weak) NSS: one particularly elementary, based

on an extension theorem and resultants, can be found in [CLO2015, Ch.4, Thm.2] for instance. Another more classical proof using *Zariski's lemma* shows an equivalent statement: Maximal ideals $\mathcal{M} \subset \mathbb{C}[\boldsymbol{x}]$ are all of the form $\mathcal{M} = (x_1 - \zeta_1, \ldots, x_n - \zeta_n)$ for some $\boldsymbol{\zeta} = (\zeta_1, \ldots, \zeta_n) \in \mathbb{C}^n$.

When the ideal $I = (f_1, \ldots, f_s)$ is generated by polynomials $f_1, \ldots, f_s \in \mathbb{Z}[\boldsymbol{x}]$, then the weak NSS reads as

> *Let $f_1, \ldots, f_s \in \mathbb{Z}[\boldsymbol{x}]$ be polynomials such that the equation system*
>
> $$f_1(\boldsymbol{x}) = 0, \ldots, f_s(\boldsymbol{x}) = 0$$
>
> *has no solution in $\mathbb{C}^n$. Then there exists $a \in \mathbb{N} \setminus \{0\}$ and $g_1, \ldots, g_s \in \mathbb{Z}[\boldsymbol{x}]$ satisfying the Bézout identity*
>
> $$a = g_1 f_1 + \cdots + g_s f_s.$$

As it is, this is a noneffective statement. Effective versions of the NSS estimate the degrees and the heights of polynomials satisfying the Bézout identity, and apply to many situations in number theory, theoretical computer science and computer algebra. I mention the following particular case of the best height estimate from [DKS2013, Cor.4.38], which "arithmeticizes" the (best) proof for degrees over varieties by Jelonek in [Jel2005, Cor.1.1], after pioneering results by Herrmann (1926), Masser and Wüstholz (1983), Brownawell (1987), Caniglia-Galligo-Heintz (1988) and Kollár (1988) for the degrees and by Berenstein-Yger (1991) for height estimates (see also [KrPa1996] and [KPS2001]).

Theorem 5.2. (An Arithmetic Nullstellensatz)
Let $f_1, \ldots, f_s \in \mathbb{Z}[\boldsymbol{x}]$ be s.t. $V_{\mathbb{C}}(f_1, , \ldots, f_s) = \emptyset$. Set $d_j := \deg(f_j)$ and $h_j := \mathrm{h}(f_j)$ for $1 \le j \le s$. Assume that $d := d_1 \ge d_2 \ge \cdots \ge d_{s-1}$ (with no condition with respect to d_s), and $h := \max\{h_1, \ldots, h_{s-1}\}$, and finally set $r := \min\{s-1, n\}$.
Then there exists $a \in \mathbb{N} \setminus \{0\}$ and $g_1, \ldots, g_s \in \mathbb{Z}[\boldsymbol{x}]$ such that for $1 \le i \le s$ one has

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

with

$$\deg(g_i f_i) \le d_1 \cdots d_r d_s$$

and

$$\begin{aligned}\mathrm{h}(a), \mathrm{h}(g_i) + \mathrm{h}(f_i) &\le \Big(\frac{h_s}{d_s} + \sum_{k=1}^{r} \frac{h}{d_k} + (6n+9)\log(n+3) + 3n \log\max\{1, s-n\}\Big) d_1 \cdots d_r d_s \\ &\le d^r h_s + r d^{r-1} d_s h + \big((6n+9)\log(n+3) + 3n\log\max\{1, s-n\}\big) d^r d_s.\end{aligned}$$

This bound is again close to optimal, as show the following examples:

(1) Brownawell-Masser-Philippon'1986: Take

$$f_1 = x_1^d,\ f_2 = x_1 x_n^{d-1} - x_2^d, \ldots,\ f_{n-1} = x_{n-2} x_n^{d-1} - x_{n-1}^d,\ f_n = 2^h - x_{n-1} x_n^{d-1}.$$

One can show that a Bézout identity

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

specialized at $\boldsymbol{\zeta} = (2^{d^{n-2}h}t^{d^{n-1}-1}, \ldots, 2^{dh}t^{d^2-1}, 2^h t^{d-1}, 1/t)$ for any $t \neq 0$ necessarily implies that $a = g_1(\boldsymbol{\zeta})2^{d^{n-1}h}t^{d_n-d}$, which implies that

$$d^n \leq \deg(g_1 f_1) \leq \max \deg(g_i f_i) \leq d^n$$
$$d^{n-1}h \leq \mathrm{h}(a) \leq \max\{\mathrm{h}(a), \mathrm{h}(g_i) + \mathrm{h}(f_i)\} \leq d^{n-1}h + c(n)d^n,$$

by specialization at $t = 0$ for the second bound. (Here the right-hand side inequalities are the ones obtained in the previous theorem.) *(2)* Take the following modification of the finite variety V_2 above:

$$f_1 = x_1 - 2^h, f_2 = x_2 - x_1^d, \ldots, f_n = x_n - x_{n-1}^d, f_{n+1} = x_n^d.$$

A Bézout identity

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

specialized at $\boldsymbol{\zeta} = (2^h, 2^{dh}, \ldots, 2^{d^{n-1}h})$ necessarily implies that $a = g_{n+1}(\boldsymbol{\zeta})2^{d^n h}$ and therefore

$$d^n h \quad \leq \quad \mathrm{h}(a) \quad \leq \max\{\mathrm{h}(a), \mathrm{h}(g_i) + \mathrm{h}(f_i)\} \quad \leq \quad d^n h + c(n)d^{n+1}.$$

The arithmetic Nullstellensatz might be useful when one wants for instance to get bounds for the polynomials in the Chinese Remainder Theorem representation of a given polynomial $f \in \mathbb{Q}[\boldsymbol{x}]/I$ in terms of its local representatives in $\mathbb{Q}[\boldsymbol{x}]/Q_k$ if $I = Q_1 \cap \cdots \cap Q_t$ is the primary decomposition of the zero-dimensional ideal I in $\mathbb{Q}[\boldsymbol{x}]$.

6. An Arithmetic Shape Lemma

In what follows $I = (f_1, \ldots, f_s) \subset \mathbb{Q}[\boldsymbol{x}]$ is a *radical* zero-dimensional ideal, i.e. $\sqrt{I} = I$, which implies that $\dim_{\mathbb{Q}} \big(\mathbb{Q}[\boldsymbol{x}]/I\big) = \deg(V)$ (see for instance [CLO2015, Ch.5, Prop.7]).

The following Arithmetic *Shape Lemma* for the radical zero-dimensional ideal I is an arithmetic version of what is also now known as (symbolic) *Geometric Resolution*, *Kronecker Parameterization* or *Rational Univariate Representation*: The classical Shape Lemma already appeared in the work of Kronecker [Kro1882], and it was reintroduced adapted to the context of Computer Algebra around 40 years ago by Chistov and Grigoriev [ChGr1982] and Canny [Can1988], and again later on by e.g. Alonso, Becker et al. [ABRW1996, Sec.2.3], Giusti, Heintz et al. [GHMP1995], and by Fabrice Rouillier [Rou1999] among others, in the form we are using here. Its meaning is that zero-dimensional radical ideals are essentially the same as univariate ideals, and working in the quotient $K[\boldsymbol{x}]/I$ under a suitable isomorphism allows to use the machinery of univariate polynomials. In particular, I will show as an application how this isomorphism allows to obtain improved height estimates for the representative of a polynomial $p \in \mathbb{Z}[\boldsymbol{x}]$ in the quotient algebra $\mathbb{Q}[\boldsymbol{x}]/I$.
The first part of the statement is now kind of classical, and the second part presents the height estimates as in [BKM2024, Lem.4.3] (just slightly more precise due to the application of Proposition 4.1). I give a complete proof since it has its own interest, and also for sake of completeness. As sometimes we know an a priori bound for the degree $\deg(V)$ of the zero-dimensional variety V that are better than the Bézout bound, I leave the height bounds in next statement in terms of this degree. I refer to [GHHMPM1997], [HMPS2000], [Sch2001, Ch.13], [SaSc2018, Prop.4], [HoLe2021] for algorithms, and previous and more general arithmetic estimates.

Theorem 6.1. (An Arithmetic Shape Lemma)
Let $f_1,\dots,f_s \in \mathbb{Z}[\boldsymbol{x}]$ define a radical *zero-dimensional ideal I, with $V = V_{\mathbb{C}}(I) \subset \mathbb{C}^n$ of degree $D := \deg(V)$. Set $d_j := \deg(f_j)$ and $h_j := \mathrm{h}(f_j)$ for $1 \le j \le s$. Assume that $d := d_1 \ge d_2 \ge \cdots \ge d_{s-1}$ (with no condition with respect to d_s), and set $h := \max\{h_1,\dots,h_{s-1}\}$. Then there exists an algebra epimorphism*

$$\begin{aligned} \varphi:\ \mathbb{Q}[\boldsymbol{x}] &\twoheadrightarrow \mathbb{Q}[t]/(\omega_0) \\ x_i &\mapsto \omega_i(t)/\omega_0'(t) \mod \omega_0 \quad \text{for } 1 \le i \le n \end{aligned}$$

where $\omega_0,\omega_1,\dots,\omega_n \in \mathbb{Z}[t]$ with ω_0 squarefree satisfy

$$\deg(\omega_0) = D, \deg(\omega_i) < D \quad \text{for} \quad 1 \le i \le n$$

and

$$\mathrm{h}(\omega_i) \le d^{n-1}h_s + (n-1)d^{n-2}d_s h + 2n\log(n+1)d^{n-1}d_s + 4D\log\big((n+1)D\big).$$

Moreover, the kernel of φ satisfies $\ker(\varphi) = I$, and therefore φ induces an algebra isomorphism

$$\overline{\varphi}:\quad \mathbb{Q}[\boldsymbol{x}]/I \quad \xrightarrow{\simeq} \quad \mathbb{Q}[t]/(\omega_0).$$

Proof. Let $L(\boldsymbol{U},\boldsymbol{x}) = U_1x_1+\cdots+U_nx_n \in \mathbb{Q}[\boldsymbol{U},\boldsymbol{x}]$ be a generic linear form, and consider the polynomial

$$\mathrm{Ch}_V(t,-\boldsymbol{U}) := \mathrm{Ch}_V(t,-U_1,\dots,-U_n) = c\prod_{\boldsymbol{\zeta}\in V}\big(t - L(\boldsymbol{U},\boldsymbol{\zeta})\big) \in \mathbb{Z}[t,\boldsymbol{U}],$$

where Ch_V is the (primitive) Chow form of V introduced in Section 4.
Given $\boldsymbol{\zeta} \in V$, $\mathrm{Ch}_V\big(L(\boldsymbol{U},\boldsymbol{\zeta}),-\boldsymbol{U}\big) = 0$ as a polynomial in $\boldsymbol{U}$ implies by the chain rule that for all i we have

$$\begin{aligned} 0 &= \partial_{U_i}\big(\mathrm{Ch}_V\big(L(\boldsymbol{U},\boldsymbol{\zeta}),-\boldsymbol{U}\big)\big)(\boldsymbol{U}) \\ &= \partial_t\big(\mathrm{Ch}_V(t,\boldsymbol{U})\big)\big(L(\boldsymbol{U},\boldsymbol{\zeta}),-\boldsymbol{U}\big)\zeta_i - \partial_{U_i}\big(\mathrm{Ch}_V(t,\boldsymbol{U})\big)(L(\boldsymbol{U},\boldsymbol{\zeta}),-\boldsymbol{U}) \end{aligned}$$

as a polynomial in $\boldsymbol{U}$ too.
Therefore, by choosing $\boldsymbol{u} = (u_1,\dots,u_n) \in \mathbb{Z}^n$ such that $\ell(\boldsymbol{x}) := L(\boldsymbol{u},\boldsymbol{x})$ satisfies $\ell(\boldsymbol{\zeta}) \ne \ell(\boldsymbol{\xi})$ for all $\boldsymbol{\zeta} \ne \boldsymbol{\xi} \in V$, i.e. ℓ is a separating linear form for V, we have that for all $\boldsymbol{\zeta} \in V$,

$$\big(\partial_t\mathrm{Ch}_V(t,-\boldsymbol{u})\zeta_i - \partial_{U_i}\mathrm{Ch}_V(t,-\boldsymbol{u})\big)\big(\ell(\boldsymbol{\zeta})\big) = \partial_t\mathrm{Ch}_V(\ell(\boldsymbol{\zeta}),-\boldsymbol{u})\zeta_i - \partial_{U_i}\mathrm{Ch}_V(\ell(\boldsymbol{\zeta}),-\boldsymbol{u}) = 0.$$

We can then define the univariate integer polynomials

$$\omega_0(t) := \mathrm{Ch}_V(t,-\boldsymbol{u}) \quad \text{and} \quad \omega_i(t) := \partial_{U_i}\mathrm{Ch}_V(t,-\boldsymbol{u}), \qquad 1 \le i \le n.$$

Since the degree D polynomial ω_0 has D distinct roots $\ell(\boldsymbol{\zeta})$, $\boldsymbol{\zeta} \in V$, it is squarefree and its derivative $\omega_0' = \partial_t\mathrm{Ch}_V(t,-\boldsymbol{u})$ is invertible modulo ω_0. Moreover, for all $\boldsymbol{\zeta} \in V$ and $1 \le i \le n$,

$$\zeta_i = \frac{\partial_{U_i}\mathrm{Ch}_V(\ell(\boldsymbol{\zeta}),-\boldsymbol{u})}{\partial_t\mathrm{Ch}_V(\ell(\boldsymbol{\zeta}),-\boldsymbol{u})} = \frac{\omega_i(\ell(\boldsymbol{\zeta}))}{\omega_0'(\ell(\boldsymbol{\zeta}))}. \tag{6}$$

This induces a morphism of algebras $\varphi : \mathbb{Q}[\boldsymbol{x}] \to \mathbb{Q}[t]/(\omega_0)$, $x_i \mapsto \omega_i(t)/\omega_0'(t) \mod \omega_0$, which is well-defined since ω_0' is invertible modulo ω_0.
Moreover φ is an epimorphism because by definition

$$\varphi(\ell(\boldsymbol{x})) = u_1\varphi(x_1)+\cdots+u_n\varphi(x_n) \equiv u_1\frac{\omega_1(t)}{\omega_0'(t)}+\cdots+u_n\frac{\omega_n(t)}{\omega_0'(t)} \equiv t \mod \omega_0$$

since by Identity (6), the two polynomials coincide in all the roots $\ell(\boldsymbol{\zeta})$ of the squarefree degree D polynomial $\omega_0 \in \mathbb{Q}[t]$:

$$u_1 \frac{\omega_1(\ell(\boldsymbol{\zeta}))}{\omega_0'(\ell(\boldsymbol{\zeta}))} + \cdots + u_n \frac{\omega_n(\ell(\boldsymbol{\zeta}))}{\omega_0'(\ell(\boldsymbol{\zeta}))} = u_1\zeta_1 + \cdots + u_n\zeta_n = \ell(\boldsymbol{\zeta}).$$

Furthermore, we show that $\ker(\varphi) = I$:

$$\begin{aligned} g \in \ker(\varphi) &\iff \varphi(g) = 0 \iff g\big(\frac{\omega_1(t)}{\omega_0'(t)}, \ldots, \frac{\omega_n(t)}{\omega_0'(t)}\big) \equiv 0 \mod \omega_0 \\ &\iff g\big(\frac{\omega_1(\ell(\boldsymbol{\zeta}))}{\omega_0'(\ell(\boldsymbol{\zeta}))}, \ldots, \frac{\omega_n(\ell(\boldsymbol{\zeta}))}{\omega_0'(\ell(\boldsymbol{\zeta}))}\big) = 0 \quad \text{for all } \boldsymbol{\zeta} \in V \quad \text{since } \omega_0 \text{ is squarefree} \\ &\iff g(\boldsymbol{\zeta}) = 0 \quad \text{for all } \boldsymbol{\zeta} \in V \quad \text{by Identity (6)} \\ &\iff g \in I \quad \text{by the NSS since } I \text{ is radical.} \end{aligned}$$

Therefore φ induces an isomorphism

$$\overline{\varphi} : \mathbb{Q}[\boldsymbol{x}]/I \xrightarrow{\simeq} \mathbb{Q}[t]/(\omega_0).$$

We now deal with the estimates:
In order to choose $\ell(\boldsymbol{x}) = u_1x_1 + \cdots + u_nx_n \in \mathbb{Z}[\boldsymbol{x}]$ that separates the points in V, we can observe that the non-zero polynomial

$$\prod_{(\boldsymbol{\zeta},\boldsymbol{\xi}) \in V \times V, \boldsymbol{\zeta} \neq \boldsymbol{\xi}} (L(\boldsymbol{U}, \boldsymbol{\zeta}) - L(\boldsymbol{U}, \boldsymbol{\xi})) \in \mathbb{C}[\boldsymbol{U}]$$

has degree $D' := D(D-1)/2 < D^2$ and therefore, there exists an element $\boldsymbol{u}$ in the grid

$$\{(k_1, \ldots, k_n) \in \mathbb{Z}^n \,:\, 0 \leq k_i < D^2\}$$

where it does not vanish.
By Inequality (4) and Theorem 4.1,

$$\begin{aligned} \mathrm{h}(\mathrm{Ch}_V) &\leq \mathrm{h}(V) + 3\log(n+1)\deg(V) \\ &\leq\ d^{n-1}h_s + (n-1)d^{n-2}d_sh + 2n\log(n+1)d^{n-1}d_s + 3D\log(n+1). \end{aligned}$$

We conclude by observing that the polynomial

$$\mathrm{Ch}_V(t, -\boldsymbol{U}) = \sum_{\alpha,i:|\alpha|+i=D} a_{\alpha,i}t^i\boldsymbol{U}^\alpha = \sum_{i=0}^{D} \big(\sum_{|\alpha|=D-i} a_{\alpha,i}\boldsymbol{U}^\alpha \big) t^i \in \mathbb{Z}[t, \boldsymbol{U}]$$

and therefore

$$\begin{aligned} \mathrm{h}(\omega_0) &= \mathrm{h}(\mathrm{Ch}_V(t, -\boldsymbol{u})) \\ &\leq \mathrm{h}(\mathrm{Ch}_V) + D\log(n+1) + D\log(D^2) \\ &\leq d^{n-1}h_s + (n-1)d^{n-2}d_sh + 2n\log(n+1)d^{n-1}d_s + 4D\log\big((n+1)D\big), \end{aligned}$$

since the number of terms is bounded by $(n+1)^D$. Similarly, for $1 \leq i \leq n$, $\partial_{U_i}\mathrm{Ch}_V(t, -\boldsymbol{U}) \in \mathbb{Z}[t, \boldsymbol{U}]$ is homogeneous of degree $D-1$, with height bounded by $\mathrm{h}(\mathrm{Ch}_V) + \log(D)$, and therefore

$$\begin{aligned} \mathrm{h}(\omega_i) &\leq \mathrm{h}(\mathrm{Ch}_V) + \log(D) + (D-1)\log(n+1) + (D-1)\log(D^2) \\ &\leq d^{n-1}h_s + (n-1)d^{n-2}d_sh + 2n\log(n+1)d^{n-1}d_s + 4D\log\big((n+1)D\big) \end{aligned}$$

as well. □

The previous result allows us for instance to get estimates for the heights of the coefficients of a representative $\overline{p} \in \mathbb{Q}[\boldsymbol{x}]/I$ of a polynomial $p \in \mathbb{Q}[\boldsymbol{x}]$, that we can call the *remainder* of p modulo I. These estimates are better than those that one would obtain by naïve methods, even in the case that the generators $f_1, \ldots, f_s \in \mathbb{Z}[\boldsymbol{x}]$ of the ideal I are a degree-preserving Gröbner basis of I. The following follows the developments of [BKM2024, Sec.4.2].

When $I \subset \mathbb{Q}[\boldsymbol{x}]$ is a zero-dimensional radical ideal, then $\dim(\mathbb{Q}[\boldsymbol{x}]/I)$ coincides with $D := \deg(V) \leq d^n$, where $d = \max_i\{\deg(f_i)\}$, and $\mathbb{Q}[\boldsymbol{x}]/I$ admits a *monomial* basis $\mathcal{B}$ with $\delta := \deg(\mathcal{B}) = \max\{\deg(b) : b \in \mathcal{B}\} \leq D$: such a basis starts with $b_1 := 1$ and then continues for $j > 1$ in an inductive process with $b_j := x_k b_i$, where $i < j$ and x_k is a variable such that $\{b_1, \ldots, b_j\}$ are still linearly independents modulo I. Since $\mathcal{B}$ has D elements, $\delta < D$ (the worst case would be for instance taking $1, x_1, \ldots, x_1^{D-1}$). Moreover, since $b = \boldsymbol{x}^\alpha$ for some $|\alpha| \leq \delta$, we have that $\mathrm{h}(b) = 0$ for every $b \in \mathcal{B}$.

Therefore, for any $p \in \mathbb{Q}[\boldsymbol{x}]$, we will get $\overline{p} = \sum_{b\in\mathcal{B}} c_b \cdot b$ with $c_b \in \mathbb{Q}$ as the representative in $\mathbb{Q}[\boldsymbol{x}]/I$ of $p \in \mathbb{Q}[\boldsymbol{x}]$. We observe that there exist of course $g_1, \ldots, g_s \in \mathbb{Q}[\boldsymbol{x}]$ such that

$$p = g_1 f_1 + \cdots + g_s f_s + \overline{p}. \tag{7}$$

In order to bound the heights of the numerators and a common denominator for the coefficients of $\overline{p}$ we define the following crucial epimorphism $\mathcal{U}$ of $\mathbb{Q}$-vector spaces, which allows us to compute the coefficients in an univariate setting:

$$\begin{array}{ccccccc} \mathcal{U} & : & \mathbb{Q}[\boldsymbol{x}] & \twoheadrightarrow & \mathbb{Q}[t]/(\omega_0) & \xrightarrow{\simeq} & \langle 1, t, \ldots, t^{D-1}\rangle_{\mathbb{Q}} \\ & & p & \mapsto & \omega_0' \varphi(p) \mod \omega_0 & \mapsto & (c_0, \ldots, c_{D-1}) \end{array},$$

where φ is defined in Theorem 6.1 and $\omega_0' \varphi(p) \equiv \sum_{i=0}^{D-1} c_i t^i \mod \omega_0$. Observe that since ω_0' is invertible modulo ω_0, $\mathcal{U}$ is a $\mathbb{Q}$-epimorphism with $\ker(\mathcal{U}) = \ker(\varphi) = I$.

Lemma 6.2. ([BKM2024, Lem.4.4])
Let $f_1, \ldots, f_s \in \mathbb{Z}[\boldsymbol{x}]$ define a radical zero-dimensional ideal I with $V = V_{\mathbb{C}}(I)$, and let $\boldsymbol{x}^\alpha$ be a monomial.
Set $d := \max\{\deg(f_j) : 1 \leq j \leq s\}$ and $h := \max\{\mathrm{h}(f_j) : 1 \leq j \leq s\}$. Then

$$\mathrm{h}(\mathcal{U}(\boldsymbol{x}^\alpha)) \leq n d^{n-1}|\alpha| h + 4n \log((n+2)d) d^n |\alpha|.$$

Proof. Let $J := \left(f_1, \ldots, f_s, x_{n+1} - \boldsymbol{x}^\alpha\right) \subset \mathbb{Z}[\boldsymbol{x}, x_{n+1}]$, which is a radical zero-dimensional ideal of degree $\deg(V) \leq d^n$, since $V_{\mathbb{C}}(J) = \{(\boldsymbol{\zeta}, \boldsymbol{\zeta}^\alpha) : \boldsymbol{\zeta} \in V\}$ as already seen before. Note that if $\ell(\boldsymbol{x}) = u_1 x_1 + \cdots + u_n x_n \in \mathbb{Z}[\boldsymbol{x}]$ is a separating linear form for V, it is still a separating linear form for $V_{\mathbb{C}}(J)$. Therefore in the construction of $\varphi_J : \mathbb{Q}[\boldsymbol{x}, x_{n+1}] \to \mathbb{Q}[t]/(\omega_0^J)$ for the ideal J in Theorem 6.1, we can choose this linear form $\ell(\boldsymbol{x})$, which also applies for $\varphi_I : \mathbb{Q}[\boldsymbol{x}] \to \mathbb{Q}[t]/(\omega_0^I)$. We observe that since $u_{n+1} = 0$ in the choice of the linear form, we have that $\omega_i^J = \omega_i^I$ for $0 \leq i \leq n$, which implies that $\varphi_J(x_i) = \varphi_I(x_i)$ for $1 \leq i \leq n$. Let $\omega_{n+1} := \omega_{n+1}^J(t) \in \mathbb{Z}[t]$ be such that $\varphi_J(x_{n+1}) = (\omega_0')^{-1}\omega_{n+1}$. Then, since $x_{n+1} \equiv \boldsymbol{x}^\alpha \mod J$, we have

$$\mathcal{U}(\boldsymbol{x}^\alpha) = \omega_0' \varphi_I(\boldsymbol{x}^\alpha) = \omega_0' \varphi_J(\boldsymbol{x}^\alpha) = \omega_0' \varphi_J(x_{n+1}) = \omega_{n+1}.$$

Therefore, applying Theorem 6.1 to $J \subset \mathbb{Q}[\boldsymbol{x}, x_{n+1}]$ with $\deg(J) = \deg(I) \leq d^n$ and $f_{s+1} = x_{n+1} - \boldsymbol{x}^\alpha$) of degree $|\alpha|$ and height 0, we get

$$\begin{aligned} \mathrm{h}(\mathcal{U}(\boldsymbol{x}^\alpha)) = \mathrm{h}(\omega_{n+1}) &\leq n d^{n-1}|\alpha| h + 2(n+1)\log(n+2) d^n |\alpha| + 4n d^n \log((n+1)d) \\ &\leq n d^{n-1}|\alpha| h + 4n \log((n+2)d) d^n |\alpha|. \end{aligned}$$

□

Corollary 6.3. ([BKM2024, Cor.4.5])
Let $f_1,\dots,f_s\in\mathbb{Z}[\boldsymbol{x}]$ define a radical zero-dimensional ideal I and let $p\in\mathbb{Z}[\boldsymbol{x}]$.
Set $d:=\max\{\deg(f_j):1\le j\le s\}$, $d_p:=\deg(p)$, and $h:=\max\{\mathrm{h}(f_j):1\le j\le s\}$, $h_p:=\mathrm{h}(p)$. Then

$$\mathrm{h}(\mathcal{U}(p))\le h_p+nd^{n-1}d_ph+5n\log((n+2)d)d^nd_p.$$

Proof. This is as the proof of Corollary 4.2: Write $p=\sum_\alpha p_\alpha\boldsymbol{x}^\alpha$ with $p_\alpha\in\mathbb{Z}$. Then

$$\mathcal{U}(p)=\sum_\alpha p_\alpha\mathcal{U}(\boldsymbol{x}^\alpha)\quad\text{ with }\quad\mathrm{h}(\mathcal{U}(\boldsymbol{x}^\alpha))\le nd^{n-1}d_ph+4n\log((n+2)d)d^nd_p.$$

Since p has at most $(d_p+1)^n$ monomials, we have

$$\begin{aligned}\mathrm{h}(\mathcal{U}(p))&\le h_p+nd^{n-1}d_ph+4n\log((n+2)d)d^nd_p+n\log(d_p+1)\\&\le h_p+nd^{n-1}d_ph+5n\log((n+2)d)d^nd_p.\end{aligned}$$

□

We are now ready to prove a height bound as presented in [BKM2024, Prop.4.6] for the numerator and a common denominator of the remainder $\overline{p}$ of an integer polynomial $p\in\mathbb{Z}[\boldsymbol{x}]$ modulo I (except that here we do not need to assume that $\delta=\deg(B)\le d$ and $\deg(p)\ge d$).

Proposition 6.4. (Height of the remainder modulo I)
Let $f_1,\dots,f_s\in\mathbb{Z}[\boldsymbol{x}]$ define a radical zero-dimensional ideal I and let $p\in\mathbb{Z}[\boldsymbol{x}]$.
Set $d:=\max\{\deg(f_j):1\le j\le s\}$, $d_p:=\deg(p)$, and $h:=\max\{\mathrm{h}(f_j):1\le j\le s\}$, $h_p:=\mathrm{h}(p)$. Then there exists $a\in\mathbb{N}\setminus\{0\}$ and $N(p)\in\mathbb{Z}[\boldsymbol{x}]$ such that $\overline{p}=N(p)/a$ with

$$\begin{aligned}&\mathrm{h}(a)\le nd^{2n-1}\delta h+5n\log((n+2)d)d^{2n}\delta,\\&\mathrm{h}(N(p))\le h_p+nd^{n-1}(d_p+d^n\delta)h+5n\log((n+2)d)d^n(d_p+d^n\delta).\end{aligned}$$

Proof. If $\overline{p}=\sum_{b\in\mathcal{B}}c_b\,b$ with $c_b\in\mathbb{Q}$, we have that

$$\mathcal{U}(p)=\mathcal{U}(\overline{p})=\sum_{b\in\mathcal{B}}c_b\,\mathcal{U}(b)$$

since $p\equiv\overline{p}\mod I$. Therefore $(c_b:b\in\mathcal{B})$ is the (unique) solution y of a square linear system of equations

$$A\,y=c$$

of size D, where the matrix $A\in\mathbb{Z}^{D\times D}$ to invert is composed by the coefficients of $\mathcal{U}(b)$, $b\in\mathcal{B}$, and the constant vector c is composed by the integer coefficients of $\mathcal{U}(p)$ in the basis $(1,t,\dots,t^{D-1})$. Solving this system of equations by Cramer's rule gives the common denominator $a=\det(A)$ and the coordinates of the numerator $N(p)\in\mathbb{Z}[\boldsymbol{x}]$ where each column of A is replaced by the constant vector.
By Hadamard's bound, the determinant of a matrix with columns $v_1,\dots,v_D\in\mathbb{Z}^D$ where all but one column has height bounded by h_A and one column has height bounded by h_c satisfies

$$\mathrm{h}(\det(v_1,\dots,v_D))\le h_c+(D-1)h_A+\frac{D\log(D)}{2}.$$

Since

$$h_A\le nd^{n-1}\delta h+4n\log((n+2)d)d^n\delta\quad\text{and}\quad h_c\le h_p+nd^{n-1}d_ph+5n\log((n+2)d)d^nd_p$$

we conclude that

$$\begin{aligned}\mathrm{h}(a) &\leq D\big(nd^{n-1}\delta h + 4n\log((n+2)d)d^n\delta\big) + \frac{D\log(D)}{2}\\ &\leq nd^{2n-1}\delta h + 5n\log((n+2)d)d^{2n}\delta\end{aligned}$$

and

$$\begin{aligned}\mathrm{h}(N(p)) &\leq h_p + nd^{n-1}d_p h + 5n\log((n+2)d)d^n d_p\\ &\quad + (D-1)\big(nd^{n-1}\delta h + 4n\log((n+2)d)d^n\delta\big) + \frac{D\log(D)}{2}\\ &\leq h_p + nd^{n-1}(d_p + d^n\delta)h + 5n\log((n+2)d)d^n(d_p + d^n\delta).\end{aligned}$$

□

We close this section by observing the the same bound for $\mathrm{h}(\overline{p})$ holds for the maximum of the absolute values of the logarithm of all non-zero coefficients of the polynomial $\overline{p}$ when $p \in \mathbb{C}[\boldsymbol{x}]$. This is because the common denominator a satisfies $|a| \geq 1$.

Corollary 6.5. *Let $p \in \mathbb{C}[\boldsymbol{x}]$ be a polynomial of degree d_p and set h_p for the maximum of the absolute value of the logarithm of all non-zero coefficients of p.*
Set $\overline{p} = \sum_{b\in B} c_b\, b \in \mathbb{C}[\boldsymbol{x}]$. Then

$$\max\{\log(|c_b|) : b \in B\} \leq h_p + nd^{n-1}(d_p + d^n\delta)h + 5n\log((n+2)d)d^n(d_p + d^n\delta).$$

7. An Arithmetic Perron's Theorem

In [Jel2005] the proof of the effective Nullstellensatz relies on bounding the degrees of a coefficient in a given algebraic equation for polynomials related to the polynomials $f_1, \ldots, f_s$, which define the empty variety. I present here a sketch of an algebraic version of his proof for the case $s = n+1$, which is the typical case (the same holds for $s < n+1$ and for $s > n+1$ one usually performs some linear combinations of $f_1, \ldots, f_s$ to restrict to $n+1$ polynomials).
Assume that $f_1, \ldots, f_{n+1} \in \mathbb{C}[\boldsymbol{x}]$ satisfy that $V_{\mathbb{C}}(f_1, \ldots, f_s) = \emptyset$, so that by the NSS there exist (unknown) $g_1, \ldots, g_{n+1}$ with

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

and consider the following algebra morphism

$$\Phi :\ \mathbb{C}[\boldsymbol{x}, z_1, \ldots, z_{n+1}] \ \to\ \mathbb{C}[\boldsymbol{x}, z],\ x_i \ \mapsto\ x_i,\ z_j \ \mapsto z f_j(\boldsymbol{x}) \quad \text{for } 1 \leq i \leq n, 1 \leq j \leq n+1.$$

The map Φ turns out to be an epimorphism because $\Phi(g_1(\boldsymbol{x})z_1 + \cdots + g_{n+1}(\boldsymbol{x})z_{n+1}) = z$. Therefore, Φ induces an algebra isomorphism

$$\overline{\Phi} :\ A := \mathbb{C}[\boldsymbol{x}, z_1, \ldots, z_{n+1}]/\ker(\Phi)\ \simeq\ \mathbb{C}[\boldsymbol{x}, z],$$

between the finitely generated algebra A over $\mathbb{C}$ and the polynomial ring $\mathbb{C}[\boldsymbol{x}, z]$, and in particular the (Krull) dimension of A equals $n+1$.

By Noether's normalization lemma (see for instance [AtMa1969, Ch.5, Ex.16]) there exist $n+1$ linear combinations of the variables $\boldsymbol{x}, z_1, \ldots, z_{n+1}$ in A, that can moreover be taken of the form $z_1 + \ell_1(\boldsymbol{x}), \ldots, z_{n+1} + \ell_{n+1}(\boldsymbol{x})$ (where $\ell_1, \ldots, \ell_{n+1}$ are linear forms in the variables $\boldsymbol{x}$) that are algebraically independent over $\mathbb{C}$ and such that A is integral over $\mathbb{C}[z_1 + \ell_1(\boldsymbol{x}), \ldots, z_{n+1} + \ell_{n+1}(\boldsymbol{x})]$.

In particular, $g_1(\boldsymbol{x})z_1+\cdots+g_{n+1}(\boldsymbol{x})z_{n+1}$ is integral over $\mathbb{C}[z_1+\ell_1(\boldsymbol{x}),\ldots,z_{n+1}+\ell_{n+1}(\boldsymbol{x})]$: Setting $\boldsymbol{y}:=(y_1,\ldots,y_{n+1})$, there exists a polynomial of some degree D (nothing to do with the previous D),

$$P(\boldsymbol{y},t)=t^D+\sum_{j=1}^{D}\sum_{\alpha}a_{\alpha,j}\boldsymbol{y}^{\alpha}t^{D-j}\quad\in\mathbb{C}[\boldsymbol{y},t]\setminus\{0\},$$

monic in t, such that

$$P\big(z_1+\ell_1(\boldsymbol{x}),\ldots,z_{n+1}+\ell_{n+1}(\boldsymbol{x}),g_1(\boldsymbol{x})z_1+\cdots+g_{n+1}(\boldsymbol{x})z_{n+1}\big)\;\equiv\;0\mod\ker(\Phi).$$

Therefore

$$\begin{aligned}0&=\Phi\big(P\big(z_1+\ell_1(\boldsymbol{x}),\ldots,z_{n+1}+\ell_{n+1}(\boldsymbol{x}),g_1(\boldsymbol{x})z_1+\cdots+g_{n+1}(\boldsymbol{x})z_{n+1}\big)\big)\\&=P\big(\Phi\big(z_1+\ell_1(\boldsymbol{x})\big),\ldots,\Phi\big(z_{n+1}+\ell_{n+1}(\boldsymbol{x})\big),\Phi\big(g_1(\boldsymbol{x})z_1+\cdots+g_{n+1}(\boldsymbol{x})z_{n+1}\big)\big)\\&=P\big(zf_1(\boldsymbol{x})+\ell_1(\boldsymbol{x}),\ldots,zf_{n+1}(\boldsymbol{x})+\ell_{n+1}(\boldsymbol{x}),z\big)\\&=z^D+\sum_{j=1}^{D}\sum_{\alpha}a_{\alpha,j}\big(zf_1(\boldsymbol{x})+\ell_1(\boldsymbol{x})\big)^{\alpha_1}\cdots\big(zf_{n+1}(\boldsymbol{x})+\ell_{n+1}(\boldsymbol{x})\big)^{\alpha_{n+1}}z^{D-j}.\end{aligned}$$

By inspection, the coefficient of z^D when expanding this expression gives an effective Bézout identity for $f_1,\ldots,f_s$.

Finding the degrees in this integral dependence equation for z is strongly related to the problem of finding an algebraic dependence equation for polynomials that are not algebraically independent. This is what is sometimes called *Perron's theorem*, since the very popular book by Perron [Per1927] gives in Satz 57 a combinatorial proof that if $f_1,\ldots,f_{n+1}\in\mathbb{C}[\boldsymbol{x}]$ are $n+1$ polynomials in n variables of degrees $d_j:=\deg(f_j)$, then there are algebraically dependent, i.e. there exists a polynomial

$$P=\sum_{\alpha}c_{\alpha}y_1^{\alpha_1}\cdots y_{n+1}^{\alpha_n}\quad\in\mathbb{C}[y_1,\ldots,y_{n+1}]\setminus\{0\}$$

which satisfies that

- $P(f_1,\ldots,f_{n+1})=0$,
- $\alpha_1d_1+\cdots+\alpha_{n+1}d_{n+1}\le d_1\cdots d_{n+1}$ for all α.

In [DKS2013, Cor.3.23] we got the following arithmetic version of Perron's theorem as a consequence of a more general version over a variety. A parameterized version of it is a crucial tool to obtain the bounds of Theorem 5.2.

Theorem 7.1. (An arithmetic Perron's theorem)
Let $f_1,\ldots,f_{n+1}\in\mathbb{Z}[\boldsymbol{x}]$, and set $d_j:=\deg(f_j)$ and $h_j:=\mathrm{h}(f_j)$ for $1\le j\le n+1$. Then there exists a polynomial

$$P=\sum_{\alpha}c_{\alpha}y_1^{\alpha_1}\ldots y_{n+1}^{\alpha_{n+1}}\quad\in\mathbb{Z}[y_1,\ldots,y_{n+1}]\setminus\{0\}$$

which satisfies that

- $P(f_1,\ldots,f_{n+1})=0$,
- $\alpha_1d_1+\cdots+\alpha_{n+1}d_{n+1}\le d_1\cdots d_{n+1}$ *for all* α,
- $\mathrm{h}(c_\alpha)+\sum_{i=1}^{n+1}\alpha_ih_i\le\Big(\sum_{i=1}^{n+1}\frac{h_i}{d_i}+(n+2)\log(2n+8)\Big)d_1\cdots d_{n+1}$ *for all* α *s.t.* $c_\alpha\neq0$.

References

[ABRW1996] M.E. Alonso, W. Becker, M.-F. Roy, T. Wörmann, *Zeros, multiplicities and idempotents for zero-dimensional systems,* in L. Gonzalez Vega, T. Recio, eds., Algorithms in Algebraic Geometry and Applications, Proc. MEGA 94, Progress in Mathematics, Birkhäuser, **143** (1996) 1-25.

[AtMa1969] M.F. Atiyah, I.G. Macdonald, *Introduction to Commutative Algebra,* Addison-Wesley (1969).

[BKM2024] L. Baldi, T. Krick, B. Mourrain, *An Effective Positivstellensatz over the Rational Numbers for Finite Semialgebraic Sets,* Preprint (2024) https://arxiv.org/abs/2410.04845

[CGH1989] L. Caniglia, A. Galligo, J. Heintz, *Some new effectivity bounds in computational geometry,* in T. Mora, ed., Proc. AAECC-6, Lect. Notes in Comput. Sci. **357**, Springer–Verlag, (1989) 131-151.

[CGH1989] L. Caniglia, A. Galligo, J. Heintz, *Some new effectivity bounds in computational geometry,* in T. Mora, ed., Proc. AAECC-6, LNCS **357**, Springer–Verlag, (1989) 131-151.

[Can1987] J. Canny, *The Complexity of Robot Motion Planning,* ACM Doctoral Dissertation Award Series. MIT Press (1987).

[Can1988] J. Canny, *Some algebraic and geometric problems in PSPACE,* in Proceedings 20 ACM STOC (1988) 460-467.

[ChGr1982] A. Chistov, D. Grigoriev, *Polynomial-time factoring of multi-variable polynomials over a global field,* LOMI preprint, E-5-82, Steklov Institute, Leningrad, (1982).

[CLO2015] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms,* 4th ed., Undergraduate texts in Mathematics, Springer (2015).

[DKS2013] C. D'Andrea, T. Krick, M. Sombra, *Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze,* Ann. Scient. Éc. Norm. Sup. **46** (2013) 549-627.

[EMT2020] I. Emiris, B. Mourain, E. Tsigaridas, *Separation bounds for polynomial systems,* J. Symb. Comp. **101** (2020) 128-151.

[GHHMPM1997] M. Giusti, J. Heintz, K. Hägele, J. Morais, L. Pardo, J. Montaña, *Lower bounds for diophantine approximations,* J. Pure Appl. Alg. **117 & 118** (1997) 277-317.

[GHMP1995] M. Giusti, J. Heintz, J. Morais, L. Pardo, *When polynomial equation systems can be "solved" fast?,* in G. Cohen, M. Giusti, T. Mora, ed., Proc. AAECC-11, LNCS **958**, Springer (1995) 205-231.

[GLS2001] M. Giusti, G. Lecerf, B. Salvy, *A Gröbner Free Alternative for Polynomial System Solving,* J. Compl. **17** (2001) 154-211.

[HMPS2000] K. Hägele, J. Morais, L. Pardo, M. Sombra, *On the intrinsic complexity of the arithmetic Nullstellensatz,* J. Pure Appl. Alg. **146** (2000) 103-183

[Hei1983] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields,* Theoret. Comput. Sci. **24** (1983) 239-277.

[HoLe2021] J. van der Hoeven, G. Lecerf, *On the Complexity Exponent of Polynomial System Solving,* Found. Comput. Math. **21** (2021) 1-51.

[Jel2005] Z. Jelonek, *On the effective Nullstellensatz,* Invent. Math. **162** (2005) 1-17.

[KrPa1996] T. Krick, L. Pardo, *A computational method for diophantine approximation,* in L. Gonzalez Vega, T. Recio, eds., Algorithms in Algebraic Geometry and Applications, Proc. MEGA 94, Progr. Math., Birkhäuser, **143** (1996) 193-253.

[KPS2001] T. Krick, L. M. Pardo, M. Sombra, *Sharp estimates for the arithmetic Nullstellensatz,* Duke Math. J. **109** (2001) 521-598.

[Kro1882] L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen,* J. Reine Angew. Math. **92** (1882), 1-122.

[MaWh1983] D. Masser, G. Wüstholz, *Fields of large trascendence degree generated by values of elliptic functions,* Invent. Math. **72** (1983) 407-464.

[Mig1992] M. Mignotte, *Mathematics for Computer Algebra,* Springer-Verlag (1992).

[Per1927] O. Perron, *Algebra I (Die Grundlagen*), de Gruyter, 1927.

[Phi1995] P. Philippon, *Sur des hauteurs alternatives. III,* J. Math. Pures Appl. **74** (1995) 345-365.

[Rou1999] F. Rouillier, *Solving zero-dimensional systems through the rational univariate reprensentation,* AAECC **9**, 5 (1999) 433-461.

[SaSc2018] M. Safey El Din, E. Schost, *Bit complexity for multi-homogeneous polynomial system solving – Application to polynomial minimization,* J. Symb. Comp. **87** (2018) 176-206.

[Sch2001] E. Schost, *Sur la résolution des systèmes polynomiaux à paramètres,* Thèse de Doctorat, Palaiseau, École Polytechnique (2000).

[Sha1974] I. Shafarevich, *Basic algebraic geometry,* Springer-Verlag (1974).
[Yap2000] C.K. Yap, *Fundamental Problems of Algorithmic Algebra,* Oxford University Press, New York (2000).