Kronecker's and Newton's approaches to solving : A first comparison[1]

D. Castro[2], K. Hägele[3], J. E. Morais[4], L. M. Pardo[2]

September 29, 1999

Abstract

In these pages we make a first attempt to compute efficiency of symbolic and numerical analysis procedures that solve systems of multivariate polynomial equations. In particular, we compare Kronecker's solution (from the symbolic approach) with approximate zero theory (introduced by M. Shub & S. Smale as a foundation of numerical analysis). To this purpose we show upper and lower bounds of the bit length of approximate zeros. We also introduce efficient procedures that transform local Kronecker's solution into approximate zeros and conversely. As an application of our study we exhibit an efficient procedure to compute splitting fields and Lagrange resolvent of univariate polynomial equations. We remark that this procedure is obtained by a convenient combination of both approaches (numeric and symbolic) to multivariate polynomial solving.

Keywords. Kronecker's solution, Newton operator, approximate zero, straight–line programs, height of Diophantine varieties, degree of algebraic varieties, Turing machine complexity.

[1]: Research was partially supported by the Spanish grant : PB96–0671–C02–02.

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

[3]: Department of Computer Science, Trinity College, University of Dublin, Ireland

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

Contents

1 Introduction and statement of main results

Let K be a number field containing the field of Gaussian rationals $\mathbb{Q}[i] \subseteq K$. In these pages we are mainly interested in the computation of $K-$rational points of zero–dimensional algebraic varieties given by systems of multivariate polynomial equations. Namely, let $f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_n]$ be a sequence of multivariate polynomials with integer coefficients. Let $V(f_1, \ldots, f_s) \subseteq \mathbb{C}^n$ be the complex algebraic variety of their common zeros, i.e.

$$V(f_1, \ldots, f_s) := \{x \in \mathbb{C}^n \ : \ f_i(x) = 0, \ 1 \le i \le s\}.$$

For sake of simplicity, let us assume that $V(f_1, \ldots, f_s)$ is a finite set (i.e. a zero–dimensional algebraic variety). The set of $K-$rational points in $V(f_1, \ldots, f_s)$ is the set of common zeros of the system $f_1, \ldots, f_s$ whose coordinates lie in K^n, namely

$$V_K(f_1, \ldots, f_s) := \{x \in K^n \ : \ f_1(x) = \cdots = f_s(x) = 0\}.$$

The goal of these pages will be to discuss several aspects of procedures performing the following task : Assume that the field K is fixed. Given the sequence $f_1, \ldots, f_s$, compute all $K-$rational points in $V_K(f_1, \ldots, f_s)$ (or eventually all $K-$rational points in $V_K(f_1, \ldots, f_s)$ of bounded height). Note that the assumption on the field K is not very restrictive : For every zero $\zeta \in V(f_1, \ldots, f_s)$, there exists a minimal number field $K(\zeta)$ containing all the coordinates of ζ. The degree of the field extension $K(\zeta)$ over $\mathbb{Q}$ can also be denoted by $\deg(\zeta)$. In the sequel, the degree $[K : \mathbb{Q}]$ may be replaced by $\deg(\zeta)$, and the results will equally hold.
For our study, we consider a precomputation task which prepares the input $F := (f_1, \ldots, f_s)$, before we study the desired $K-$rational points. Procedures performing this precomputation task are usually called *multivariate polynomial system solvers* applied to the input F. The output of such polynomial system solvers is called the *solution* of the system F. Observe that all usual notions of solution of F will yield a description of the variety $V(f_1, \ldots, f_s)$ (cf. also [CGH$^+$99]).
Here, we consider two (conceptually different) notions which define what a *solution of the system* F should be : coming from different fields, the notions are related to a symbolic/geometric and a numerical analysis/diophantine approximation context : *Kronecker's geometric solution* and *Newton's approximate zero solution.*
Thus, our study includes a comparative study of both approaches with regard to the basic problem described above. It must be said that our study is not intended to be either complete or definitive. It just tries to point out some similarities and differences between both approaches to solving that yield some statements and some open questions of interest. In this sense, we have tried to write down as many comments as possible to clarify (as much as we can) the relations between both approaches to solving.
Moreover, we have tried to put both approaches under the same hypotheses. This means that our input system of multivariate polynomials $F := (f_1, \ldots, f_s)$ is well–suited for the application of either Kronecker's or Newton's approach to solving. Therefore we will assume the following hypotheses :

i) The number of equations equals the number of variables (i.e. $s = n$ above)

ii) The variety $V(f_1, \ldots, f_n)$ is zero–dimensional and contains exactly D points, i.e. the degree of $V(f_1, \ldots, f_n)$ (in the sense of [Hei83]) is exactly D.

iii) The $K-$rational points in $V_K(f_1, \ldots, f_n)$ are smooth with respect to the system $F := (f_1, \ldots, f_n)$, i.e. for every $\zeta \in V_K(f_1, \ldots, f_n)$, the Jacobian matrix

$$DF(\zeta) := \left(\frac{\partial f_i}{\partial X_j}(\zeta) \right)_{1 \le i,j \le n}$$

is a non–singular matrix (i.e. $DF(\zeta) \in GL(n, K)$).

iv) The sequence $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, f_n]$ is a reduced regular sequence, i.e. for every i, $1 \leq i \leq n-1$, the ideals $(f_1, \ldots, f_i)$ are radical ideals of codimension i in $\mathbb{Q}[X_1, \ldots, X_n]$.

v) The degrees of the input polynomials satisfy $\deg(f_i) \leq 2$, for $1 \leq i \leq n$.

It must be said that constrains *i)* and *iv)* are not relevant for Kronecker's approach to solving. Applying the iterative version of Bertini's Theorem (as described in [Mor97, Häg98, HMPS00] or [GS99]) we can easily reduce the over–determined input system to a system satisfying properties *i)* and *iv)*. Anyway, we prefer to keep these hypotheses to simplify exposition, notations, and – hopefully – reading.
The rest of the introduction presents the new results, classified into three main categories :

i) Newton's approach to solving.

Here, we show how to extend the approximate zero theory introduced by S. Smale in [Sma81] (cf. also [Sma85, Sma86a, Sma86b]), and deeply developed in collaboration with M. Shub in the series of papers [SS85, SS86, SS93a, SS93b, SS93c, SS94a, SS94b], to a diophantine approximation context.

ii) Kronecker's approach to solving.

This recalls Kronecker's approach to solving and shows the main statements which relate both approaches by means of an algorithm based on the L^3 (or LLL) reduction procedure (as introduced in [LLL82b] and used in [KLL84, Len84]).

iii) Application: Computation of splitting field and Lagrange resolvent.

Finally we exhibit an algorithm that combines both approaches to compute efficiently the splitting field of a univariate polynomial equation and also the corresponding Lagrange resolvent.

1.1 Newton's approach to solving

Let M_K be a proper class of absolute values on the number field K in the sense of [Lan83]. For every $\nu \in M_K$ we have an absolute value $|\cdot|_\nu \ : K \longrightarrow \mathbb{R}$. The class M_K is chosen such that it satisfies Weil's product formula with respect to well-defined multiplicities. We denote by $S \subseteq M_K$ the set of sub–indices $\nu \in M_K$ such that the absolute value $|\cdot|_\nu$ is archimedean and, consequently, by $M_K \setminus S$ the class of sub–indices $\nu \in M_K$ such that $|\cdot|_\nu$ is non–archimedean. For every $\nu \in M_K$, we shall denote by K_ν the completion of K with respect to the absolute value $|\cdot|_\nu$. We also denote by $|\cdot|_\nu \ : K_\nu \longrightarrow \mathbb{R}$ the corresponding extension of $|\cdot|_\nu$ to the completion K_ν.
Let $\zeta \in V_K(f_1, \ldots, f_n)$ be a smooth $K-$rational point of the zero–dimensional complex algebraic variety $V(f_1, \ldots, f_n)$. We are interested in approximating ζ using iterations of the Newton operator. Therefore, we introduce the Newton operator of system F as the following list of rational mappings :

$$N_F(X_1, \ldots, X_n) := \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} - Df(X_1, \ldots, X_n)^{-1} \begin{pmatrix} f_1(X_1, \ldots, X_n) \\ \vdots \\ f_n(X_1, \ldots, X_n) \end{pmatrix}.$$

An *approximate zero* z in K^n for the system F with associate zero $\zeta \in V_K(f_1, \ldots, f_n)$ with respect to the absolute value $|\cdot|_\nu$ is a point such that the sequence of iterates of the Newton operator is well–defined and converges quadratically to ζ. Roughly speaking, an approximate zero $z \in K^n$ with associate zero $\zeta \in K^n$ is a point which lies in the basin of attraction of the actual zero ζ with respect to the Newton operator N_F. Formally, we define approximate zeros as follows :

Definition 1 *Let $F := (f_1, \ldots, f_n)$ be a system of multivariate polynomials with integer coefficients : $f_i \in \mathbb{Z}[X_1, \ldots, X_n]$ for $1 \leq i \leq n$. Let $\nu \in M_K$ define an absolute value $|\cdot|_\nu \ : K \longrightarrow \mathbb{R}$. Let $\zeta \in V_K(f_1, \ldots, f_n)$ be a smooth $K-$rational point (i.e. $DF(\zeta) \in GL(n, K)$). Let $z := (z_1, \ldots, z_n) \in K^n$ be an affine point. We say that z is an approximate zero of the system F with associate zero $\zeta \in K^n$ with respect to the absolute value $|\cdot|_\nu$, if the following properties hold :*

- *$DF(z) \in GL(n, K)$ is a non–singular matrix.*
- *The following sequence is well–defined :*

$$z_1 := N_F(z) \in K^n, \text{ and } z_k := N_F(z_{k-1}) \text{ for } k \geq 2.$$

- *For every $k \in \mathbb{N}$, $k \geq 1$, the following inequality holds :*

$$\|z_k - \zeta\|_\nu \leq \frac{1}{2^{2^{k-1}}} \|z - \zeta\|_\nu,$$

where $\|\cdot\|_\nu \ : K_\nu \longrightarrow \mathbb{R}$ is the corresponding norm associated to the absolute value $|\cdot|_\nu$ (cf. Subsection 2.1.4 below for more details).

From a computational point of view, we want to compute approximate zeros of smooth $K-$rational points and we want to write them over a finite alphabet. In particular for every smooth $K-$rational zero $\zeta \in V_K(f_1, \ldots, f_n)$ and every absolute value $\nu \in M_K$, we consider a subfield L of K, such that the completion L_ν of L with respect to the absolute value $|\cdot|_\nu$ contains the entries of ζ, namely $\zeta \in L_\nu^n$. Thus, we look for approximate zeros $z \in L^n$ with associate zero $\zeta \in L_\nu^n$. Let us observe that if the absolute value $|\cdot|_\nu$ is archimedean, we may fix L to be $L := \mathbb{Q}[i]$. Moreover, we are interested in the heights of approximate zeros $z \in L^n$ with actual zeros $\zeta \in L_\nu^n$. In the case where $L = \mathbb{Q}[i]$, the height of a point $z \in \mathbb{Q}[i]^n$ essentially equals its bit length (i.e. the number of tape cells in a Turing machine required to write down the list of digits describing z). In the sequel, we shall therefore identify the logarithmic height $ht(z)$ and its bit length.

A first relevant task consists in stating conditions which are sufficient for verifying the property of being an approximate zero. This is achieved by means of a local condition based on a quantity (called γ), which is essentially yielded by the Lipschitz constant appearing in the inverse mapping Theorem (cf. [Dem89], Ch. 1, for instance). These ideas were introduced by S. Smale in the early eighties (cf. [Sma81]) and deeply developed in the series of papers written by M. Shub and S. Smale [SS85] to [SS94b]) (more detailed references are given in Section 3.2 below).

With the same notations as above, let $\nu \in M_K$ be an absolute value on the field K. We define the *quantity* γ :

$$\gamma_\nu(F, \zeta) := \sup_{k \geq 2} \left\| \frac{(DF(\zeta))^{-1}(D^{(k)}F(\zeta))}{k!} \right\|_\nu^{\frac{1}{k-1}},$$

where the norm is considered as the norm with respect to the absolute value $|\cdot|_\nu$ of the multilinear operator

$$DF(\zeta)^{-1}D^{(k)}F(\zeta) \ : (K_\nu^n)^k \longrightarrow K_\nu^n.$$

This quantity yields a locally sufficient condition for having an approximate zero. This statement is known as the $\gamma-$Theorem and it holds equally true for archimedean and non–archimedean absolute values.

Theorem 2 ($\gamma-$Theorem) *With the same notations and assumptions as before, let $F := (f_1, \ldots, f_n)$ be a sequence of multivariate polynomials with coefficients in K. Let $\zeta \in V_K(f_1, \ldots, f_n)$ be a smooth $K-$rational zero (i.e. $DF(\zeta) \in GL(n, K)$ is a non-singular matrix). Let $|\cdot|_\nu \ : K \longrightarrow \mathbb{R}_+$ be an absolute value on K. For every $z \in K^n$ satisfying the inequality :*

$$\|\zeta - z\|_\nu \gamma_\nu(F, \zeta) \leq \frac{3 - \sqrt{7}}{2}$$

holds : z is an approximate zero of the system F with associate zero ζ with respect to the absolute value $|\cdot|_\nu$.

The proof of this statement follows step by step the proof of the usual $\gamma-$Theorems (cf. the compiled version in [BCSS98b]).
To establish upper and lower bounds for the bit length of approximate zeros, we have established several technical statements. One of them is an extension of the well–known Eckardt & Young Theorem [EY36] to the non–archimedean case :
Let $\nu \in M_K$ be an absolute value over K and K_ν the completion of K with respect to the absolute value $|\cdot|_\nu$. Let us denote by $\Sigma_\nu \subseteq \mathcal{M}_n(K_\nu)$ the variety of singular $n \times n$ matrices with entries in K_ν. Similarly, let Σ be the subset of Σ_ν of all singular $n \times n$ matrices with entries in K. Finally, let

$$d_\nu^{(F)} \ : \mathcal{M}_n(K_\nu) \times \mathcal{M}_n(K_\nu) \longrightarrow \mathbb{R}_+$$

be the Frobenius (also called Hilbert–Weil) metric on $\mathcal{M}_n(K_\nu)$ with respect to the absolute value $|\cdot|_\nu$ (cf. Subsection 3.1 below). Then, the following Theorem holds :

Theorem 3 (Eckardt & Young) *Let $\nu \in M_K$ be an absolute value. For every non–singular $n \times n$ matrix $A \in GL(n, K)$, the following equality holds :*

$$d_\nu^{(F)}(A, \Sigma) = d_\nu^{(F)}(A, \Sigma_\nu) = \inf\{d_\nu^{(F)}(A, M) \ : \ M \in \Sigma\} = \frac{1}{\|A^{-1}\|_\nu}.$$

For every multivariate polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$ with integer coefficients, we define its logarithmic height $ht(f)$ as the logarithm of the maximum of the absolute values of its coefficients. This notion introduced, we have the following statement which shows lower bounds for the bit length of approximate zeros.

Theorem 4 (Lower Bounds) *Let $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ be a sequence of multivariate polynomials. Let us assume that the following properties hold :*

i) $\max\{\deg(f_i) \ : \ 1 \leq i \leq n\} = 2$,

ii) $ht(f_i) \leq h$ *for* $1 \leq i \leq n$.

Let $\zeta \in V_K(f_1, \ldots, f_n)$ be a smooth $K-$rational point of the system $F := (f_1, \ldots, f_n)$. Let $|\cdot|_\nu \ : K \longrightarrow \mathbb{R}_+$ be an absolute value defined on K, and let $L \subseteq K$ be a number field such that $\zeta \in L_\nu^n$. Then, for every $z \in L^n$, $z \neq \zeta$ satisfying :

$$||z - \zeta||_\nu \gamma_\nu(F, \zeta) \leq \frac{3 - \sqrt{7}}{2},$$

the following inequality holds :

$$ht(z) \geq \frac{1}{3[L \, : \, \mathbb{Q}]} \left(\log \gamma_\nu(F, \zeta) - [L \, : \, \mathbb{Q}] \left(5 \log n + 2h\right) - 3\right).$$

Using Theorem 3 above, the following inequality also holds :

$$ht(z) \geq \frac{1}{3[L \, : \, \mathbb{Q}]} \Big(\log d_\nu^{(F)}(DF(\zeta)^{-1}, \Sigma_\nu) - [L \, : \, \mathbb{Q}] \left(7 \log n + 3h\right) - 5\Big).$$

Moreover, in the case where $L = \mathbb{Q}[i]$ is the field of Gaussian rationals, the two previous lower bounds may be rewritten as :

$$ht(z) \geq \frac{1}{6} \left(\log \gamma_\nu(F, \zeta) - (10 \log n + 4h + 3)\right), \text{ and}$$

$$ht(z) \geq \frac{1}{6} \Big(\log d_\nu^{(F)}(DF(\zeta)^{-1}, \Sigma_\nu) - (14 \log n + 6h + 5)\Big).$$

Let us observe that the "negative terms" in the previous lower bounds are linear in the input length (i.e. the bit length of the input system $F := (f_1, \ldots, f_n)$), whereas the "positive part" depends semantically on the smooth $K-$rational solution $\zeta \in V_K(f_1, \ldots, f_n)$.

Last, but not least, we may also show a few lower bounds for the average height of approximate zeros associated to a $\mathbb{Q}-$definable irreducible component of the solution variety $V(f_1, \ldots, f_n)$. To this end, we introduce some additional notations. Let $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ be a sequence of multivariate polynomials satisfying hypotheses $i)$ to $v)$ above. Let $\zeta \in K^n$ be a smooth $K-$rational zero of the system $F := (f_1, \ldots, f_n)$. Let $V := V(f_1, \ldots, f_n) \subset \mathbb{C}^n$ be the algebraic variety given as the common zeros of the polynomials $f_1, \ldots, f_n$. Let $\mathcal{V}_\zeta \subseteq V$ be the $\mathbb{Q}-$definable irreducible component of V that contains ζ . Let us assume $D := \deg(\mathcal{V}_\zeta)$ be the number of points in $\mathcal{V}_\zeta$. Let us observe that $D = \deg(\zeta) \leq [K \ : \mathbb{Q}]$. Let us assume

$$V_\zeta := \{\zeta_1, \ldots, \zeta_D\}.$$

Let $\| \cdot \| \ : K^n \longrightarrow \mathbb{R}$ be the standard hermitian norm induced in K^n by the inclusion $i \ : K \hookrightarrow \mathbb{C}$. A sequence of points $z := (z_1, \ldots, z_D) \in \mathbb{Q}[i]^{nD}$ is said to be an approximate zero of the system F with associate variety $\mathcal{V}_\zeta$ that satisfies the $\gamma-$Theorem, if for every i, $1 \leq i \leq D$, the following holds :

$$\|z_i - \zeta_i\| \leq \frac{3 - \sqrt{7}}{2\gamma(F, \zeta_i)},$$

where $\gamma(F, \zeta_i)$ is the quantity associated with the hermitian norm $\| \cdot \|$.

For every given approximate zero $z := (z_1, \ldots, z_D) \in \mathbb{Q}[i]^{nD}$ of the system F with associate variety V_ζ, the average height (also the average bit length) of z is defined in the following terms

$$ht_{av}(z) := \frac{1}{D} \sum_{i=1}^{D} ht(z_i).$$

Finally, let us denote by $\mathbb{Z}_K \subset K$ the ring of algebraic integers of the number field K. Then, we have the following lower bound for the average bit length of approximate zeros with associate variety $\mathcal{V}_\zeta$:

Proposition 5 *With the previous notations, let $\zeta \in V_K(f_1, \ldots, f_n)$ be a smooth $K-$rational with entries in $\mathbb{Z}_K$, i.e. $\zeta \in \mathbb{Z}_K^n$. Let us also assume that for every archimedean absolute value $| \cdot |_\nu$ (i. e. $\nu \in S$), the following holds :*

$$3\|\zeta\|_\nu \gamma_\nu(F, \zeta) \geq 3 - \sqrt{7}.$$

Then the average height of any approximate zero $z \in \mathbb{Q}[i]^{nD}$ of the system F with associate variety V_ζ that satisfies the γ–Theorem, also satisfies the following inequality :

$$ht_{av}(z) \geq \frac{1}{2} \left[ht(\zeta) - (\frac{1}{2} \log n + \log 2) \right].$$

In order to illustrate the meaning of this lower bound, we give here a few Corollaries which are proved in Subsection 3.2.

Corollary 6 *With the same notations as in Proposition 5 above, let $\zeta \in \mathbb{Z}_K^n \cap V_K(f_1, \ldots, f_n)$ be a smooth $K-$rational zero of the system $F := (f_1, \ldots, f_n)$ and let us assume that for every archimedean absolute value $| \cdot |_\nu \ : K \longrightarrow \mathbb{R}$ (i. e. for every $\nu \in S$), the following holds :*

$$\gamma_\nu(F, \zeta) \geq 3 - \sqrt{7}.$$

Then the average height of any approximate zero $z \in \mathbb{Q}[i]^{nD}$ of the system F with associate variety V_ζ that satisfies the γ–Theorem, also satisfies the following inequality :

$$ht_{av}(z) \geq \frac{1}{2} \left[ht(\zeta) - (\frac{1}{2} \log n + \log 2) \right].$$

Moreover, the previous techniques show how to deform a given system of multivariate polynomials by means of a single additional equation of low degree in such a way that the average bit length of the new system is essentially greater than the height of the particular zero you want to approximate.

Corollary 7 *Let $F := (f_1, \ldots, f_n)$ be a system of multivariate polynomials with integer coefficients satisfying the conditions i) to v) given on page 3. Let $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathbb{Z}_K^n \cap V_K(f_1, \ldots, f_n)$ be a smooth $K-$rational zero whose coordinates are algebraic integers. Let us now define the system of polynomial equations in $n + 1$ variables :*

$$G := (g_1, \ldots, g_{n+1}) \in (\mathbb{Z}[X_1, \ldots, X_{n+1}])^{n+1} ,$$

given by the following rules :

- *$g_i := f_i \in \mathbb{Z}[X_1, \ldots, X_{n+1}]$ for every i, $1 \leq i \leq n$,*
- *$g_{n+1} := (X_{n+1} - X_n)\,(X_{n+1} - (X_n + 1))$.*

Let $\zeta' \in V_K(g_1, \ldots, g_{n+1}) \cap \mathbb{Z}_K^{n+1}$ be the affine point given by :

$$\zeta' := (\zeta_1, \ldots, \zeta_n, \zeta_n) \in \mathbb{Z}_K^{n+1}.$$

Let $\mathcal{V}_{\zeta'} \subseteq V(g_1, \ldots, g_{n+1})$ be the $\mathbb{Q}-$definable irreducible component of $V(g_1, \ldots, g_{n+1})$ containing ζ'. Then, the average height of any approximate zero $z \in \mathbb{Q}[i]^{(n+1)D}$ of the system F with associate variety $\mathcal{V}_{\zeta'}$ that satisfies the $\gamma-$Theorem, also satisfies the following inequality :

$$ht_{av}(z) \geq \frac{1}{2}\left[ht(\zeta) - (\frac{1}{2}\log(n + 1) + \log 2)\right].$$

In Subsection 3.2 below, we exhibit several examples where all of the previous lower bounds for the bit length of approximate zeros apply. In fact, all our examples have been chosen such that the bit length of the corresponding approximate zero is exponential in the input length (i.e. in the bit length of the input system of multivariate polynomials with integer coefficients). Therefore, any of these examples allows us to conclude the following Corollaries 8 to 10 :

Corollary 8 *Computing approximate zeros in $\mathbb{Q}[i]$ for archimedean absolute values, using binary encoding of the output requires exponential running time and exponential output length, and these two lower bounds cannot be improved while maintaining this encoding. Namely, computing approximate zeros with binary encoding is in the complexity class* **EXTIME** $\setminus$ **P**.

Corollary 9 *Floating point encoding of approximate zeros requires an exponential number of digits and this lower bound cannot be improved. Namely, floating point encoding is not suitable for efficient computation of approximate zeros of systems of multivariate polynomial equations.*

As continuous fraction encoding of numbers in $\mathbb{Q}[i]$ is close to the binary encoding, we easily conclude the following :

Corollary 10 *Computing approximate zeros in $\mathbb{Q}[i]$ for archimedean absolute values, using continuous fraction encoding of the output requires exponential running time and exponential output length, and these two lower bounds cannot be improved while maintaining this encoding. Namely, computing approximate zeros with continuous fraction encoding is in the complexity class* **EXTIME** $\setminus$ **P**.

These lower bounds suggest that a central point of interest should be to study the bit length of approximate zeros satisfying the $\gamma-$Theorem. In order to shed some light in this direction, we prove the following statements :

Theorem 11 (Upper Bounds) *Let $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ be polynomials with integer coefficients. Let us assume that the following properties hold :*

- $\max\{\deg(f_i) : 1 \leq i \leq n\} \leq 2$, *and*
- $ht(f_i) \leq h$ *for* $1 \leq i \leq n$.

Let $\zeta \in V_K(f_1, \ldots, f_n)$ be a smooth $K-$rational point. Let $|\cdot|_\nu \ : K \longrightarrow \mathbb{R}_+$ be an absolute value on K. Then, the following inequality holds :

$$\log \gamma_\nu(F, \zeta) \leq 3[K \ : \ \mathbb{Q}]n \left(n^2 + 4\log n + h + ht(\zeta) + 3\right).$$

In particular, we show the following estimate for the bit length of approximate zeros in $\mathbb{Q}[i]^n$:

Corollary 12 (Upper bound on the bit length of approximate zeros) *With the same assumptions and notations as in Theorem 11 above, let $\zeta \in V_K(f_1, \ldots, f_n)$ be a smooth $K-$rational zero, and let $|\cdot|_\nu$ be an absolute value on K. Let $L \subseteq K$ be a number field such that $\zeta \in L_\nu^n$. Then there exist approximate zeros $z \in L^n$ of the system $F := (f_1, \ldots, f_n)$ with approximate zero ζ with respect to the absolute value $|\cdot|_\nu$, such that the logarithmic height $ht(z)$ of z is at most linear in the following quantities :*

$$\frac{1}{[L \ : \ \mathbb{Q}]} \log |\Delta_L| + [K \ : \ \mathbb{Q}]n \left(n^2 + h + nht(\zeta)\right),$$

where $|\Delta_L|$ is the absolute value of the discriminant of the field L.
Moreover, in the case where $L = \mathbb{Q}[i]$ (for instance, if $|\cdot|_\nu$ is archimedean), there exist approximate zeros $z \in \mathbb{Q}[i]^n$ for the system F with associate zero ζ with respect to $|\cdot|_\nu$ such that their bit lengths are at most linear in the following quantity :

$$[K \ : \ \mathbb{Q}]n \left(n^2 + h + nht(\zeta)\right), \textit{ in other words :}$$

$$ht(z) \leq O\left([K \ : \ \mathbb{Q}]n \left(n^2 + h + nht(\zeta)\right)\right).$$

Let us observe, that these two upper bounds above (i.e. Theorem 11 and Corollary 12) depend mainly on the input length : the dimension of the ambient space n and the height of the input polynomials h, and on two parameters which in turn depend on the actual zero to approximate : the degree $[K \ : \ \mathbb{Q}]$ of a field containing the coordinates and the logarithmic height $ht(\zeta)$ of the particular zero. These two quantities are bounded respectively by the geometric Bézout inequality (cf. [Hei83] or [Ful84, Vog84]) and the arithmetic Bézout inequality (cf. [BGS93, Phi91, Phi94, Phi95] or [KP94, KP96, Som98, Häg98, HMPS00], for instance). Moreover, combining these two upper bounds (Theorem 11 and Corollary 12) with the previously shown lower bounds and several examples described in Subsection 3.2, we may conclude that the upper bounds shown in Theorem 11 and Corollary 12 are optimal.
On the other hand, the $\gamma-$Theorem above has some aesthetic consequences which we may explain in terms of the existence of a *universal radius of convergence* independent of the absolute value under consideration. To this end, we recall the well–known Implicit Function Theorem for complete Noetherian local rings in the following terms :

Theorem 13 (Non–archimedean Basin of Attraction) *Let $F := (f_1, \ldots, f_n) \in \mathbb{Z}[X_1, \ldots, X_n]^n$ be a system of multivariate polynomials satisfying the hypotheses of Theorem 11 above. Let $\nu \in M_K$ define a non–archimedean absolute value $|\cdot|_\nu$ on K. Let us also assume that the restriction*

$$|\cdot|_\nu \ : \mathbb{Q} \longrightarrow \mathbb{R}_+$$

defines a $p-$adic absolute value, where $p \in \mathbb{N}$ is a prime number. Let $\zeta \in K^n$ be a smooth $K-$rational zero of the system which lies in the closed unit sphere of K^n, i.e.

$$\zeta \in B_\nu(0,1) := \{x \in K^n \ : \ \|x\|_\nu \leq 1\}.$$

Let us finally assume that $|\det DF(\zeta)|_\nu = 1$. Then, for every $z \in B_\nu(0,1)$ satisfying

$$\|z - \zeta\|_\nu \leq \frac{1}{p}$$

holds : z is an approximate zero of the system F with associate zero ζ with respect to the absolute value $|\cdot|_\nu$.

This statement is nothing but the usual Hensel Lemma in local algebra (cf. [ZS58, Mor97], for instance). However, this statement has a drawback : The radius of the basin of attraction centered at ζ depends on the concrete absolute value $|\cdot|_\nu$. The Theorem 11 above shows that there exists a *universal radius*, which depends only on the system F and the smooth $K-$rational zero, but does not depend on any particular absolute value.
To prove this claim, let us introduce quantity $\widetilde{\gamma}(F, \zeta)$ as follows : With the same notations and assumptions as above, we define the *universal quantity*

$$\widetilde{\gamma}(F, \zeta) := \left(\prod_{\nu \in M_K} \max\{1, \gamma_\nu(F, \zeta)\}^{n_\nu} \right)^{\frac{1}{[K:\mathbb{Q}]}}.$$

Let us observe that this quantity is well–defined and finite according to Theorem 11 above. Moreover, it does not depend on any particular absolute value under consideration. Thus, we may conclude the following Theorem :

Corollary 14 (Universal $\gamma-$Theorem) *With the same notations and assumptions as in Theorem 4, for every $z \in \mathbb{Q}[i]^n$ and every absolute value $|\cdot|_\nu$ satisfying the following inequality*

$$\|z - \zeta\|_\nu \widetilde{\gamma}(F, \zeta) \leq \frac{3 - \sqrt{7}}{2}$$

holds : z is an approximate zero for the system F with associate zero ζ and with respect to the absolute value $\nu \in M_K$.

Let us point out that the existence of such a universal quantity does not imply the existence of a universal basin of attraction independent of the absolute value under consideration (cf. Subsection 3.3 below). In fact, we show the following statement :

Corollary 15 *Let $F := (f_1, \ldots, f_n)$ be a sequence of multivariate polynomials with integer coefficients satisfying our hypotheses i) to v) on page 3. Let $\zeta \in V_K(f_1, \ldots, f_n)$ be a smooth $K-$rational zero. The only point $z \in K^n$ that satisfies the universal $\gamma-$Theorem near γ for all absolute values in M_K is $z = \zeta$. Namely, for every $z \in K^n$ satisfying the following inequality for every $\nu \in M_k$*

$$\|z - \zeta\|_\nu \leq \frac{3 - \sqrt{7}}{2\widetilde{\gamma}(F, \zeta)}$$

holds $z = \zeta$.

1.2 Kronecker's approach to solving

In [Kro82], Kronecker introduced a notion of solution of unmixed complex algebraic varieties, which we are going to reproduce here. Let $f_1, \ldots, f_i \in \mathbb{Z}[X_1, \ldots, X_n]$ be a sequence of polynomials defining a radical ideal $(f_1, \ldots, f_i)$ of codimension i in $\mathbb{C}[X_1, \ldots, X_n]$. Let $V := V(f_1, \ldots, f_i) \subseteq \mathbb{C}^n$ be the complex algebraic variety of codimension i given by the common zeros of the f_i. A *solution* of V is a birational isomorphism of V with some complex algebraic hypersurface in a space of adequate dimension.

Technically, this is is expressed as follows. First of all, let us assume that the variables $X_1, \ldots, X_n$ are in Noether position with respect to the variety V, i.e. we assume that the following is an integral ring extension :

$$\mathbb{Q}[X_1, \ldots, X_{n-i}] \hookrightarrow \mathbb{Q}[X_1, \ldots, X_n]/(f_1, \ldots, f_i).$$

Let $u := \lambda_{n-i+1}X_{n-i+1} + \cdots + \lambda_n X_n \in \mathbb{Q}[X_1, \ldots, X_n]$ be a linear form in the dependent variables $\{X_{n-i+1}, \ldots, X_n\}$. Thus we have a linear projection

$$\mathcal{U} \ : \mathbb{C}^n \longrightarrow \mathbb{C}^{n-i+1} \ : \ (x_1, \ldots, x_n) \longmapsto (x_1, \ldots, x_{n-i}, u(x_1, \ldots, x_n)) \, .$$

Let us also consider the restriction $\mathcal{U} \mid_V \ : V \longrightarrow \mathbb{C}^{n-i+1}$. The linear form u is called a *primitive element*, if and only if the projection $\mathcal{U} \mid_V$ defines a birational isomorphism of V with some complex hypersurface H_u in $\mathbb{C}^{n-i+1}$ with minimal equation $\chi_u \in \mathbb{Q}[X_1, \ldots, X_{n-i}, T]$. Then, a Kronecker solution of variety V consists of a description of the primitive element u, the hypersurface H_u through the minimal equation χ_u, and a description of the inverse of the birational isomorphism, i.e. $(\mathcal{U} \mid_V)^{-1}$. Formally, this list of items can be described as follows :

- The list of variables in Noether position $X_1, \ldots, X_n$ (which implies a description of the dimension of V).
- The primitive element $u := \lambda_{n-i+1}X_{n-i+1} + \cdots + \lambda_n X_n$ given by its coefficients in $\mathbb{Z}$.
- The minimal equation of the hypersurface H_u, namely
$$\chi_u \in \mathbb{Z}[X_1, \ldots, X_{n-i}, T].$$
- A description of $(\mathcal{U} \mid_V)^{-1}$. This description is given by the following list :
  - A non–zero polynomial $\rho \in \mathbb{Z}[X_1, \ldots, X_{n-i}]$.
  - A list of polynomials $v_j \in \mathbb{Z}[X_1, \ldots, X_{n-i}, T]$, $n - i + 1 \leq j \leq n$, such that the degrees with respect to variable T satisfy $\deg_T(v_j) \leq \deg_T(\chi_u)$ for every j, $n - i + 1 \leq j \leq n$.

  such that the following holds
$$(\mathcal{U} \mid_V)^{-1}(x, t) = \left(x_1, \ldots, x_{n-i}, \rho^{-1}(x)v_{n-i+1}(x, t), \ldots, \rho^{-1}(x)v_n(x, t)\right),$$
  where $x := (x_1, \ldots, x_{n-i}) \in \mathbb{C}^{n-i}$ and $t \in \mathbb{C}$.

Kronecker conceived an iterative procedure to solve multivariate systems of equations $F := (f_1, \ldots, f_n)$ defining zero–dimensional complex varieties, which can be described in the following terms :

First, you start with system (f_1) and you "solve" the unmixed variety of codimension 1, $V(f_1) \subseteq \mathbb{C}^n$. Then you proceed iteratively : From Kronecker's solution of the variety $V(f_1, \ldots, f_i)$ you eliminate the new equation f_{i+1} to obtain a Kronecker solution of the "next" variety $V(f_1, \ldots, f_{i+1})$. Proceed until you reach $i = n$. This iterative procedure has two main drawbacks, which can be explained in the following terms :

- First of all, the space problem arising with the representation of the intermediate polynomials. The polynomials χ_u, ρ and v_j are polynomials of high degree (eventually of degree 2^i) involving several variables. Thus, to represent them, one has to handle all their coefficients, which amounts to the following quantities

$$\binom{2^i + n - i + 1}{n - i + 1},$$

which for $i := n/2$ amounts to more than $2^{n^2/4}$ coefficients of great bit length.

- Secondly, Kronecker's iterative procedure introduces a nesting of interpolation procedures required for the iterative process and the linear change of coordinates required by each computation of a Noether normalisation. This nesting of interpolation procedures is difficult to avoid and increases the run time complexity.

Therefore, the procedure was forgotten by contemporary mathematicians and hardly mentioned in the literature of algebraic geometry. Macaulay quotes Kronecker's procedure in [Mac16] and so does König in [Kön03]. But both thought that this procedure would require excessive run time to be efficient, and so it was progressively forgotten. Traces of this procedure can be found spread over the algebraic geometry literature without giving the required relevance to it. For example, Kronecker's notion of solution was used by O. Zariski in [Zar95] to define a notion of dimension for algebraic varieties, claiming that it was also used in the same form by Severi and others.

In 1995, two works rediscovered Kronecker's approach to solving without previous knowledge of it's existing ancestors. These two works [GHMP95, Par95] were able to overcome the first drawback (space problem of representation) of the previous methods. The technical trick was the use of a data structure coming from semi–numerical modeling : straight–line programs. This idea of representing polynomials by programs evaluating them goes back to previous work of the same research group (such as [GH93, FGS95, KP94] or [KP96]). Moreover, these ideas were the natural continuation of the ideas previously developed in [GH91].

To overcome the second drawback (Nesting), the authors introduced a method based on Newton's method applied in a non–archimedean context (the approximate zeros in the corresponding non–archimedean basin of attraction were called *Lifting Fibers* in [GHH$^+$97]). This result was obtained in the two papers [GHH$^+$97, GHM$^+$98]. The key trick to avoid the nesting of interpolation procedures is based on Hensel's Lemma (also Implicit Mapping Theorem). Perhaps, the following statement could help explain the relations existing between Hensel's Lemma and Approximate Zero Theory.

To this end, let us introduce some more notations. Let $f_1, \ldots, f_r \in \mathbb{C}[X_1, \ldots, X_n]$ be a sequence of polynomials defining a radical ideal of codimension r in $\mathbb{C}[X_1, \ldots, X_n]$. Let us assume that the variables $X_1, \ldots, X_n$ are in Noether position with respect to the ideal $I := (f_1, \ldots, f_r)$, i.e. assume that the following ring extension is integral

$$\mathbb{C}[X_1, \ldots, X_{n-r}] \hookrightarrow \mathbb{C}[X_1, \ldots, X_n]/I.$$

Let $P := (p_1, \ldots, p_{n-r}) \in \mathbb{C}^{n-r}$ be an affine point, let $\mathcal{O}_P$ be the ring of formal power series at P, and let $\mathcal{M}_P$ be the field of fractions of $\mathcal{O}_P$. Then, the following is finite ring extension

$$\mathcal{M}_P \hookrightarrow B := \mathcal{M}_P[X_{n-r+1}, \ldots, X_n]/(f_1, \ldots, f_r),$$

and B is a zero–dimensional $\mathcal{M}_P-$algebra. Thus, it makes sense to look for approximate zeros of the solutions in $\mathcal{M}_P^r$ of the system of polynomial equations $F := (f_1, \ldots, f_r)$. The following statement about Hensel's Lemma explains the connections existing between Kronecker's solution and Approximate Zero Theory.

Theorem 16 (Hensel's Lemma) *With the same assumptions and notations as above, let $\zeta \in \mathcal{M}_P^r$ be a solution of the system F. Let $\|\cdot\| : \mathcal{M}_P^r \longrightarrow \mathbb{R}$ be usual non–archimedean norm in $\mathcal{M}_P^r$.*

Let $\mathbb{C}(X_1, \ldots, X_{n-r})$ be the field of rational functions. Then, for every $z \in \mathbb{C}(X_1, \ldots, X_{n-r})^r$, if $\|z\| \leq 1$, and

$$\|z - \zeta\| < \frac{1}{2},$$

then z is an approximate zero for the system $F := (f_1, \ldots, f_r)$ with associate zero $\zeta \in \mathcal{M}_P^r$.

Unfortunately, those two works [GHH$^+$97, GHM$^+$98] introduced (for the Lifting Fibers) run time requirements which depend on the heights of the intermediate varieties (in the sense of [BGS93, Phi91, Phi94, Phi95, Som98]). This drawback was finally overcome in the paper [GHMP97], where integer numbers were represented by straight–line programs and the following result established :

Theorem 17 *[GHMP97] There exists a bounded error probability Turing machine M which performs the following task : Given a system of multivariate polynomial equations $F := (f_1, \ldots, f_n)$, satisfying the following properties*

- $\deg(f_i) \leq 2$ *and $ht(f_i) \leq h$ for $1 \leq i \leq n$,*
- *the ideals $(f_1, \ldots, f_i)$ are radical ideals of codimension i in the ring $\mathbb{Q}[X_1, \ldots, X_n]$ for $1 \leq i \leq n-1$,*
- *the variety $V(f_1, \ldots, f_n) \subseteq \mathbb{C}^n$ is a zero–dimensional complex algebraic variety,*

the machine M outputs a Kronecker solution of the variety $V(f_1, \ldots, f_n)$. The running time of the machine M is polynomial in the following quantities

$$\delta(F)nh,$$

where δ is the maximum of the degrees of the intermediate varieties (in the sense of [Hei83]), namely

$$\delta(F) := \max\{\deg(V(f_1, \ldots, f_i)) \ : 1 \leq i \leq n-1\}.$$

It must be said that the coefficients of the polynomials involved in a Kronecker solution of the variety $V(f_1, \ldots, f_n)$ are given by straight–line programs that evaluate integer numbers. However, the complexity estimates for the Turing machine M are independent from the height.

Our attempt in these pages is to compare this approach to solving developed by Kronecker to that of Newton as described in the previous Subsection.

The exposition of new results starts with a small improvement of the Witness Theorem in [HS80] and [BCSS96] (cf. also [BCSS98b]). When dealing with straight–line program data structures, some relevant technical methods of comparison must be developed. These methods are known as probabilistic zero tests for polynomials given by straight–line programs. Examples of these tests are those introduced in [Sch79, Zip79, HS80] and the Witness Theorem, introduced in [HS80] for the case of polynomials with integer coefficients, and in [BCSS96] for polynomials with coefficients in a number field.

As we already had to introduce a few technical notions and methods spread over the literature of number theory, numerical analysis, algebraic complexity theory and elimination theory (described in Section 2), we can give for free (without introducing any further material) the following improvement of the estimates for the Witness Theorem, which is proved in Subsection 4.1.

Theorem 18 (Witness Theorem) *Let $P \in K[X_1, \ldots, X_n]$ be a non–zero polynomial evaluable by a non–scalar straight–line program Γ of size L, non–scalar depth ℓ and parameters in $\mathcal{F} \subseteq K$. Let $\omega_0 \in K$ be such that the following holds :*

$$ht(\omega_0) \geq \max\{\log 2, ht(\mathcal{F})\}.$$

Let $N \in \mathbb{N}$ be a non–negative integer such that

$$\log N > \log(\ell + 1) + (\ell + 2)(\log 2)(\log\log(4L)).$$

Let us define recursively the following sequence of algebraic numbers (known as Kronecker's scheme) :

$$\omega_1 := \omega_0^N, \text{ and for } 2 \le i \le n,\ \omega_i := \omega_{i-1}^N.$$

Then, the point $\underline{\omega} := (\omega_1, \ldots, \omega_n) \in K^n$ is a witness for P (i.e. $P(\underline{\omega}) \neq 0$).

Moreover, we observe that *approximate zeros are succinct encodings of generic points of the variety $V(f_1, \ldots, f_n)$.* This means that for every smooth $K-$rational zero $\zeta \in V_K(f_1, \ldots, f_n)$, the binary encoding of an approximate zero $z \in \mathbb{Q}[i]^n$ is sufficient information to compute the $\mathbb{Q}-$irreducible component of $V(f_1, \ldots, f_n)$ containing ζ. In more precise terms we show the following statement :

Theorem 19 (From Approximate Zeros to Geometric Solution) *With the same assumptions as in Theorem 17 above, there exists a bounded error probability Turing machine M, such that taking as input the binary encoding of an approximate zero $z \in \mathbb{Q}[i]$ of the system F with associate zero $\zeta \in V_K(f_1, \ldots, f_n)$ for an archimedean absolute value $|\cdot|_\nu$ (where $\nu \in S$), M outputs a Kronecker solution of the $\mathbb{Q}-$irreducible component W of $V(f_1, \ldots, f_n)$ containing ζ. Moreover, the running time of this probabilistic Turing machine is polynomial in the following quantities*

$$\deg(W)\,(n\ h\ ht(z) ht(\zeta)),$$

where $\deg(W)$ *is the degree of the $\mathbb{Q}-$irreducible component W containing ζ.*

The key idea for the proof of this Theorem is the use of the L^3 (or LLL) reduction algorithm as described in Subsection 4.5 below.
Conversely, as approximate zeros may depend on the height of the actual zero they approximate, we could be interested in the computation of approximate zeros for actual zeros of small (bounded) height.

Theorem 20 (From Kronecker's solution to Newton's solution) *There exists a bounded error probability Turing machine M which performs the following task : Given a sequence of polynomial equations $F := (f_1, \ldots, f_n)$ of degree at most 2 and height at most h, and given a positive integer number $H \in \mathbb{N}$ in binary encoding, the machine M outputs approximate zeros for the archimedean absolute value $|\cdot|\ : K \longrightarrow \mathbb{R}$ induced on K by the inclusion $i\ : K \hookrightarrow \mathbb{C}$ for all those zeros $\zeta \in V_K(f_1, \ldots, f_n)$, whose logarithmic height is at most H, i.e.*

$$ht(\zeta) \le H.$$

The running time of M is polynomial in the following quantities :

$$(n\ \ h\delta(F)) + (D\ n\ h\ H),$$

where the notations are the same as in Theorem 17 before.

A proof of this statement is given in Subsection 4.4 below, based again on an application of the L^3 reduction algorithm.
Let $Vol(F)$ be the normalized volume of the Newton polytope of the set

$$\{1, X_1, \ldots, X_n, M(F)\}$$

where $M(F)$ is the set of all monomials occurring in the polynomials $f_1, \ldots, f_n$ (cf. [Ber75, Kus76, Stu96]).
As $\delta(F) \le Vol(F)$ we obviously conclude the following Corollary for the sparse case.

Corollary 21 (Sparse case) *There exists a bounded error probability Turing machine M which performs the following task : Given a sequence of polynomial equations $F := (f_1, \ldots, f_n)$ of degree at most d and height at most h, and given a positive integer number $H \in \mathbb{N}$ in binary encoding, the machine M outputs approximate zeros for the archimedean absolute value $|\cdot|\ : K \longrightarrow \mathbb{R}$ induced on K by the inclusion $i\ : K \hookrightarrow \mathbb{C}$ for all those zeros $\zeta \in V_K(f_1, \ldots, f_n)$, whose logarithmic height is at most H, i.e.*

$$ht(\zeta) \leq H.$$

The running time of M is polynomial in the following quantities :

$$(n\ \ d\ h\sharp M(F)Vol(F)) + (D\ n\ h\ H),$$

where the notations are the same as in Theorem 17 before.

1.3 Application : Computation of splitting field and Lagrange resolvent

Combining both Kronecker's and Newton's approach to solving, we exhibit an efficient procedure for computing the splitting field and the Lagrange resolvent of an irreducible monic univariate polynomial $f \in \mathbb{Q}[X]$ of degree d. Let us recall that the splitting field of f is the minimal number field $K(f)$ containing the field of rational numbers $\mathbb{Q}$ and all roots of f (i.e. the minimal number field where f splits completely, also called the normal closure of the equation $f = 0$). This normal closure $K(f)$ is nothing but the Galois field of f and it satisfies

$$[K(f)\ :\ \mathbb{Q}] = \sharp\left(\mathrm{Gal}_{\mathbb{Q}}(f)\right),$$

where $\mathrm{Gal}_{\mathbb{Q}}(f)$ is the Galois group of the polynomial f. The splitting field of f can be identified with an irreducible component of the zero–dimensional algebra (known as the universal decomposition algebra)

$$A := \mathbb{Q}[X_1, \ldots, X_d]/(\sigma_0 - a_0, \ldots, \sigma_{d-1} - a_{d-1}),$$

where $\sigma_0, \ldots, \sigma_{d-1}$ are the elementary symmetric functions and f is written as $f(X) := a_0 + a_1X + \cdots + a_{d-1}X^{d-1} + X^d$. Let us also observe that the Lagrange resolvent is nothing but the Chow (or Cayley) elimination polynomial of the zero–dimensional residue algebra $A/\mathfrak{m}$, where $\mathfrak{m}$ is a well-chosen maximal ideal of A. Therefore, we can also show the following Theorem as a consequence of the comparison between Newton's and Kronecker's approach to solving :

Theorem 22 (Splitting Field and Lagrange Resolvent) *There exists a probabilistic Turing machine, which for every given univariate polynomial $f \in \mathbb{Z}[X]$ of degree at most d and logarithmic height at most h computes the following items :*

i) Approximate zeros in $\mathbb{Q}[i]$ of all zeros of f,

ii) a geometric description of the splitting field $K(f)$ of the polynomial f,

iii) and the Lagrange resolvent of the equation $f = 0$.

The running time of M is polynomial in the following quantities :

$$\sharp\left(Gal_{\mathbb{Q}}(f)\right)(dh).$$

1.4 Structure of the paper

As we have used different notions coming from different fields and different approaches, and we want to make our pages as readable as possible, we have included a section on fundamental tools, where all notions are introduced and some elementary and technical Lemmata are shown. The well–read reader might want to skip this section and go directly to the body of the paper. The Section 3 is devoted to establish the proofs for the results concerning Newton's approach to solving. In the Section 4, the relation between both approaches is studied, showing how to go from Kronecker's solution to Newton's and conversely. Finally, the Section 5 gives the proof for our statement about the computation of splitting field and the Lagrange resolvent.

2 Fundamental tools

2.1 Heights and norms

2.1.1 Multivariate polynomials

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

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

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

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

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

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

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

To simplify some expressions we often use the following notation : Given $\underline{X} := (X_1, \ldots, X_n)$ a list of variables and $\underline{\mu} := (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n$ a multi–index, we write $\underline{X}^{\underline{\mu}}$ to denote

$$\underline{X}^{\underline{\mu}} := X_1^{\mu_1} \cdots X_n^{\mu_n}.$$

2.1.2 Absolute values over number fields

We resume here in a very concise form the language and notation used for absolute values over number fields. For an introduction refer to e.g. [Lan83, Chapter 1], whereas a more complete exposition of the theory of absolute values can be found in Artin's *Algebraic Numbers and Algebraic Functions* [Art51] or [McC76]. Let $\mathbb{K}$ be the algebraic closure of a number field K.

Let $| \cdot |_\nu \; : K \longrightarrow \mathbb{R}_+$ be an absolute value defined on the number field K. By K_ν we denote the completion of K with respect to this absolute value $| \cdot |_\nu$ and by $\mathbb{K}_\nu$ we denote the algebraic closure of K_ν. For sake of simplicity, we also denote by $| \cdot |_\nu \; : K_\nu \longrightarrow \mathbb{R}_+$ the (unique) extension to K_ν of the absolute value $| \cdot |_\nu$ defined on K. We also assume that for archimedean $| \cdot |_\nu$ the algebraic closure $\mathbb{K}_\nu$ is included in $\mathbb{C}$.

Finally, we denote by n_ν the degree of K_ν over the completion of $\mathbb{Q}$ with respect to the absolute value $| \cdot |_\nu : \mathbb{Q} \longrightarrow \mathbb{R}$. Following [Lan83], let M_K be a proper set of absolute values of K. We assume that M_K has been chosen such that it satisfies Weil's *product formula* with multiplicities n_ν : For all $x \in K \setminus \{0\}$ holds

$$\frac{1}{[K : \mathbb{Q}]} \sum_{\nu \in M_K} n_\nu \log |x| = 0 \qquad (1)$$

where log stands for the natural logarithm, cf. [Lan83, Chapter 2].
Let us recall that by [Lan83, Proposition 4.3], for any given absolute value w on $\mathbb{Q}$ and all absolute values ν extending w to K, the following holds :

$$\sum_{\nu | w} n_\nu = [K : \mathbb{Q}]. \tag{2}$$

Observe that the proper set of absolute values M_K has only a finite number of archimedean absolute values (precisely the independent extensions of the ordinary archimedean value on $\mathbb{Q}$ to K induced by the non–isomorphic embeddings of K into $\mathbb{C}$, see below).
Let us recall that for archimedean valuations, i.e. $\nu \in S$, the absolute value $|\cdot|_\nu$ is defined in the following terms : for every $\nu \in S$, there exists an associated embedding $\sigma_\nu : K \longrightarrow \mathbb{C}$, such that for all $a \in K$ holds

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

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

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

Now, for all valuations $\nu \in M_K$, we define the *(logarithmic) height of P with respect to the absolute value* $|\cdot|_\nu$ as the logarithm of the maximum of the absolute values of the coefficients of P with respect to $|\cdot|_\nu$, i.e.

$$ht_\nu(P) := \max_{|\mu| \leq d} \{\log |P_\mu|_\nu\}.$$

Similarly, for every affine point $\underline{x} := (x_0, \ldots, x_n) \in K^{n+1}$ and for every $\nu \in M_K$ we may define the height of $\underline{x}$ with respect to the absolute value $|\cdot|_\nu$ as

$$ht_\nu(\underline{x}) := \max\{\log |x_i|_\nu \ : \ 0 \leq i \leq n\}$$

Finally, we define in the same way for a finite set $\mathcal{F} \subseteq K$ the *(logarithmic) height of $\mathcal{F}$ with respect to the absolute value* $|\cdot|_\nu$ as

$$ht_\nu(\mathcal{F}) := \max\{\log |a|_\nu : a \in \mathcal{F}\}.$$

Let us observe that all these notions of height depend on the absolute value $|\cdot|_\nu$ and on the field extension $\mathbb{Q} \subseteq K$. Later on (in Subsection 2.1.3 below), we discuss a notion of height independent of the absolute value and the field extension under consideration : Weil's height.
For archimedean absolute values we define the *weight of P with respect to the absolute value* $|\cdot|_\nu$ as the sum of the absolute values of the coefficients of P, i.e. for a polynomial $P \in K[X_1, \ldots, X_n]$ as

$$wt_\nu(P) := \log \left(\sum_{|\mu| \leq d} |P_\mu|_\nu \right).$$

Let us remark that $wt_\nu(P) = wt(\sigma_\nu(P))$ holds. Moreover, if $P \in K[X_1, \ldots, X_n]$ is a polynomial of degree at most d, the following relations hold :

$$ht_\nu(P) \leq wt_\nu(P) \leq \log \binom{d+n}{n} + ht_\nu(P).$$

2.1.3 Height of affine points

The measures we have chosen for the estimation of degrees and heights in our complexity study have a double aspect : geometric and diophantine. The geometric aspect refers to properties coming from algebraic geometry. Typically we may consider degrees of polynomials, number of monomials or the cardinality of zero–dimensional solution sets given by systems of multivariate polynomial equations. The diophantine aspect is more concerned with metric properties of the polynomials and the solution sets.

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

We start with the standard definition for the height of a projective point (cf. [Lan83]).

Given a projective point $\underline{x} := (x_0 : x_1 : \ldots : x_n) \in \mathbb{P}^n(K)$ with coordinates in the number field K, we define the logarithmic *height of the projective point* $\underline{x}$ (or simply the height) as :

$$ht(\underline{x}) := \frac{1}{[K:\mathbb{Q}]}\left(\sum_{\nu\in M_K} n_\nu ht_\nu(\underline{x})\right),$$

which does not depend on the number field K under consideration. For any affine point $\underline{x} := (x_1, \ldots, x_n) \in K^n$, we define its affine logarithmic height as the height of the projective point $(1 : x_1 : \ldots : x_n) \in \mathbb{P}^n(K)$, i.e.

$$ht(x) := ht(1 : x_1 : \ldots : x_n) := \frac{1}{[K:\mathbb{Q}]}\left(\sum_{\nu\in M_K} n_\nu \max\{0, ht_\nu(\underline{x})\}\right)$$

This notion of logarithmic height of an affine point is not so far from computational terms. Let us assume $K := \mathbb{Q}[i]$ as number field and $\underline{x} \in \mathbb{Q}[i]^n$ a point in the corresponding affine space. The point $\underline{x} := (x_1, \ldots, x_n)$ can also be seen as a list of objects that may be represented by digits on a tape of a Turing machine (cf. [BDG88] for more details). The bit length of $\underline{x}$ is understood as the amount of tape cells of the Turing machine required to keep written numerators and denominators of the coordinates of the list $\underline{x}$. Let us denote by $\ell(\underline{x})$ this bit length. An elementary argument shows the following inequalities relating bit length and height :

$$ht(\underline{x}) \leq \ell(\underline{x}) \leq 4n ht(\underline{x}).$$

In the sequel we use either bit length or height to refer to these essentially equivalent notions for affine points in $\mathbb{Q}[i]^n$.

Given a finite set $\mathcal{F} := \{b_i : 1 \leq i \leq M\} \subseteq K$, we can associate the affine point in K^M whose coordinates are the elements of $\mathcal{F}$. Then, the height of $\mathcal{F}$ will be defined as the height of this affine point, namely :

$$ht(\mathcal{F}) := ht(b_1, \ldots, b_M).$$

Let us observe that if the finite set $\mathcal{F}$ consists of just one point $\mathcal{F} = \{\alpha\} \subset K$, the height $ht(\mathcal{F})$ gives the usual notion of logarithmic height of the algebraic number $\alpha \in K$. This notion of logarithmic height verifies the conditions *a*) to *e*) of Proposition 4 of Chapter 7 of [BCSS98b] in logarithmic form, namely :

Lemma 23 *Let $x, y \in K$ be two complex algebraic numbers. With the previous notations, the following inequalities hold :*

i) $ht(a) = \log|a| \;\; \forall a \in \mathbb{Z}, \quad ht(x) = ht(-x) = ht(x^{-1}) \;\; \forall x \in K \setminus \{0\},$

ii) $ht(x+y) \leq ht(x) + ht(y) + \log 2,$

iii) $ht(x^k) = kht(x)$,

iv) $ht(x+y) \geq ht(x) - (ht(y) + \log 2)$, *and*

v) $ht(xy) \geq ht(x) - ht(y)$ *for* $y \neq 0$.

vi) *For every absolute value* $\nu \in M_K$ *and* $x \in K \setminus \{0\}$ *the following holds*

$$-[K\ :\ \mathbb{Q}]ht(x) \leq \log |x|_\nu \leq [K\ :\ \mathbb{Q}]ht(x).$$

It is not always wise to use these properties in the obvious inductive form or to apply them as a recursive tool. For instance, the following Lemma shows how to bound the height of the sum of algebraic numbers.

Lemma 24 *Given* $x_1, \ldots, x_n \in K$ *algebraic numbers, we have:*

$$ht(\sum_{i=1}^n x_i) \leq \log n + ht(x_1, \ldots, x_n).$$

Proof.– Let $\underline{x} := (x_1, \ldots, x_n) \in K^n$ be the corresponding affine point. We have

$$ht(\sum_{i=1}^n x_i) = \frac{1}{[K:\mathbb{Q}]} \left(\sum_{\nu \in M_K} n_\nu \max\{0, \log \left| \sum_{i=1}^n x_i \right|_\nu \} \right).$$

Now, we discuss separately archimedean and non–archimedean absolute values to obtain the following inequality :

$$ht(\sum_{i=1}^n x_i) \leq \frac{1}{[K:\mathbb{Q}]} \left(\sum_{\nu \in S} n_\nu \max\{0, \log n + ht_\nu(\underline{x})\} \right) +$$

$$\frac{1}{[K:\mathbb{Q}]} \left(\sum_{\nu \in M_K \setminus S} n_\nu \max\{0, ht_\nu(\underline{x})\} \right) \leq$$

$$\leq \frac{1}{[K:\mathbb{Q}]} \left(\sum_{\nu \in S} n_\nu \log n \right) + \frac{1}{[K:\mathbb{Q}]} \left(\sum_{\nu \in M_K} n_\nu \max\{0, ht_\nu(\underline{x})\} \right)$$

By Identity 2 on page 17 above, we easily conclude $ht(\sum_{i=1}^n x_i) \leq \log n + ht(\underline{x})$ as desired. ■

For multivariate polynomials $P \in K[X_1, \ldots, X_n]$ of degree at most d, we can identify the polynomial P with the affine point $\overline{P} \in K^M$, whose coordinates are the coefficients of P. Let M be the combinatorial number :

$$M := \binom{d+n}{n},$$

then, the height of P is defined as the height of the affine point $\overline{P} \in K^M$. This yields the following identity

$$ht(P) := ht(\overline{P}) = \frac{1}{[K:\mathbb{Q}]} \left(\sum_{\nu \in M_K} n_\nu \max\{0, ht_\nu(P)\} \right).$$

Another useful notion is that of absolute logarithmic weight, which is also independent of the field extension. For every polynomial $P \in K[X_1, \ldots, X_n]$, we define its weight in the following terms :

- *Archimedean weight :*
$$wt_a(P) := \frac{1}{[K:\mathbb{Q}]}\left(\sum_{\nu\in S} n_\nu \max\{0, wt_\nu(P)\}\right),$$

- *Non–archimedean weight :*
$$wt_{na}(P) := \frac{1}{[K:\mathbb{Q}]}\left(\sum_{\nu\in M_K\setminus S} n_\nu \max\{0, ht_\nu(P)\}\right),$$

- *Weight :*
$$wt(P) := wt_a(P) + wt_{na}(P).$$

Let us observe that, if $P \in \mathbb{Z}[X_1, \ldots, X_n]$ is a polynomial with integer coefficients, this notion of height agrees with the logarithm of the standard weight, i.e.

$$wt(P) = \log WT(P).$$

These notions of height and weight have many relevant applications and properties. Let us shortly point out some relevant facts concerning univariate polynomials.

Lemma 25 *Let $P = \sum_{k=0}^{d} a_k X^k \in K[X]$ be a univariate polynomial and $x \in K$ an algebraic number. Then holds :*
$$ht(P(x)) \leq \log(d+1) + ht(P) + dht(x).$$

Proof.– Let us define the affine points $\underline{a} := (a_0, a_1, \ldots, a_d) \in K^{d+1}$ and $\underline{A} := (a_0, a_1x, \ldots, a_dx^d) \in K^{d+1}$. Then, we may apply the previous Lemma 24 to obtain

$$ht(P(\alpha)) \leq \log(d+1) + ht(\underline{A}).$$

Now, for every $\nu \in M_K$ we have the following obvious inequality

$$\max\{0, ht_\nu(\underline{A})\} \leq \max\{0, ht_\nu(\underline{a})\} + d\max\{0, \log|vx|\}.$$

This yields the following upper bound :

$$ht(\underline{A}) \leq ht(\underline{a}) + dht(x) \leq ht(P) + dht(x),$$

which proves the Lemma. ■

Lemma 26 (A lower bound) *Given $P = \sum_{k=0}^{d} a_d X^d \in K[X]$ an univariate polynomial, and $x \in K$, we have:*
$$ht(P(x)) \geq ht(x) - (\log d + 2ht(P) + \log 2)$$

Proof.– This proof follows the same strategy as the proof in [BCSS98b], modified by the bounds described in the two Lemmata 24,25 above. ■

An obvious consequence of the previous Lemma is the following estimate for the height of the zeros of a univariate polynomial.

Corollary 27 *Given $P = \sum_{k=0}^{d} a_d X^d \in K[X]$, and $\zeta \in K$ such that $P(\zeta) = 0$. Then, we have*
$$ht(\zeta) \leq (\log d + 2ht(P) + \log 2).$$

It seems convenient to recall the reader the following, simpler estimate :

Lemma 28 *Let $\underline{x} \in K^n$ and $\underline{y} \in K^m$ be two points in two affine spaces, we have*
$$ht(\underline{x}, \underline{y}) \leq ht(\underline{x}) + ht(\underline{y}).$$

2.1.4 Norms of affine points and linear operators

For the purposes of our study, we are interested in the normed vector space K^n endowed with the norms induced by the absolute values in M_K. Let $\nu \in M_K$ an absolute value and $|\cdot|_\nu \ : K \longrightarrow \mathbb{R}_+$ the absolute value function. We can endow K^n with a norm $\|\cdot\|_\nu \ : K^n \longrightarrow \mathbb{R}_+$ in the following way :

- If $|\cdot|_\nu$ is archimedean (i.e. $\nu \in S$), we define $\|v\|_\nu := \sqrt{\sum_{i=1}^{n} |z_i|_\nu^2}$.
- Otherwise (i.e. if $\nu \in M_K \setminus S$), we define $\|v\|_\nu := \max_{i=1}^{n} |z_i|_\nu$.

Let K_ν be the completion of K with respect to the absolute value $|\cdot|_\nu$. According to the previous rules, we may also define the (unique) extensions to K_ν and K_ν^n of the previous functions defined on K. In other words, we also use $|\cdot|_\nu$ and $\|\cdot\|_\nu$ to denote the mappings

$$|\cdot|_\nu \ : K_\nu \longrightarrow \mathbb{R}_+ \text{ and } \|\cdot\|_\nu \ : K_\nu^n \longrightarrow \mathbb{R}_+.$$

Thus, we may introduce the standard notions of norm for linear and multilinear operators over $K_\nu-$vector spaces :
Let us assume that $A \ : K_\nu^n \longrightarrow K_\nu^n$ is a linear mapping. As usual, we define the norm $\|A\|_\nu$ of the $n \times n$ matrix $A \in \mathcal{M}_n(K_\nu)$ in the following terms :

$$\|A\|_\nu := \sup\{\|A(v)\|_\nu \ : \ v \in K_\nu^n \ , \|v\|_\nu \leq 1\}.$$

Given a multilinear operator

$$A \ : (K_\nu^n)^m \longrightarrow K_\nu^n,$$

we define its norm in a straight forward way as :

$$\|A\|_\nu := \sup\{\|A(v_1, \ldots, v_m)\|_\nu \ : \ v_i \in K_\nu^n, \|v_i\|_\nu \leq 1, \ \forall i, 1 \leq i \leq m\}.$$

Let us also introduce the Frobenius or Hilbert–Weil norm $\|\cdot\|_\nu^{(F)}$ on $\mathcal{M}_n(K_\nu)$, associated to the absolute value $\nu \in M_K$. First of all, let us assume that $|\cdot|_\nu$ is archimedean. Let $\sigma_\nu \ : K_\nu \longrightarrow \mathbb{C}$ the embedding of the completion of K into the field of complex numbers. For every square matrix $A \in \mathcal{M}_n(K_\nu)$ we define its Frobenius norm in the following terms :

$$\|A\|_\nu^{(F)} := \sqrt{Tr(A_\nu^* A_\nu)} = \sqrt{\sum_{i,j=1}^{n} |a_{ij}|_\nu^2},$$

where Tr stands for the standard trace of a square matrix, $A_\nu := \sigma_\nu(A) \in \mathcal{M}_n(\mathbb{C})$ and A_ν^* is the transposed conjugate matrix of A_ν.
On the other hand, if $|\cdot|_\nu$ is non–archimedean and $A := (a_{i,j})_{i,j} \in \mathcal{M}_n(K_\nu)$, we define the Frobenius norm of A with respect to the non–archimedean absolute value $|\cdot|_\nu$ in the following terms :

$$\|A\|_\nu^{(F)} := \max\{|a_{i,j}|_\nu \ : \ 1 \leq i, j \leq n\}.$$

Let us consider in $\mathcal{M}_n(K_\nu)$ the subgroup $GL(n, K_\nu)$ of all non–singular $n \times n$ matrices with entries in K_ν. Similarly, we denote by $GL(n, K)$ the subgroup of $GL(n, K_\nu)$ of all non–singular $n \times n$ matrices with entries in the number field K. According to our notation introduced before, we define the algebraic varieties $\Sigma_\nu \subseteq \mathcal{M}_n(K_\nu)$ and $\Sigma \subseteq \mathcal{M}_n(K)$ of $n \times n$ singular matrices respectively in the following terms :

$$\Sigma_\nu := \mathcal{M}_n(K_\nu) \setminus GL(n, K_\nu) \text{ and } \Sigma := \mathcal{M}_n(K) \setminus GL(n, K).$$

These notions of norms of linear and multilinear operators verify the obvious usual properties. Let us point just a few of them which are going to be used in the sequel.

Lemma 29 *Let $\nu \in M_K$ be an absolute value on K. Let $A := (a_{i,j})_{i,j} \in \mathcal{M}_n(K_\nu)$ be a square matrix and let $B\ : (K_\nu^n)^m \longrightarrow K_\nu^n$ a multilinear operator. Let J denote a suitable set of indices for B, i.e. $B := (b_j)_{j \in J}$ are the entries of B. The following properties hold :*

i) (cf. [Cia82], for instance) For archimedean $|\cdot|_\nu$ holds $\|A\|_\nu \leq \|A\|_\nu^{(F)} \leq \sqrt{n}\|A\|_\nu$.

ii) (cf. [Tyl94]) For non–archimedean $|\cdot|_\nu$ holds the equality $\|A\|_\nu = \|A\|_\nu^{(F)}$.

iii) Moreover, if A and B have entries in the number field K, they can be seen as points of the affine spaces K^{n^2} and K^{m^n}, respectively. Thus, the following inequalities hold :

$$\log\|A\|_\nu \leq \log\|A\|_\nu^{(F)} \leq \log n + ht_\nu(A) \leq \log n + [K:\mathbb{Q}]\max\{ht(a_{i,j})\ :\ 1 \leq i,j \leq n\},$$

$$\log\|B\|_\nu \leq (m+1)\log n + [K\ :\ \mathbb{Q}]\max\{ht(b_j)\ :\ j \in J\}.$$

iv) For every $\nu \in M_K$, these notions of norm behave as expected with respect to matrix products, i.e.

$$\|AB\|_\nu \leq \|A\|_\nu\|B\|_\nu$$

v) In particular, if A is a non–singular $A \in GL(n, K_\nu))$, the following inequalities hold :

$$\|A^{-1}B\|_\nu \geq \frac{\|B\|_\nu}{\|A\|_\nu},$$

$$\|A^{-1}\|_\nu \leq \frac{\|A\|_\nu^{n-1}}{|\det(A)|_\nu}.$$

vi) If the matrix A is non–singular, then for every square matrix $C \in \mathcal{M}_n(K_\nu)$ holds :

$$\textit{If } \|A-C\|_\nu < \frac{1}{\|A^{-1}\|_\nu} \textit{ then this implies } C \in GL(n, K_\nu).$$

We relate norms, height and weight for images of polynomial mappings in the following Lemma :

Lemma 30 *Let $F\ : K^n \longrightarrow K^m$ a polynomial mapping, where $m \geq n$. Let us assume that $F := (f_1, \ldots, f_m)$, where $f_i \in K[X_1, \ldots, X_n]$ is a polynomial of degree at most d such that*

$$wt(f_i) \leq w,\ \forall i, 1 \leq i \leq m.$$

Let $x := (x_1, \ldots, x_n) \in K^n$ be an affine point. The following inequalities hold :

i) $ht(F(x)) \leq w + dht(x)$.

ii) Let $DF(x)\ : K_\nu^n \longrightarrow K_\nu^m$ be the tangent mapping given by the Jacobian matrix of F at x. Then holds :

$$\log\|DF(x)\|_\nu \leq \log(mnd) + (d-1)ht_\nu(x) + \max\{wt_\nu(f_i)\ :\ 1 \leq i \leq m\},$$

as well as the upper bound

$$\log\|DF(x)\|_\nu \leq \log(mnd) + [K\ :\ \mathbb{Q}]\left(w + (d-1)ht(x)\right).$$

iii) (Liouville lower bound) For every $\nu \in M_K$, the following holds :

$$\log\|F(x)\|_\nu \geq -[K:\mathbb{Q}]\left(w + dht(x)\right).$$

Proof.– Claim *i*) follows by a strategy similar to that introduced in the proof of Lemma 25. The only difference consists in replacing the height by the weight when discussing archimedean absolute values. Claim *ii*) uses the following chain of inequalities :

$$\|DF(x)\|_\nu \leq \|DF(x)\|_\nu^{(F)} \leq \log(nm) + \log\max\{|\frac{\partial f_i}{\partial X_j}(x)|_\nu \ : \ 1 \leq i \leq m, 1 \leq j \leq m\}.$$

Finally, we just have to observe that $\log|\frac{\partial f_i}{\partial X_j}(x)|_\nu \leq \log d + wt_\nu(f_i) + (d-1)ht_\nu(x)$. The rest follows then from the relations between local and logarithmic weights and heights. To prove Claim *iii*), we argue in the following way : Let us assume that $f_i(\underline{x}) \neq 0$. In this case, we have

$$ht(f_i(\underline{x})^{-1}) = ht(f_i(\underline{x})).$$

Moreover, the following inequality holds :

$$\frac{1}{[K:\mathbb{Q}]}\log|f_i(\underline{x})|_\nu^{-1} \leq \frac{1}{[K:\mathbb{Q}]}\left(\sum_{\nu\in M_K} n_\nu \max\{0, \log|f_i(\underline{x})|_\nu^{-1}\}\right) = ht(f_i(\underline{x})).$$

Using the upper bound of Claim *i*), we conclude the following inequality :

$$\frac{1}{[K:\mathbb{Q}]}\log|f_i(\underline{x})|_\nu^{-1} \leq ht(f_i(\underline{x})) \leq w + dht(\underline{x}).$$

Hence, the following holds : $\log\|F(\underline{x})\|_\nu \geq \log|f_i(\underline{x})|_\nu \geq -[K:\mathbb{Q}]\,(w + dht(\underline{x}))$. ■

3 Newton's approach to solving : On the bit length of approximate zeros

In this Section we shall prove the main statements concerning approximate zeros given in the Introduction. The Section is divided into three Subsections : The first is devoted to a proof of the Eckardt & Young Theorem for non–archimedean absolute values, the second and third show respectively lower and upper bounds for the bit length of approximate zeros.

3.1 Eckardt & Young Theorem.

First of all, we show Theorem 3 from page 6 of the Introduction. To this end, we quickly recall some of the notation : Let us consider in $\mathcal{M}_n(K_\nu)$ the subgroup $GL(n, K_\nu)$ of all non–singular $n \times n$ matrices with entries in K_ν. Similarly, we denote by $GL(n, K)$ the subgroup of $GL(n, K_\nu)$ of all non–singular $n \times n$ matrices with entries in the number field K. We define the algebraic varieties $\Sigma_\nu \subseteq \mathcal{M}_n(K_\nu)$ and $\Sigma \subseteq \mathcal{M}_n(K)$ of $n \times n$ singular matrices respectively as

$$\Sigma_\nu := \mathcal{M}_n(K_\nu) \setminus GL(n, K_\nu), \text{ and } \Sigma := \mathcal{M}_n(K) \setminus GL(n, K).$$

Let us also recall that $d_\nu^{(F)}$ is the Frobenius (also Hilbert–Weil) metric on $\mathcal{M}_n(K_\nu)$. Then, the following holds :

Theorem 31 (Eckardt & Young) *Let $\nu \in M_K$ be an absolute value. For every non–singular $n \times n$ matrix $A \in GL(n, K)$, the following equality holds :*

$$d_\nu^{(F)}(A, \Sigma) = d_\nu^{(F)}(A, \Sigma_\nu) = \inf\{d_\nu^{(F)}(A, M) \ : \ M \in \Sigma\} = \frac{1}{\|A^{-1}\|_\nu}.$$

Proof.– Let us start by assuming that $|\cdot|_\nu$ is an archimedean absolute value. The proofs of [EY36, BCSS98a] establish the following identity :

$$d_\nu^{(F)}(A, \Sigma_\nu) = \frac{1}{\|A^{-1}\|_\nu}.$$

Now, since Σ is dense in Σ_ν for the Frobenius norm, the statement follows for the archimedean case. Let us assume now that $\nu \in M_K \setminus S$ defines a non–archimedean absolute value $|\cdot|_\nu$, and that $A = (a_{i,j})_{i,j} \in GL(n, K)$ is a non–singular matrix. Let $A_{i,j}$ be the minor of matrix A obtained by suppressing row i and column j. Thus, from Claim *ii*) of Lemma 29 on page 22, we conclude the following identity :

$$\frac{1}{\|A^{-1}\|_\nu} = \min\left\{ \left| \frac{\det(A)}{A_{i,j}} \right|_\nu \ : \ A_{i,j} \neq 0 \right\}.$$

Without loss of generality, we may assume that this minimum is reached at $A_{1,1}$, i.e. we assume that the following identity holds :

$$\frac{1}{\|A^{-1}\|_\nu} = \left| \frac{\det(A)}{A_{1,1}} \right|_\nu.$$

Let us consider the following $(n-1) \times (n-1)$ system of linear equations :

$$\begin{array}{rcl} X_2 a_{2,2} + \ldots + X_n a_{2,n} & = & a_{2,1} \\ \vdots & \vdots & \vdots \\ X_2 a_{n,2} + \ldots + X_n a_{n,n} & = & a_{n,1} \end{array} \tag{3}$$

As the minor $A_{1,1}$ is non–zero, this system of equations has a unique solution, which we shall denote by $(\lambda_2, \ldots, \lambda_n) \in K_\nu^{n-1}$. Using Cramer's rule, we can determine the values λ_i, for every i, $2 \le i \le n$ in the following terms :

$$\lambda_i := \frac{(-1)^i A_{1,i}}{A_{1,1}} \in K.$$

Now we define the $n \times n$ square matrix M as

$$M := \begin{pmatrix} m_{1,1} & \cdots & m_{1,n} \\ \vdots & & \vdots \\ m_{n,1} & \cdots & m_{n,n} \end{pmatrix} \in \mathcal{M}_n(K),$$

whose entries are given by the following rules :

- For every $j \neq 1$, we define $m_{i,j} := a_{i,j} \in K$.
- For every i, $1 \le i \le n$, we define $m_{i,1} := \sum_{j=2}^{n} \lambda_i a_{i,j}$.

Obviously, the matrix M is singular and its entries are in K (i.e. $M \in \Sigma$). Moreover, we have

$$A - M := \begin{pmatrix} c_{1,1} & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}, \text{ where } c_{1,1} = a_{1,1} - \sum_{i=2}^{n} \lambda_i a_{1,i}.$$

Using the identity that relates the values λ_i and the minors of the matrix A, one easily concludes that

$$c_{1,1} = a_{1,1} - \frac{1}{A_{1,1}} \sum_{i=2}^{n} (-1)^i a_{1,i} A_{1,i} = \frac{\det(A)}{A_{1,1}}.$$

Thus, we conclude the following inequality :

$$d_\nu^{(F)}(A, \Sigma) \leq \|A - M\|_\nu^{(F)} = \left| \frac{\det(A)}{A_{1,1}} \right|_\nu = \frac{1}{\|A^{-1}\|_\nu}$$

On the other hand, Claim $v)$ of Lemma 29 on page 22 shows that

$$d_\nu^{(F)}(A, \Sigma) \geq d_\nu^{(F)}(A, \Sigma_\nu) \geq \frac{1}{\|A^{-1}\|_\nu}$$

and therefore the proof is concluded for the non–archimedean case, too. ■

3.2 Approximate zero theory : Lower bounds for the bit length of approximate zeros.

Following the notations and assumptions of Subsection 1.1, we state a few more technical details, which will be used in the proofs of our statements concerning approximate zero theory.
Introduced by S. Smale as a basic ingredient to study the complexity of Gauss' proof of the Fundamental Theorem of Algebra (cf. [Sma81, BCSS98a] and the references therein), the notion of *approximate zero* has evolved to become a new foundation for numerical analysis. Previously, there had been several deep studies of the univariate case ([Sma81, Sma85, Sma86a, Sma86b, Ren87, SS86, SS85]), where the notion was successfully extended by M. Shub and S. Smale to the multivariate case (cf. [SS93a, SS93b, SS93c, SS96, SS94b]). Recent advances within this school have been obtained by J.P. Dedieu ([Ded96, Ded97c, Ded97b, Ded97a, DSa, DSb, DS98]), G. Malajovich ([Mal93, Mal94, Mal95]) and J.C. Yakoubsohn ([Yak95b, Yak95a] and M.H. Kim [Kim]).
A useful technical tool to prove the $\gamma-$Theorem 2 (given on page 5 of the Introduction) is the following Proposition :

Proposition 32 *With the same notations and assumptions as in Theorem 2, let us assume that*

$$u := \|z - \zeta\|_\nu \gamma_\nu(F, \zeta) \leq \frac{3 - \sqrt{7}}{2} < 1 - \frac{\sqrt{2}}{2}.$$

Then $DF(z) \in GL(n, K)$ is a non–singular matrix, and the following inequality holds :

$$\|DF(z)^{-1} DF(\zeta)\|_\nu \leq \frac{(1-u)^2}{\psi(u)},$$

where $\psi(u) := 2u^2 - 4u + 1$.

Let us observe two facts concerning the $\gamma-$neighbourhood of an isolated smooth zero $\zeta \in V_K(f_1, \ldots, f_n)$: First, any smooth zero $\zeta \in V_K(f_1, \ldots, f_n)$ is a fixed point of the Newton operator. Second, singular zeros $\zeta' \in V_K(f_1, \ldots, f_n)$ satisfy $DF(F, \zeta') \notin GL(n, K)$. Thus, no other zero $\zeta' \in V_K(f_1, \ldots, f_n)$ lies in the $\gamma_\nu-$neighbourhood of ζ. In other words, the following inequality holds for every $\zeta' \in V_K(f_1, \ldots, f_n)$, $\zeta' \neq \zeta$:

$$\|\zeta - \zeta'\|_\nu \gamma_\nu(F, \zeta) \geq \frac{3 - \sqrt{7}}{2}.$$

In fact, defining $sep_\nu(F, K)$ as the minimum "separating" distance of any two $K-$rational zeros with respect to the absolute value $\nu \in M_K$, we have

$$sep_\nu(F, K) \geq \frac{3-\sqrt{7}}{2\gamma_\nu(F, \zeta)}. \tag{4}$$

Using the identity established in the Eckardt & Young Theorem 3 on page 6, we can show the following lower bound for $\gamma_\nu(F, \zeta)$:

Proposition 33 *Let $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ be a sequence of multivariate polynomials. Let us assume that the following holds :*

- $d = \max\{\deg(f_i) \ : \ 1 \leq i \leq n\} \geq 2,$
- $ht(f_i) \leq h,\ wt(f_i) \leq w,\ 1 \leq i \leq n.$

Let $\zeta \in V_K(f_1, \ldots, f_n)$ be a smooth $K-$rational point with respect to the system of polynomials $F := (f_1, \ldots, f_n)$. Then, with the same notations as before, the following inequality holds :

$$\log \gamma_\nu(F, \zeta) \geq \frac{\log d_\nu^{(F)}(DF(\zeta)^{-1}, \Sigma)}{d-1} - (\frac{h}{d-1} + 2\log d).$$

Proof.– Using Claim $v)$ of Lemma 29, we have the following inequality :

$$\gamma_\nu(F, \zeta)^{d-1} \geq \frac{\|\frac{D^{(d)}F(\zeta)}{d!}\|_\nu}{\|DF(\zeta)\|_\nu}.$$

From Theorem 3 we obviously conclude

$$\frac{1}{\|DF(\zeta)\|_\nu} = d_\nu^{(F)}(DF(\zeta)^{-1}, \Sigma).$$

On the other hand $D^{(d)}F(\zeta)$ is a multilinear operator whose entries do not depend on ζ. Moreover, since $d = \max\{\deg(f_i) \ : \ 1 \leq i \leq n\}$, we are sure that this multilinear operator is not identically zero. Let us use the following notation for the dense encoding of the polynomials $f_1, \ldots, f_n$:

$$f_i := \sum_{|\mu| \leq d} a_\mu^{(i)} \underline{X}^\mu,$$

where $\mu \in \mathbb{N}^n$ are multi–indices. Now, there exists some $\mu := (\mu_1, \ldots, \mu_n) \in \mathbb{N}^n$, such that $|\mu| = d$, and some $i \in \mathbb{N}$, $1 \leq i \leq n$, such that $a_\mu^{(i)} \neq 0$. Then, the following inequality holds :

$$\|\frac{D^{(d)}F(\zeta)}{d!}\|_\nu \geq \|\frac{\mu_1! \cdots \mu_n!}{d!}\|_\nu |a_\mu^{(i)}|_\nu.$$

As the polynomials $f_1, \ldots, f_n$ have integer coefficients, we know that the following also holds :

$$\log \|\frac{D^{(d)}F(\zeta)}{d!}\|_\nu \geq -(d\log d + h) \geq -(d\log d + w).$$

Thus, we conclude $\log \gamma_\nu(F, \zeta) \geq \dfrac{\log d_\nu^{(F)}(DF(\zeta)^{-1}, \Sigma)}{d-1} - \left(\dfrac{d\log d}{d-1} + \dfrac{h}{d-1}\right).$ ■

To prove Theorem 4 from page 6, we establish the following Theorem and then derive Theorem 4 :

Theorem 34 *Let $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ be a sequence of multivariate polynomials. Let us assume that the following properties hold*

- $d = \max\{\deg(f_i) \,:\, 1 \leq i \leq n\} \geq 2,$
- $wt(f_i) \leq w,\ 1 \leq i \leq n.$

Let $\zeta \in V_K(f_1, \ldots, f_n)$ be a smooth $K-$rational point of the system $F := (f_1, \ldots, f_n)$. Let $|\cdot|_\nu : K \longrightarrow \mathbb{R}_+$ be an absolute value defined on K, and let $L \subseteq K$ be a number field such that $\zeta \in L_\nu^n$. Then, for every $z \in L^n$, $z \neq \zeta$ satisfying

$$||z - \zeta||_\nu \gamma_\nu(F, \zeta) \leq \frac{3 - \sqrt{7}}{2},$$

the following inequality holds :

$$ht(z) \geq \frac{1}{2d-1}\left(\frac{\log \gamma_\nu(F, \zeta) - \log(n^2 d) - 2}{[L \,:\, \mathbb{Q}]} - 2w\right).$$

With the same assumptions also holds :

$$ht(z) \geq \frac{1}{2d-1}\left(\frac{\log d_\nu^{(F)}(DF(\zeta)^{-1}, \Sigma_\nu) - (d-1)(\log(n^2 d^3) + 2)}{(d-1)[L \,:\, \mathbb{Q}]} - 3w\right).$$

Moreover, in the case where $L = \mathbb{Q}[i]$ is the field of Gaussian rationals, the two previous lower bounds can be rewritten as :

$$ht(z) \geq \frac{1}{2d-1}\left(\frac{\log \gamma_\nu(F, \zeta) - \log(n^2 d) - 2}{2} - 2w\right) \text{ and}$$

$$ht(z) \geq \frac{1}{2d-1}\left(\frac{\log d_\nu^{(F)}(DF(\zeta)^{-1}, \Sigma_\nu) - (d-1)(\log(n^2 d^3) + 2)}{2(d-1)} - 3w\right).$$

Proof.– Let us consider the Taylor expansion of F at ζ :

$$F(z) = \sum_{k=1}^{d} \frac{D^{(k)}F(\zeta)(z - \zeta)^k}{k!}.$$

The following inequality holds :

$$\|F(z)\|_\nu = \left\| DF(z)DF(z)^{-1}DF(\zeta) \sum_{k=1}^{d} \frac{DF(\zeta)^{-1}DF^{(k)}(\zeta)(z - \zeta)^k}{k!} \right\|_\nu$$

$$\leq \|DF(z)\|_\nu \|DF(z)^{-1}DF(\zeta)\|_\nu \cdot \left(\sum_{k=1}^{d} (\gamma_\nu(F, \zeta)\|z - \zeta\|_\nu)^{k-1}\right) \|\zeta - z\|_\nu$$

Defining $u := \|\zeta - z\|_\nu \gamma_\nu(F, \zeta)$ and $\psi(u) := 2u^2 - 4u + 1$, from Proposition 32 above (cf. also Lemma 2 in [BCSS98a, p. 146]), we conclude the following inequality :

$$\|F(z)\|_\nu \leq \|DF(z)\|_\nu \frac{(1-u)u}{\psi(u)\gamma_\nu(F, \zeta)}.$$

Since $\frac{(1-u)u}{\psi(u)}$ is increasing in the closed interval $\left[0, \frac{3-\sqrt{7}}{2}\right]$, we have

$$\|F(z)\|_\nu \leq \|DF(z)\|_\nu \frac{c_1}{\gamma_\nu(F, \zeta)},$$

where $c_1 = \dfrac{4}{\sqrt{7}-1}$. By Claim *iii)* of Lemma 30, the following holds :

$$\log \|F(z)\|_\nu \geq -[L \,:\, \mathbb{Q}](w + dht(z)),$$

whereas by Claim *ii)* of Lemma 30, we conclude that

$$\log \|DF(z)\|_\nu \leq \log(n^2 d) + [L \,:\, \mathbb{Q}]\left((d-1)ht(z) + w\right).$$

Thus, we obtain :

$$-[L \,:\, \mathbb{Q}](w + dht(z)) \leq \log(n^2 d) + [L \,:\, \mathbb{Q}]\left((d-1)ht(z) + w\right) + \log c_1 - \log \gamma_\nu(F,\zeta).$$

Hence we conclude :

$$\log \gamma_\nu(F,\zeta) - \log(n^2 d) - 2 - 2[L \,:\, \mathbb{Q}]w \leq (2d-1)[L \,:\, \mathbb{Q}]ht(z), \text{ and}$$

$$ht(z) \geq \frac{1}{2d-1}\left(\frac{\log \gamma_\nu(F,\zeta) - \log(n^2 d) - 2}{[L \,:\, \mathbb{Q}]} - 2w\right).$$

In particular, in the case where $L = \mathbb{Q}[i]$ is the field of Gaussian rationals, we can conclude the following lower bound :

$$ht(z) \geq \frac{1}{2d-1}\left(\frac{\log \gamma_\nu(F,\zeta) - \log(n^2 d) - 2}{2} - 2w\right).$$

On the other hand, using Proposition 33, and noting that the logarithmic height of the polynomials $f_1, \ldots, f_n$ is bounded by the logarithmic weight, from this lower bound one easily concludes the following inequality :

$$ht(z) \geq \frac{1}{2d-1}\left(\frac{\log d_\nu^{(F)}(DF(\zeta)^{-1}, \Sigma_\nu) - (d-1)(\log(n^2 d^3) + 2)}{(d-1)[L \,:\, \mathbb{Q}]} - 3w\right).$$

In the case of $L = \mathbb{Q}[i]$, this yields the following lower bound :

$$ht(z) \geq \frac{1}{2d-1}\left(\frac{\log d_\nu^{(F)}(DF(\zeta)^{-1}, \Sigma_\nu) - (d-1)(\log(n^2 d^3) + 2)}{2(d-1)} - 3w\right).$$

■

Let us remark that in these lower bounds the "positive part" is essentially $\log \gamma(F,\zeta)$, whereas the "negative part" is always bounded by the input length. This result helps interpreting our observations on the first example given on page 32 below.
In particular, we can conclude the validity of Theorem 4 (as given in the Introduction on page 6) by noting that the weight of a multivariate polynomial with integer coefficients of degree at most 2 is easily bounded in terms of its logarithmic height, namely :

$$wt(f_i) \leq 2\log n + ht(f_i)$$

It is worth observing that the same techniques also allow us to establish interesting results on the lower bound for sparse polynomials systems. This can be done in the following way :

Corollary 35 *Let $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ be a sequence of multivariate polynomials. Let us assume that the following properties hold :*

- *$d = \max\{\deg(f_i) \,:\, 1 \leq i \leq n\} \geq 2$,*

- *$ht(f_i) \leq w$, $1 \leq i \leq n$,*
- *The polynomials $f_1, \ldots, f_n$ have at most M non–zero coefficients.*

Let $\zeta \in V_K(f_1, \ldots, f_n)$ be a smooth $K-$rational point of the system $F := (f_1, \ldots, f_n)$. Let $|\cdot|_\nu : K \longrightarrow \mathbb{R}_+$ be an absolute value defined on K, and let $L \subseteq K$ be a number field such that $\zeta \in L_\nu^n$. Then, for every $z \in L^n$, $z \neq \zeta$ satisfying

$$||z - \zeta||_\nu \gamma_\nu(F, \zeta) \leq \frac{3 - \sqrt{7}}{2},$$

the following inequality holds :

$$ht(z) \geq \frac{1}{2d-1} \left(\frac{\log \gamma_\nu(F, \zeta) - \log(n^2 d) - 2}{[L \,:\, \mathbb{Q}]} - 2(\log M + h) \right).$$

With the same assumptions also holds

$$ht(z) \geq \frac{1}{2d-1} \left(\frac{\log d_\nu^{(F)}(DF(\zeta)^{-1}, \Sigma_\nu) - (d-1)(\log(n^2 d^3) + 2)}{(d-1)[L \,:\, \mathbb{Q}]} - 3(\log M + h) \right).$$

Moreover, in the case where $L = \mathbb{Q}[i]$ is the field of Gaussian rationals, the two previous lower bounds may be rewritten as :

$$ht(z) \geq \frac{1}{2d-1} \left(\frac{\log \gamma_\nu(F, \zeta) - \log(n^2 d) - 2}{2} - 2(\log M + h) \right), \text{ and}$$

$$ht(z) \geq \frac{1}{2d-1} \left(\frac{\log d_\nu^{(F)}(DF(\zeta)^{-1}, \Sigma_\nu) - (d-1)(\log(n^2 d^3) + 2)}{2(d-1)} - 3(\log M + h) \right).$$

Now we will show Proposition 5 from page 7 of the Introduction. Let us recall that statement :

Proposition 36 *With the notations and assumptions introduced in Section 1, let $F := (f_1, \ldots, f_n)$ be a sequence of $n-$variate polynomials with integer coefficients defining a zero–dimensional algebraic variety $V(f_1, \ldots, f_n)$, and let $\zeta \in V_K(f_1, \ldots, f_n) \cap \mathbb{Z}_K^n$ be a smooth $K-$rational point whose entries are algebraic integers. Let us also assume that for every archimedean absolute value $|\cdot|_\nu$ (i. e. $\nu \in S$), the following holds :*

$$3\|\zeta\|_\nu \gamma_\nu(F, \zeta) \geq 3 - \sqrt{7}.$$

Then the average height of any approximate zero $z \in \mathbb{Q}[i]^{nD}$ of the system F with associate variety V_ζ that satisfies the $\gamma-$Theorem, also satisfies the following inequality :

$$ht_{av}(z) \geq \frac{1}{2} \left[ht(\zeta) - (\frac{1}{2} \log n + \log 2) \right].$$

Proof.– Let us denote by $V_\zeta \subseteq V(f_1, \ldots, f_n)$ the $\mathbb{Q}-$definable irreducible component of $V(f_1, \ldots, f_n)$ containing ζ. Let $D := \deg(V_\zeta)$ and $V_\zeta := \{\zeta_1, \ldots, \zeta_D\}$. Let us write $z := (z_1, \ldots, z_D) \in \mathbb{Q}[i]^{nD}$, such that for every i, $1 \leq i \leq D$, the following inequalities hold :

$$\|z_i - \zeta_i\| \leq \frac{3 - \sqrt{7}}{2\gamma(F, \zeta_i)},$$

where $\|\cdot\| \;: K^n \longrightarrow \mathbb{R}$ is the standard hermitian norm induced by the inclusion $\iota \;: K \hookrightarrow \mathbb{C}$. Thus, we conclude that for every i, $1 \leq i \leq D$, the following inequality holds :

$$\|z_i\| \geq \|\zeta_i\| - \frac{3 - \sqrt{7}}{2\gamma(F, \zeta_i)}.$$

Without loss of generality, let us assume that $K = K(\zeta) = K(V_\zeta)$, and let $D := [K : \mathbb{Q}]$. Let us also consider the class of all $\mathbb{Q}-$ embeddings of K in $\mathbb{C}$, i.e. $\sigma_1, \ldots, \sigma_D : K \hookrightarrow \mathbb{C}$. In a slight abuse of notation, we also use $\sigma_1, \ldots, \sigma_D$ to denote the corresponding embeddings of the affine space K^n in $\mathbb{C}^n$, namely

$$\sigma_1, \ldots, \sigma_D : K^n \hookrightarrow \mathbb{C}^n.$$

Thus, we have $V_\zeta := \{\sigma_1(\zeta), \ldots, \sigma_D(\zeta)\}$, and we may conclude that for every i, $1 \leq i \leq D$, the following inequality holds :

$$\|z_i\| \geq \|\sigma_i(\zeta)\| - \frac{3-\sqrt{7}}{2\gamma(F, \sigma_i(\zeta))}. \tag{5}$$

Moreover, for every i, $1 \leq i \leq D$, there exists an archimedean absolute value $\nu_i \in S$, such that the following two equalities hold :

- $\|\zeta_i\| = \|\sigma_i(\zeta)\| = \|\zeta\|_{\nu_i}$,
- $\gamma(F, \zeta_i) = \gamma(F, \sigma_i(\zeta)) = \gamma_{\nu_i}(F, \zeta)$.

Our hypothesis on ζ would obviously imply for every i, $1 \leq i \leq D$ the following inequality :

$$\|\zeta_i\| - \frac{3-\sqrt{7}}{2\gamma(F, \zeta_i)} \geq \frac{1}{2}\|\zeta\|_{\nu_i}.$$

Thus, we conclude that for every i, $1 \leq i \leq D$ holds :

$$\|z_i\| \geq \frac{1}{2}\|\zeta\|_{\nu_i}.$$

Let us denote $z_i := (z_{i,1}, \ldots, z_{i,n}) \in \mathbb{Q}[i]^n$ for every i, $1 \leq i \leq D$. Then, we may conclude the following inequality :

$$\sqrt{n}\max\{1, |z_{i,1}|, \ldots, |z_{i,n}|\} \geq \frac{1}{2}\|\zeta\|_{\nu_i},$$

which implies that for every i, $1 \leq i \leq D$ holds :

$$\log\left(\sqrt{n}\max\{1, |z_{i,1}|, \ldots, |z_{i,n}|\}\right) \geq ht_{\nu_i}(\zeta) - \log 2. \tag{6}$$

This implies $2ht(z_i) + \frac{1}{2}\log n \geq ht_{\nu_i}(\zeta) - \log 2$. Adding all these quantities, we obtain the following inequality :

$$2\left(\sum_{i=1}^{D} ht(z_i)\right) \geq \left(\sum_{i=1}^{D} ht_{\nu_i}(\zeta)\right) - D\left(\frac{1}{2}\log n + \log 2\right),$$

or equivalently, the following inequality :

$$2\left(\sum_{i=1}^{D} ht(z_i)\right) \geq \left(\sum_{\nu \in S} n_\nu ht(\zeta)\right) - D\left(\frac{1}{2}\log n + \log 2\right).$$

Finally, since $D = [K : \mathbb{Q}]$ and $\zeta \in \mathbb{Z}_K^n$, we conclude that

$$ht_{av}(z) \geq \frac{1}{2}\left[ht(\zeta) - \left(\frac{1}{2}\log n + \log 2\right)\right],$$

as desired. ■

The proof of Corollary 5 on page 7 of the Introduction follows a similar sequence of arguments. We reproduce the statement here and show how it can be proved.

Corollary 37 *With the same notations as in Proposition 36, let $\zeta \in \mathbb{Z}_K^n \cap V_K(f_1, \ldots, f_n)$ be a smooth $K-$rational zero of the system $F := (f_1, \ldots, f_n)$ and let us assume that for every archimedean absolute value $|\cdot|_\nu \, : K \longrightarrow \mathbb{R}$ (i. e. for every $\nu \in S$), the following holds :*

$$\gamma_\nu(F, \zeta) \geq \frac{3-\sqrt{7}}{2}.$$

Then the average height of any approximate zero $z \in \mathbb{Q}[i]^{nD}$ of the system F with associate variety V_ζ that satisfies the $\gamma-$Theorem, also satisfies the following inequality :

$$ht_{av}(z) \geq \frac{1}{2}\left[ht(\zeta) - (\frac{1}{2}\log n + \log 2)\right].$$

Proof.– Using the same notations and steps as in the proof of the Proposition 36 on page 29, we obtain the following inequalities for every i, $1 \leq i \leq D$ (cf. inequality 5 on page 30) :

$$\|z_i\| \geq \|\zeta\|_{\nu_i} - \frac{3-\sqrt{7}}{2\gamma_{\nu_i}(F,\zeta)}.$$

Now, provided that $\|\zeta\|_{\nu_i} \geq 1$, since $\gamma_{\nu_i}(F,\zeta) \geq \frac{3-\sqrt{7}}{2}$, we conclude that :

$$3\|\zeta\|_{\nu_i} \geq 3 - \sqrt{7}.$$

Hence,

$$\|z_i\| \geq \|\zeta\|_{\nu_i} - \frac{3-\sqrt{7}}{2\gamma_{\nu_i}(F,\zeta)} \geq \frac{1}{2}\|\zeta\|_{\nu_i}.$$

In this case, we may conclude (as in inequality 6 above) the following inequality :

$$\log\left(\sqrt{n}\max\{1, |z_{i,1}|, \ldots, |z_{i,n}|\}\right) \geq ht_{\nu_i}(\zeta) - \log 2.$$

Otherwise, if $\|\zeta\|_{\nu_i} \leq 1$, the following inequality obviously holds :

$$\log\left(\sqrt{n}\max\{1, |z_{i,1}|, \ldots, |z_{i,n}|\}\right) \geq ht_{\nu_i}(\zeta) - \log 2.$$

Thus, to complete the proof, one proceeds as in the proof of the Proposition 5 on page 29. ■

Let us recall Corollary 7 from page 8 of the Introduction before proving it :

Corollary 38 *Let $F := (f_1, \ldots, f_n)$ be a system of multivariate polynomials with integer coefficients satisfying the conditions i) to v) given on page 3. Let $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathbb{Z}_K^{n+1} \cap V_K(f_1, \ldots, f_n)$ be a smooth $K-$rational zero whose coordinates are algebraic integers. Let us now define the system of polynomial equations in $n+1$ variables :*

$$G := (g_1, \ldots, g_{n+1}) \in \left(\mathbb{Z}[X_1, \ldots, X_{n+1}]\right)^{n+1},$$

given by the following rules :

- $g_i := f_i \in \mathbb{Z}[X_1, \ldots, X_{n+1}]$ *for every* i, $1 \leq i \leq n$,
- $g_{n+1} := (X_{n+1} - X_n)(X_{n+1} - (X_n + 1))$.

Let $\zeta' \in V_K(g_1, \ldots, g_{n+1}) \cap \mathbb{Z}_K^{n+1}$ be the affine point given by

$$\zeta' := (\zeta_1, \ldots, \zeta_n, \zeta_n) \in \mathbb{Z}_K^{n+1}.$$

Let $V_{\zeta'} \subseteq V(g_1, \ldots, g_{n+1})$ be the $\mathbb{Q}-$definable irreducible component of $V(g_1, \ldots, g_{n+1})$ containing ζ'. Then the average height of any approximate zero $z \in \mathbb{Q}[i]^{(n+1)D}$ of the system F with associate variety $V_{\zeta'}$ that satisfies the $\gamma-$Theorem, also satisfies the following inequality :

$$ht_{av}(z) \geq \frac{1}{2}\left[ht(\zeta) - (\frac{1}{2}\log(n+1) + \log 2)\right].$$

Proof.– Let us consider the two affine points in $V(g_1,\ldots,g_{n+1})\cap\mathbb{Z}_K^{n+1}$ given by

$$\zeta' := (\zeta_1,\ldots,\zeta_n,\zeta_n)\in\mathbb{Z}_K^{n+1},\ \text{and}\zeta” := (\zeta_1,\ldots,\zeta_n,\zeta_{n+1})\in\mathbb{Z}_K^{n+1}.$$

We make use of Inequality 4 on page 26 to conclude that for every archimedean absolute value $\nu\in M_K$, the following holds :

$$1=\|\zeta'-\zeta”\|_\nu\geq\frac{3-\sqrt{7}}{2\gamma_\nu(G,\zeta')}.$$

In particular, we conclude that for every archimedean absolute value $\nu\in S$ holds :

$$\gamma_\nu(G,\zeta')\geq\frac{3-\sqrt{7}}{2}.$$

Now, let us assume $D:=\deg(V_{\zeta'})=[K\ :\ \mathbb{Q}]$ and $V_{\zeta'}:=\{\zeta'_1,\ldots,\zeta'_D\}$. Let $\sigma_1,\ldots,\sigma_D\ :K\hookrightarrow\mathbb{C}$ be the set of $\mathbb{Q}-$embeddings of K in $\mathbb{C}$ and let us denote accordingly $\sigma_1,\ldots,\sigma_D\ :K^n\hookrightarrow\mathbb{C}^n$. Then $V_{\zeta'}:=\{\sigma_1(\zeta'),\ldots,\sigma_D(\zeta')\}$, and for every i, $1\leq i\leq D$, there exists $\nu_i\in S$ such that :

- $\|\zeta'_i\|=\|\sigma_i(\zeta')\|=\|\zeta'\|_{\nu_i}$ and
- $\gamma(F,\zeta'_i)=\gamma(F,\sigma_i(\zeta'))=\gamma_{\nu_i}(F,\zeta')$.

Now, if $\|\zeta'\|_{\nu_i}\geq 1$, we obviously have

$$3\|\zeta'\|_{\nu_i}\gamma_{\nu_i}(F,\zeta')\geq 3\left(\frac{3-\sqrt{7}}{2}\right)\geq 3-\sqrt{7}.$$

Following the same steps as in the proof of Proposition 5 on page 29 above, we may conclude that the following inequality holds for $\|\zeta'\|_{\nu_i}\geq 1$ (recall Inequality 6 from page 30) :

$$\log\left(\sqrt{n+1}\max\{1,|z_{i,1}|,\ldots,|z_{i,n+1}|\}\right)\geq ht_{\nu_i}(\zeta')-\log 2=ht_{\nu_i}(\zeta)-\log 2.$$

On the other hand, the same inequality also holds for $\|\zeta'\|_{\nu_i}\leq 1$. Thus, we proceed again as in the proof of Proposition 5 on page 29. ■

3.2.1 Examples

The following examples illustrate how the previous lower bounds for the bit length of approximate zeros apply. We start with an example inspired by a classical univariate example due to M. Mignotte (cf. [Mig89]) :

Example 1 (Using $\log\gamma$ as in Theorem 34) *Let us consider the system of multivariate polynomials $F:=(f_1,\ldots,f_{n+1})$ given by the following rules :*

- $f_1:=X_1-2$,
- $f_i:=X_i-X_{i-1}^2$ *for every i, $2\leq i\leq n-1$,*
- $f_n:=X_{n+1}-X_n^2$,
- $f_{n+1}:=X_{n+1}X_n-2(X_{n-1}X_n-1)^2$.

This system F has three solutions in $\mathbb{C}^{n+1}$, where two of them, say $\zeta_1,\zeta_2\in\mathbb{R}^{n+1}$, satisfy the following inequality :

$$\|\zeta_1-\zeta_2\|\leq\frac{2}{2^{\frac{5\cdot 2^{n-2}}{2}}}\leq\frac{2}{2^{2^{n-1}}}.$$

Thus, using Inequality 4 from page 26, we may conclude :

$$\frac{2}{2^{2^{n-1}}} \geq \|\zeta_1 - \zeta_2\| \geq \frac{3-\sqrt{7}}{2\gamma(F,\zeta_i)}.$$

By the first lower bound given in Theorem 34 on page 27, we conclude that for all approximate zeros $z_1, z_2 \in \mathbb{Q}[i]^{n+1}$ *of the system* F *associated to* ζ_1, ζ_2 *respectively and satisfying the corresponding* $\gamma-$*Theorem, the following holds :*

$$ht(z_i) \geq \frac{1}{6}\left(\log \gamma(F,\zeta_i) - 2\log(n+1)\right) - O(1) \geq \frac{1}{6}\left(2^{n-1} - 2\log(n+1)\right) - O(1).$$

and that they require exponential bit length, both for binary or continuous fraction encodings. Floating point encoding also requires an exponential number of digits.
Let us observe that alternative examples with low separation between the roots can be easily obtained without using Mignotte's example. Consider for example the following system $F := (f_1, \ldots, f_n)$ *given by :*

- $f_1 := 2X_1 - 1$,
- $f_i := X_i - X_{i-1}^2$, *for every* i, $2 \leq i \leq n-1$,
- $f_n := X_n(X_n - X_{n-1})$.

This system has two distinct solutions $\zeta_1 \neq \zeta_2$ *at a distance* $\|\zeta_1 - \zeta_2\| \leq \frac{1}{2^{2^{n-2}}}$, *and the same lower bound applies.*

Example 2 (Using $\log d^{(F)}(DF(\zeta)^{-1}, \Sigma)$ as in Theorem 34) *Let us consider the system of multivariate polynomial equations* $F := (f_1, \ldots, f_{n+1})$ *given by the following rules :*

- $f_1 := X_{n+1}(2X_1 - 1)$,
- $f_i := X_{n+1}(X_i - X_{i-1}^2)$, *for every* i, $2 \leq i \leq n$,
- $f_{n+1} := X_{n+1}^2 - X_n^2$.

We consider the solution of this system given by :

$$\zeta := \left(\frac{1}{2}, \frac{1}{2^2}, \ldots, \frac{1}{2^{2^{n-1}}}, \frac{1}{2^{2^{n-1}}}\right).$$

Thus, we consider the Jacobian matrix of the system F *at* ζ, *i.e.*

$$DF(\zeta) := \left(\frac{\partial f_i}{\partial X_j}(\zeta)\right)_{1 \leq i,j \leq n+1}.$$

The entries of this non–singular matrix are given by the following rules :

$$\begin{array}{ll}
\textit{If } j = i \leq n, & \dfrac{\partial f_i}{\partial X_j}(\zeta) = \dfrac{1}{2^{2^{n-1}}}, \\
\textit{if } 1 \leq j = i-1,\ i \leq n, & \dfrac{\partial f_i}{\partial X_j}(\zeta) = \dfrac{-2}{2^{2^{n-1}+2^{j-1}}}, \\
\textit{if } j = n,\ i = n+1, & \dfrac{\partial f_{n+1}}{\partial X_n}(\zeta) = \dfrac{-2}{2^{2^{n-1}}}, \\
\textit{if } j = i = n+1, & \dfrac{\partial f_{n+1}}{\partial X_{n+1}}(\zeta) = \dfrac{2}{2^{2^{n-1}}}, \\
\textit{and otherwise} & \dfrac{\partial f_i}{\partial X_j}(\zeta) = 0.
\end{array}$$

We conclude that : $\|DF(\zeta)\| \leq \|DF(\zeta)\|^{(F)} \leq \dfrac{2(n+1)^2}{2^{2^{n-1}}}$.

Thus holds : $\dfrac{2^{2^{n-1}}}{2(n+1)^2} \leq \dfrac{1}{\|DF(\zeta)\|} = d^{(F)}(DF(\zeta^{-1}, \Sigma)$.

Now, using the lower bound shown in Theorem 34 on page 27 with $d = 3$, $w = \log 3$ *and* $n = n+1$, *we conclude that for every* $z \in \mathbb{Q}[i]^{n+1}$ *satisfying the* $\gamma-$*Theorem with associate zero* ζ, *the following inequality holds :*

$$ht(z) \geq \frac{1}{20}\left(2^{n-1} - 6\log(n+1)\right) - 2.$$

As mentioned in the Introduction on page 8, the same comments also show the validity of Corollaries 8, 9 and 10.

Example 3 (Using Proposition 5 or Corollary 7) *Consider the following sequence of multivariate polynomials* $F := (f_1, \ldots, f_{n+1})$ *given by the following rules :*

- $f_1 := X_1 - 2$,
- $f_i := X_i - X_{i-1}^2$, *for every* i, $2 \leq i \leq n$,
- $f_{n+1} := (X_{n+1} - X_n)(X_{n+1} - (X_n + 1))$.

This system has two solutions $\zeta_1, \zeta_2 \in \mathbb{Z}^{n+1}$, *which can be described as follows :*

$$\zeta_1 := \left(2, 2^2, \ldots, 2^{2^{n-1}}, 2^{2^{n-1}}\right) \in \mathbb{Z}^{n+1} \text{ and } \zeta_2 := \left(2, 2^2, \ldots, 2^{2^{n-1}}, 1 + 2^{2^{n-1}}\right).$$

By Inequality 4 on page 26, we may conclude that for $i = 1, 2$ *holds :*

$$1 := \|\zeta_1 - \zeta_2\| \geq \frac{3 - \sqrt{7}}{2\gamma(F, \zeta_i)}.$$

In particular, since $3\|\zeta_i\|\gamma(F, \zeta_i) \geq 3 - \sqrt{7}$, *we may apply either Corollary 7 or Proposition 5 to conclude that for every* $z_1, z_2 \in \mathbb{Q}[i]^{n+1}$ *satisfying the* $\gamma-$*Theorem with associate zero* ζ_1 *and* ζ_2 *respectively, the following holds :*

$$ht(z_i) \geq \frac{1}{2}\left[2^{n-1} - \log(n+1) - \log 2\right].$$

Again, Corollaries 8, 9 and 10 follow from this example.

3.3 Approximate zero theory : Upper bounds for the bit length of approximate zeros

Here we show the statements of the Introduction concerning upper bounds for the bit length of approximate zeros. We start with the following statement and then show Theorem 11 from page 9 of the Introduction.

Theorem 39 (Upper bounds for $\gamma(F, \zeta)$) *Let* $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ *be polynomials with integer coefficients. Let us assume that the following properties hold*

- $d := \max\{\deg(f_i) \ : \ 1 \leq i \leq n\}$,
- $wt(f_i) \leq w$, $1 \leq i \leq n$.

Let $\zeta \in V_K(f_1, \ldots, f_n)$ *be a smooth* $K-$*rational point. Let* $|\cdot|_\nu \ : K \longrightarrow \mathbb{R}_+$ *be an absolute value on* K. *Thus, the following inequality holds :*

$$\log \gamma_\nu(F, \zeta) \leq [K \ : \ \mathbb{Q}](t+1)\left(t^2 + 8\log t + 2w + t ht(\zeta)\right),$$

where $t := \max\{d, n\} \geq 2$.

Proof.– First of all, using Claim *iv*) of Lemma 29 on page 22, the following inequality holds :

$$\gamma_\nu(F,\zeta) \leq \max_{k\geq 2}\left(\|(DF(\zeta))^{-1}\|_\nu \left\| \frac{D^{(k)}F(\zeta)}{k!} \right\|_\nu \right)^{\frac{1}{k-1}}.$$

By Claim *v*) of Lemma 29 the following holds :

$$\|DF(\zeta)^{-1}\|_\nu = \frac{1}{d_\nu^{(F)}(DF(\zeta,\Sigma)} \leq \frac{\|DF(\zeta)\|_\nu^{n-1}}{|\det(DF(\zeta)|_\nu}.$$

By Claim *iii*) of Lemma 30, we obtain :

$$\log|\det(DF(\zeta))|_\nu \geq -[K\ :\ \mathbb{Q}]n\left(\log n + ht(DF(\zeta))\right).$$

Now, using Lemma 28, we have :

$$ht(DF(\zeta)) \leq n^2 + \max\{ht\left(\frac{\partial f_i}{\partial X_j}(\zeta)\right)\ :\ 1\leq i,j\leq n\}.$$

Thus, we may use Claim *i*) of Lemma 30 to conclude :

$$\max\{ht\left(\frac{\partial f_i}{\partial X_j}(\zeta)\right)\ :\ 1\leq i,j\leq n\} \leq w + \log d + (d-1)ht(\zeta).$$

This chain of inequalities yields :

$$-\log|\det(DF(\zeta)|_\nu \leq [K\ :\ \mathbb{Q}]n\left(n^2 + \log n + w + \log d + (d-1)ht(\zeta)\right).$$

On the other hand, using Claim *ii*) of Lemma 30, we have :

$$\log\|DF(\zeta)\|_\nu \leq \log(n^2d) + [K\ :\ \mathbb{Q}]\left(w + (d-1)ht(\zeta)\right).$$

Moreover, using Claim *iii*) of Lemma 29, we obtain :

$$\begin{aligned}\log\|\frac{D^{(k)}F(\zeta)}{k!}\|_\nu \leq{} & (k+1)\log n \\ & +[K\ :\ \mathbb{Q}]\max\{ht\left(\frac{1}{k!}\frac{\partial^{|\mu|}f_i}{\partial \underline{X}^\mu}(\zeta)\right)\ :\ \mu\in\mathbb{N}^n, |\mu|=k, 1\leq i\leq n\}.\end{aligned}$$

Now, using Claim *i*) of Lemma 30 on page 22, we conclude that for every multi–index $\mu\in\mathbb{N}^n$, $|\mu|=1$ and for every i, $1\leq i\leq n$, the following holds :

$$ht\left(\frac{1}{k!}\frac{\partial^{|\mu|}f_i}{\partial \underline{X}^\mu}(\zeta)\right) \leq k\log k + d\log d + w + (d-1)ht(\zeta).$$

Thus, adding all these quantities, we obtain :

$$\log\|\frac{D^{(k)}F(\zeta)}{k!}\|_\nu \leq [K\ :\ \mathbb{Q}]\left(2(d+1)\log n + 2d\log d + w + (d-1)ht(\zeta)\right).$$

Thus, taking $t := \max\{d,n\}\geq 2$, we conclude :

$$\log\gamma_\nu(F,\zeta) \leq \Big([K\ :\ \mathbb{Q}]\left(4(t+1)\log t + w + (t-1)ht(\zeta)\right) - \log d_\nu^{(F)}(DF(\zeta)^{-1},\Sigma)\Big).$$

Finally, combining all upper bounds above, we may conclude :

$$\log\gamma_\nu(F,\zeta) \leq [K\ :\ \mathbb{Q}](t+1)\left(t^2 + 8\log t + 2w + tht(\zeta)\right).$$

■

Theorem 40 (Lower bounds for γ) *With the same assumptions and notations as in Theorem 39 above, the following holds :*

$$\log \gamma_\nu(F,\zeta) \geq -\left(\frac{3}{d-1}\right)[K:\mathbb{Q}](\log n + w + d^2(ht(\zeta))).$$

Proof.– First of all, the following obvious inequality holds :

$$\gamma_\nu(F,\zeta) \geq \frac{\|D^{(d)}F(\zeta)\|_\nu^{\frac{1}{d-1}}}{\|DF(\zeta)\|_\nu^{\frac{1}{d-1}}}.$$

From Lemma 30, Claim *ii*) the following holds :

$$-\frac{1}{d-1}\log\|DF(\zeta)\| \geq \frac{-1}{d-1}\log(n^2d) + [K:\mathbb{Q}](w + (d-1)ht(\zeta)).$$

From Lemma 30, Claim *iii*) we also have :

$$\log\|D^{(d)}F(\zeta)\| \geq -[K:\mathbb{Q}](d\log d + w + dht(\zeta))$$

Combining both inequalities we can conclude the inequality stated at the Theorem. ■

Remark 41 *Using [BCSS98a, Proposition 3, p. 50] the previous upper and lower bounds may also be written in the terms of the height of the approximate zero. With the same notations and assumptions as in Theorem 39 let $z \in \mathbb{Q}[i]^n$ be an approximate zero of system F satisfying the following inequality :*

$$\|z-\zeta\|_\nu \leq \frac{3-\sqrt{7}}{2\gamma_\nu(F,\zeta)}$$

First of all, the following two inequalities hold :

$$\log\gamma_\nu(F,z) \leq \left((t+1)\left(t^2 + 8\log t + 2w + tht(z)\right)\right),$$

$$\log\gamma_\nu(F,z) \geq -\left(\frac{3}{d-1}\right)2(\log n + w + d^2(ht(z)))$$

where $t := \max\{d,n\} \geq 2$. Now, we apply [BCSS98a, Proposition 3, p. 50] to conclude :

$$\log\gamma_\nu(F,\zeta) \leq c\log\gamma_\nu(F,z) \leq c'\log\gamma_\nu(F,\zeta),$$

where $c, c' > 0$ are universal constants. In particular, we also conclude the following lower bound for the height of the approximate zero :

$$ht(z) \geq \Omega\left(\frac{\log\gamma_\nu(F,\zeta) - (t+1)(t^2 + 8\log t + 2w)}{t(t+1)}\right).$$

Let us observe the analogies between this lower bound and those stated at Theorem 4 above.

Once again, we can conclude the validity of Theorem 11 as given in the Introduction, since it is a particular case of the Theorem above. Now we are in condition to show Corollary 12 from page 9 of the Introduction. Let us recall that statement :

Corollary 42 (Upper bound on the bit length of approximate zeros) *With the same assumptions and notations as in Theorem 11, let $\zeta \in V_K(f_1, \ldots, f_n)$ be a smooth $K-$rational zero, and let $|\cdot|_\nu$ be an absolute value on K. Let $L \subseteq K$ be a number field such that $\zeta \in L_\nu^n$. Then there exist approximate zeros $z \in L^n$ of the system $F := (f_1, \ldots, f_n)$ with approximate zero ζ with respect to the absolute value $|\cdot|_\nu$, such that the logarithmic height $ht(z)$ of z is at most linear in the following quantities :*

$$\frac{1}{[L\ :\ \mathbb{Q}]}\log|\Delta_L| + [K\ :\ \mathbb{Q}]t\left(t^2 + w + tht(\zeta)\right),$$

where w is an upper bound for the logarithmic weight of the polynomials $f_1, \ldots, f_n$, $t := \max\{d, n\}$, and $|\Delta_L|$ is the absolute value of the discriminant of the field L.
Moreover, in the case where $L = \mathbb{Q}[i]$ (for instance, if $|\cdot|_\nu$ is archimedean), there exist approximate zeros $z \in \mathbb{Q}[i]^n$ for the system F with associate zero ζ with respect to $|\cdot|_\nu$, such that their bit length is at most linear in the following quantity :

$$[K\ :\ \mathbb{Q}]t\left(t^2 + w + tht(\zeta)\right),$$

in other words :

$$ht(z) \leq c_1[K\ :\ \mathbb{Q}]t\left(t^2 + w + tht(\zeta)\right).$$

where $c_1 > 0$ is a small universal constant.

This statement follows immediately from the upper bounds for $\gamma_\nu(F, \zeta)$ described in Theorem 39 above, together with the following two statements on the classical Dirichlet Theorem. The first statement is an extension of the classical Dirichlet Theorem to the case of archimedean absolute values (cf. [Sch80, Cas97] for instance) :

Theorem 43 (Archimedean Dirichlet Theorem, 1842) *Suppose given $n{\cdot}m$ real numbers α_{ij} $(1 \leq i \leq n, 1 \leq j \leq m)$ and that $Q > 1$ is an integer. Then, there exist integers $q_1, \ldots, q_m, p_1, \ldots, p_n$ with :*

$$1 \leq \max(|q_1|, \ldots, |q_m|) < Q^{\frac{n}{m}},$$

$$|\alpha_{i1}q_1 + \ldots + \alpha_{im}q_m - p_i| \leq \frac{1}{Q}\ (1 \leq i \leq n).$$

On the other hand, for non–archimedean absolute values, we made use of the following statement. A proof can be found in [BVdPV96] or [Tyl94].

Theorem 44 (Non–archimedean Dirichlet Theorem) *Let K be a number field and $\nu \in M_K \setminus S$ a non–archimedean absolute value defined on K. Let $\zeta \in K_\nu$ be a point in the completion of K with respect to $|\cdot|_\nu$. Then, for every $\tau \in K_\nu$, $1 \leq |\tau|_\nu$, there exists $z \in K$, such that the following holds :*

i) $ht(z) \leq \dfrac{1}{2[K\ :\ \mathbb{Q}]}\log|\Delta_L| + \log|\tau|_\nu + \log c,$

ii) $|\zeta - z|_\nu \leq \dfrac{|\Delta_K|^{\frac{1}{2[H\ :\ \mathbb{Q}]}}e^{c+ht(\zeta)}}{|\tau|_\nu}.$

Thus, taking either sufficiently big denominators (for the archimedean case) or τ such that $|\tau|_\nu$ is big enough (for the non–archimedean case), Corollary 12 follows.
To conclude the statements claimed at the Introduction, let us say that the Universal $\gamma-$Theorem (Corollary 14 stated at the Introduction) follows obviously as a consequence of Theorem 2 and the universal condition number is well–defined as a consequence of Theorem 39 on page 34 above.
Finally, we have to prove Corollary 15. We recall that statement from page 10 of the Introduction :

Corollary 45 *Let $F := (f_1, \ldots, f_n)$ be a sequence of multivariate polynomials with integer coefficients satisfying conditions i) to v) stated on page 3 of the Introduction. Let $\zeta \in V_K(f_1, \ldots, f_n)$ a smooth $K-$rational zero. The only point $z \in K^n$ which satisfies the Universal $\gamma-$Theorem near γ for all absolute values in M_K is $z = \zeta$. Namely, for every $z \in K^n$ satisfying for every $\nu \in M_k$ the following inequality*

$$\|z - \zeta\|_\nu \leq \frac{3 - \sqrt{7}}{2\widetilde{\gamma}(F, \zeta)}$$

holds $z = \zeta$.

Proof.– First, let us consider $z \in K^n$, such that for every absolute value $\nu \in M_K$ holds :

$$\|z - \zeta\|_\nu \leq \frac{3 - \sqrt{7}}{2\widetilde{\gamma}(F, \zeta)}.$$

As $\widetilde{\gamma}(F, \zeta) \geq 1$, we easily conclude that for all non–archimedean absolute values $\nu \in M_K \setminus S$ holds $\|z - \zeta\|_\nu \leq 1$. In particular, the coordinates of the affine point $z - \zeta$ are algebraic integers in K, i.e. $z - \zeta \in \mathbb{Z}_K^n$.
On the other hand, for archimedean absolute values holds $\|z - \zeta\|_\nu \leq 1$, and hence, we obtain :

$$e^{ht(z-\zeta)} \leq \left(\prod_{\nu \in S} \|z - \zeta\|_\nu^{n_\nu} \right)^{\frac{1}{[K \,:\, \mathbb{Q}]}} < 1.$$

This last condition can only be satisfied, if $z - \zeta = 0 \in K^n$ and thus the claim follows. ■

4 Kronecker's approach to solving

In this Section we prove Theorems 18, 19, 20 as stated in the Introduction. To this end, we have divided this Section into three main parts.

- An improvement of the Witness Theorem. In this Subsection we introduce some standard notations concerning straight–line programs encoding of multivariate polynomials. We also show an improvement of the Witness Theorem of [BCSS98b, BCSS98a] using parallel complexity estimates.
- From Kronecker's to Newton's solution. In this Subsection we show Theorem 20. In fact, using the main statement of [GHMP95, Par95, GHM$^+$98, GHH$^+$97, GHMP97], this Theorem is established by exhibiting a procedure that transforms a Kronecker description of a solution variety into a list of approximates zeros of bounded height.
- From Newton's to Kronecker's solution. In this Subsection we show Theorem 19, exhibiting a procedure that transforms approximate zeros into a Kronecker description of a certain $\mathbb{Q}$–definable irreducible component of a solution variety.

4.1 An improvement of the Witness Theorem

In the sequel we will work with the complexity model of non–scalar straight–line programs (see for instance [Hei89, Str90, Par95, MPR91] or [KP96]) : a non–scalar straight–line program is a structure which evaluates (and hence represents) a given polynomial of $K[X_1, \ldots, X_n]$, taking K–linear operations for free.

Remark 46 *We shall tacitly assume that our straight–line programs do not contain any divisions.*

We represent a straight–line program for the evaluation of a polynomial $P \in K[X_1, \ldots, X_n]$ by a *directed acyclic graph* $\mathcal{G}$ whose nodes are labeled gates which perform arithmetical operations. Therefore we identify the nodes of $\mathcal{G}$ with the corresponding gates. The graph $\mathcal{G}$ disposes of $n+1$ particular nodes labeled by the variables $X_1, \ldots, X_n$ and the constant 1. These nodes are called the input gates of $\mathcal{G}$. We define the depth of a gate ν of our graph as the length of the longest path which joins ν with some input gate. Let us denote the gates of the directed acyclic graph by pairs of integer numbers (i, j), where i represents the depth of the gate and j is the corresponding value of an arbitrary numbering imposed to the set of gates of depth i (this notation for the analysis of parallel complexity has been inspired by [MP93] and [MMP96]).

Definition 47 (Non-scalar straight–line program) *A* division-free non–scalar straight–line program *with inputs $X_1, \ldots, X_n$ is a pair $\Gamma := (\mathcal{G}, Q)$, where $\mathcal{G}$ is a directed acyclic graph, with $n+1$ input gates, unbounded fan–in, and Q is a function that assigns to every gate (i, j) one of the following instructions :*

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

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

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

Observe that the rather complicated notation in Definition 47 (non–scalar straight–line program) arises from the fact that a single non–scalar node in the graph represents the total of all scalar (i.e. K–linear) operations contributing to this node.

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

$$Q_{i,j} = \sum_{|\mu| \leq 2^i} Q_{i,j}^{\mu}(\underline{A}, \underline{B}) \, X_1^{\mu_1} \ldots X_n^{\mu_n}. \tag{7}$$

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

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

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

$$P(X_1, \ldots, X_n) = Q_{i,j}(\underline{\alpha}, \underline{\beta}, X_1, \ldots, X_n). \tag{8}$$

Taking into account the representation of (7) we can rewrite Identity (8) as :

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

for all μ with $|\mu| \le 2^i$ and $P_\mu = 0$ for $|\mu| > 2^i$. Let us remark that the *degree of such a polynomial* $P = Q_{i,j}(\underline{\alpha}, \underline{\beta}, X_1, \ldots, X_n)$ is generically equal to 2^i in the space of parameters.
Finally, we say that $P \in K[X_1, \ldots, X_n]$ is computable by a straight–line program Γ with parameters in the finite set $\mathcal{F} := \{\alpha_{ij}^{rs}, \beta_{ij}^{r's'}\}$.
Here we resume how these notions and the logarithmic height (Subsection 2.1.3) relate, by establishing bounds for polynomials given by straight–line programs using the different notions of height.
First of all, we can easily bound the number of parameters used by a non–scalar straight–line program Γ of size L in n variables by $2L(L-(n+1))$.
The following Lemma relates the notions of height and weight with the notions of size, non–scalar depth and height of the parameters used in a straight–line program.

Lemma 48 ([HMPS00]) *Let Γ be a non–scalar straight–line program over K of size L, non–scalar depth ℓ and parameters in a finite set $\mathcal{F} \subseteq K$ that evaluates a polynomial $P \in K[X_1, \ldots, X_n]$. Then, we have the following inequality.*

$$ht(P) \le wt(P) \le (2^{\ell+1} - 2)(\log L + ht(\mathcal{F})).$$

Moreover, for a given $\underline{x} = (x_1, \ldots, x_n) \in K^n$ we have the following upper bound:

$$ht(P(\underline{x})) \le (2^{\ell+1} - 2)\left(\log L + ht(\mathcal{F}) + ht(\underline{x})\right).$$

We start with the proof of an improvement of the Witness Theorem of [BCSS98b] and [BCSS98a]. A witness is a point where a non–zero polynomial does not vanishes. The main problem will be given a non–zero polynomial, show explicitely a witness. This can be performed by a procedure based on repeated squaring (Kronecker's scheme). In fact, this idea of using an explicit witness by repeated squaring for zero tests of polynomials goes back to Kronecker and can also be found in [HS82]. Here we discuss the effect of the depth, using some of the statements described in Subsections 2.1.3 and the Lemma 48 above.

Definition 49 *A witness for a polynomial $P \in K[X_1, \ldots, X_n]$ is a point $\underline{\omega} \in K^n$ such that $P(\underline{\omega}) = 0$ implies $P = 0$.*

In other words, a witness is a point $\underline{\omega} \in K^n$ from the set of K–rational points $V_K(P)$ of the hypersurface $V(P)$ (if any). There exist several methods for finding such a point, here we insist on the idea of explicit exhibition of such a witness in terms of the complexity of the given polynomial P.

Theorem 50 (Theorem) *Let $P \in K[X_1, \ldots, X_n]$ be a non–zero polynomial evaluable by a non–scalar straight–line program Γ of size L, non–scalar depth ℓ and parameters in $\mathcal{F} \subseteq K$. Let $\omega_0 \in K$ be such that the following holds :*

$$ht(\omega_0) \ge \max\{\log 2, ht(\mathcal{F})\}.$$

Let $N \in \mathbb{N}$ be a non–negative integer such that

$$\log N > \log(\ell + 1) + (\ell + 2)(\log 2)\left(\log\log(4L)\right).$$

Let us define recursively the following sequence of algebraic numbers (Kronecker's scheme) :

$$\omega_1 = \omega_0^N,$$

and for every i, $2 \le i \le n$, let us define

$$\omega_i = \omega_{i-1}^N.$$

Then, the point $\underline{\omega} := (\omega_1, \ldots, \omega_n) \in K^n$ is a witness for P (i.e. $P(\underline{\omega}) \neq 0$).

Proof.– Before giving the arguments (very close to those in [HS82] and [BCSS98a]), we have to introduce some additional notations. Let Γ be a non–scalar straight–line program of size L, depth ℓ with input variables $\underline{X} := (X_1, \ldots, X_n)$. Let $P \in K[X_1, \ldots, X_n]$ be a polynomial evaluable by the straight–line program Γ with parameters in $\mathcal{F} \subseteq K$. Let us also assume the following dense encoding for P :

$$P := \sum_{\underline{\mu}} P_{\underline{\mu}} \, \underline{X}^{\underline{\mu}}.$$

For every $0 \leq j \leq n$ and every affine point $\underline{\omega} := (\omega_1, \ldots, \omega_n) \in K^n$, we consider the polynomials

$$P_{\underline{\omega}}^{(j)} := \sum_{\underline{\mu} \in \mathbb{N}^n} P_{\underline{\mu}} \, \omega_1^{\mu_1} \cdots \omega_j^{\mu_j} \; X_{j+1}^{\mu_{j+1}} \cdots X_n^{\mu_n} \in K[X_{j+1}, \ldots, X_n],$$

where $P_{\underline{\mu}} \in K$. Let us observe that $P_{\underline{\omega}}^{(0)} = P \in K[X_1, \ldots, X_n]$, whereas $P_{\underline{\omega}}^{(n)} = P(\underline{\omega}) \in K$. We shall apply induction on n, starting from $P_{\underline{\omega}}^{(0)}$ and ending at $P_{\underline{\omega}}^{(n)}$. In order to perform this inductive argument we need a list of polynomials to go from step j to step $j+1$. Roughly speaking, this list of polynomials are the coefficients of $P_{\underline{\omega}}^{(j)}$ as element in $K[X_{j+1}][X_{j+2}, \ldots X_n]$. More precisely, for every $0 \leq j < n$, every $\underline{\omega} \in K^n$ and every multi–index $\underline{\alpha} := (\alpha_{j+1}, \ldots, \alpha_n) \in \mathbb{N}^{n-j}$ we introduce the following univariate polynomials :

$$P_{\underline{\alpha},\underline{\omega}}^{(j,j+1)} := \sum_{\underline{\mu} \in \mathbb{N}^n} P_{\underline{\mu}} \, \omega_1^{\mu_1} \cdots \omega_j^{\mu_j} \; X_{j+1}^{\alpha_{j+1}} \in K[X_{j+1}].$$

The following identity relates polynomials $P_{\underline{\alpha},\underline{\omega}}^{(j,j+1)}$ and polynomials $P_{\underline{\omega}}^{(j)}$:

$$P_{\underline{\omega}}^{(j)} = \sum_{\underline{\alpha} \in \mathbb{N}^{n-j}} P_{\underline{\alpha},\underline{\omega}}^{(j,j+1)}(X_{j+1}) X_{j+2}^{\alpha_{j+2}} \cdots X_n^{\alpha_n}.$$

Moreover, as the coefficients in K of $P_{\underline{\alpha},\underline{\omega}}^{(j,j+1)}$ are some of the coefficients in K of $P_{\underline{\omega}}^{(j)}$ we obviously conclude from Lemma 48 the following inequalities :

$$ht(P_{\underline{\alpha},\underline{\omega}}^{(j,j+1)}) \leq ht(P_{\underline{\omega}}^{(j)}) \leq (2^{\ell+1} - 1) \left(\log L + ht(\mathcal{F}) + ht(\omega_1, \ldots, \omega_j) \right).$$

We are now in condition to prove Theorem 50 by an inductive argument on the number n of variables involved. This proof is strongly based on the following Lemma. With the previous notations and assumptions, let $\omega_0 \in K$ be such that

$$ht(\omega_0) \geq \max\{\log 2, ht(\mathcal{F})\}.$$

Let us recursively define the following algebraic numbers

$$\omega_1 := \omega_0^N \text{ and } \omega_{j+1} := \omega_j^N, \;\text{ for every } j, \;\; 2 \leq j \leq n-1,$$

where $N \in \mathbb{N}$ verifies the following inequality

$$N > \left((\ell + 1) + 2^{\ell+2} \log(4L) \right).$$

Finally, let $\underline{\omega} \in K^n$ be the affine point

$$\underline{\omega} := (\omega_1, \ldots, \omega_n) \in K^n.$$

Lemma 51 *With the previous notations, for every j, $0 \leq j < n$, and for every multi–index $\underline{\alpha} \in \mathbb{N}^{n-j}$, if $P_{\underline{\alpha},\underline{\omega}}^{(j,j+1)} \in K[X_{j+1}]$ is a non–zero polynomial, then we have :*

$$P_{\underline{\alpha},\underline{\omega}}^{(j,j+1)}(\omega_{j+1}) \neq 0.$$

Assuming that this Lemma is true, the proof of Theorem 50 runs as follows. If $P := P_{\underline{\omega}}^{(0)} \in K[X_1, \ldots, X_n]$ is a non–zero polynomial, then there exists some non–zero coefficient $P_{\underline{\alpha},\underline{\omega}}^{(0,1)} \in K[X_1]$, which is a non–zero univariate polynomial. Then, by the Claim above, we have $P_{\underline{\alpha},\underline{\omega}}^{(0,1)}(\omega_1) \neq 0$. Thus, the polynomial $P_{\underline{\omega}}^{(1)} \in K[X_2, \ldots, X_n]$ has as coefficients the list

$$P_{\underline{\omega}}^{(1)} = \sum_{\underline{\alpha}} P_{\underline{\alpha},\underline{\omega}}^{(0,1)}(\omega_1) X_2^{\alpha_2} \cdots X_n^{\alpha_n}.$$

In particular, the polynomial $P_{\underline{\omega}}^{(1)}$ is a non–zero polynomial and it has a non–zero coefficient

$$P_{\underline{\alpha},\underline{\omega}}^{(1,2)} \in K[X_2].$$

The same argument, using the Lemma above, shows that $P_{\underline{\omega}}^{(2)} \in K[X_3, \ldots, X_n]$ is a non–zero polynomial. Inductively, we obtain $P(\underline{\omega}) := P_{\underline{\omega}}^{(n)} \in K$ as a non–zero polynomial and the statement claimed is proved. ■

Thus, to conclude the proof, we will have to prove Lemma 51 introduced above.

Proof.– [of Lemma 51] First of all, we recall the following inequalities.

- $N > \left((\ell + 1) + 2^{\ell+2} \log(4L)\right)$
- $ht(P_{\underline{\alpha},\underline{\omega}}^{(j,j+1)}) \leq ht(P_{\underline{\omega}}^{(j)}) \leq (2^{\ell+1} - 1)\left(\log L + ht(\mathcal{F}) + ht(\omega_1, \ldots, \omega_j)\right)$
- For every $\nu \in M_K$ holds $\max\{0, \log|\omega_1|_\nu, \ldots, \log|\omega_j|_\nu\} = \max\{0, \log|\omega_j|_\nu\}$.
- Thus, we have $ht(\omega_1, \ldots, \omega_j) \leq ht(\omega_j)$.

Hence, we conclude that $ht(\mathcal{F}) + ht(\omega_1, \ldots, \omega_j) \leq 2ht(\omega_j)$, and by Lemma 48, we conclude the following inequality :

$$ht(P_{\underline{\alpha},\underline{\omega}}^{(j,j+1)}) \leq ht(P_{\underline{\omega}}^{(j)}) \leq (2^{\ell+1} - 2)\left(\log L + 2ht(\omega_j)\right).$$

Moreover, we have the following inequality : $\log\deg(P_{\underline{\alpha},\underline{\omega}}^{(j,j+1)}) \leq \ell \log 2 \leq \ell ht(\omega_j)$.
By virtue of Corollary 27, if $P_{\underline{\alpha},\underline{\omega}}^{(j,j+1)} \neq 0$, the following inequality holds for every $\zeta \in K$ satisfying $P_{\underline{\alpha},\underline{\omega}}^{(j,j+1)}(\zeta) = 0$:

$$ht(\zeta) \leq \left((\ell + 1) + 2^{\ell+2}\log(4L)\right) ht(\omega_j) < N ht(\omega_j) = ht(\omega_{j+1}).$$

In particular, if $P_{\underline{\alpha},\underline{\omega}}^{(j,j+1)}$ is not the zero polynomial, we have as desired :

$$P_{\underline{\alpha},\underline{\omega}}^{(j,j+1)}(\omega_{j+1}) \neq 0.$$

Now, as a final comment to conclude the proof : The lower bound of the statement of Theorem 50 above,

$$\log_2 N > \log_2(\ell + 1) + (\ell + 2)(\log 2)\left(\log\log(4L)\right)$$

obviously implies the lower bound used to prove Lemma 51, i.e.

$$N > \left((\ell + 1) + 2^{\ell+2}\log(4L)\right).$$

■

In order to transform Theorem 50 above into a deterministic procedure, we just have to observe that the number of parameters used by a non–scalar straight–line program Γ of size L is at most $2L^2$. Thus, we conclude the following Corollary :

Corollary 52 *Let $P \in K[X_1, \ldots, X_n]$ be a non–zero polynomial evaluable by a non–scalar straight–line program Γ of size L, non–scalar depth ℓ and parameters in $\mathcal{F} := \{x_1, \ldots, x_r\} \subseteq K$. Let $\omega_{-1} \in K$ be such that*

$$ht(\omega_{-1}) := \max\{\log 2, ht(x_1), \ldots, ht(x_r)\}.$$

Let us define $\omega_0 \in K$ as $\omega_0 := \omega_{-1}^{2L^2}$. Let $N \in \mathbb{N}$ be a non–negative integer such that

$$\log N > \log(\ell + 1) + (\ell + 2)(\log 2) (\log \log(4L)) .$$

Let us define recursively the following sequence of algebraic numbers (Kronecker's scheme) :

$$\omega_1 = \omega_0^N ,$$

and for every i, $2 \leq i \leq n$, let us define $\omega_i = \omega_{i-1}^N$. Then, the point $\underline{\omega} := (\omega_1, \ldots, \omega_n) \in K^n$ is a witness for P (i.e. $P(\underline{\omega}) \neq 0$).

Remark 53 *i) The procedure described in Corollary 52 above for choosing ω_{-1} can be improved in several obvious cases. For instance, if $K = \mathbb{Q}$ and $\mathcal{F} \subseteq \mathbb{Z}$, the same assertion holds taking $\omega_0 = \omega_{-1}$.*

ii) Theorem 50 above is an improvement of the previous established requirements for N. In [BCSS98b, BCSS98a] the authors showed a lower bound for N of the order :

$$\log N > 4nL^2 + 4L,$$

which is obviously less sharp.

iii) THE GENERAL DENSE CASE. *For generically many polynomials $P \in K[X_1, \ldots, X_n]$ of degree at most d, the optimal straight–line program is of size*

$$L = \binom{d+n}{n}$$

and non–scalar depth of order $\ell = \log d + O(1)$. The parameters of this straight–line program are the coefficients of P. Our Theorem 50 says that there exists a (small) universal constant $c_2 > 1$, such that the requirement for selecting the non– negative integer N in Kronecker's scheme is just the one described by the following inequality :

$$\log N > c_2 n \log^2 d.$$

Previous requirements were of order $\log N > 4n\binom{d+n}{n}^2 + 4\binom{d+n}{n}$.

iv) THE SPARSE/FEWNOMIAL CASE. *Let us assume the our polynomial $P \in K[X_1, \ldots, X_n]$ has very few terms with non–zero coefficients (i.e. P is sparse as much as it is a fewnomial). Let us assume that P has degree at most d and also that at most M of its terms have non–zero coefficients. Among the fewnomials of this class the (generically) optimal non–scalar straight–line program that evaluates P has size of order $L = c_3 M d$ (where $c_3 > 0$ is a universal constant), and depth $\log_2 d + O(1)$. Once again, the parameters are the non–zero coefficients of the non–zero terms of P. Thus, Theorem 50 above says that there exists a (small) universal constant $c_3 > 1$, such that the only requirement for selecting the non–negative integer N in Kronecker's scheme is the following one :*

$$\log N > c_3 \log d \left(\log \log d + \log \log M\right) .$$

Previous estimates were of order $\log N > 4n\left(c_3 M d\right)^2 + 4c_3 M d$.

4.2 Factoring polynomials given by straight–line programs.

Factoring univariate polynomials given by straight–line program encoding has been subject of research since the eighties. An excellent reference list can be found in the works of E. Kaltofen ([Kal90, Kal92]). However, we have not found any reference related to the subject described above : computing just those irreducible factors of "a priori" bounded height. Thus, we have to develop this subject here. We establish the following technical statement :

Theorem 54 *There exists a bounded error probabilistic Turing machine M that performs the following task : Given as input for M :*

- *a univariate polynomial $f \in \mathbb{Z}[T]$ with integer coefficients given by straight–line program encoding, and*
- *a positive integer number $H \in \mathbb{N}$ given in binary encoding,*

the output of M is a list of irreducible polynomials $\{f_1, \ldots, f_s\} \subset \mathbb{Z}[T]$, such that the following holds :

- $\displaystyle\prod_{i=1}^{s} f_i$ *divides f,*
- *$wt(f_i) \leq \log_2(d+1) + H$ for every i, $1 \leq i \leq s$, and*
- *for every irreducible factor g of f, the following holds : either $wt(g) > H$ or $g \in \{f_1, \ldots, f_s\}$.*

The running time of M is polynomial in :

$$d \; L \; H \; \eta,$$

where $d = \deg(f)$, L is the size of the straight–line program Γ that evaluates the coefficients of f, and η is an upper bound for the bit length of the integer parameters used by Γ.

The proof of this Theorem is divided into four main tasks which are essentially the usual four steps in any univariate polynomial factoring procedure :

i) choosing a "good" prime number,

ii) efficient factoring modulo this prime number,

iii) Newton–Hensel lifting, and

iv) A modified L^3 basis reduction algorithm.

Now we proceed to describe these four tasks. The notations introduced above will be used in the remaining parts of this description.

Task 1: Choosing a "good" prime number

Lemma 55 *There exists a bounded error probability Turing machine M_1 that performs the following task. The input of M_1 is a polynomial $f \in \mathbb{Z}[T]$ given as in Theorem 54 above. The output of M_1 is a prime number $p \in \mathbb{N}$, such that the following properties hold :*

- *the leading coefficient of f is non–zero in $\mathbb{Z}/p\mathbb{Z}$, and*
- *the polynomial $\bar{f} \in \mathbb{Z}/p\mathbb{Z}[T]$ obtained from f by taking residues module p is squarefree.*

The running time of M_1 is polynomial in the following quantities :

$$d \; L \; \eta,$$

where $d = \deg(f)$, L is the length of the straight–line program Γ encoding the coefficients of f, and η is an upper bound of the logarithmic height of the parameters used by Γ.

Proof.– This Lemma follows by an strategy similar to that used in [IM83]. More precisely, we combine the Prime Number Theorem (cf. [Ros94], for instance) with the upper bounds shown in Lemma 48.

First of all, let us write f as $f = a_dT^d + \ldots + a_0$, where $a_i \in \mathbb{Z}$ for every $i, \ 0 \le i \le d$. Let us assume that the straight–line program Γ that evaluates $a_0, \ldots, a_d \in \mathbb{Z}$ has size L, depth ℓ, and the parameters used by Γ are of logarithmic height at most η.

Let us define the following integer number

$$\tau := a_d \mathrm{disc}_T(f) \in \mathbb{Z} \setminus \{0\},$$

where $\mathrm{disc}_T(f)$ is the discriminant of f. From Lemma 48 we conclude

$$ht(\mathrm{disc}_T(f)) \le d(\log d + (2^{\ell+1} - 2)(\log L + \eta)).$$

Now, let $N \in \mathbb{N}$ be a positive integer number such that

$$d(\log d + 2(2^{\ell+1} - 2)(\log L + \eta)) < N2^N.$$

Thus, the machine M_1 proceeds as follows :

- First of all, M_1 chooses at random $4N$ disjoint lists $L_1, \ldots, L_{4N}$ of integer numbers between 2^N and 2^{2N}. We assume that each list L_i contains $4N$ different integer numbers.
- Then, M_1 uses a probabilistic primality test running in polynomial time (cf. [AH92, AM93, SG86, Mor90, Mor91], for instance) to detect a prime number $p_i \in L_i$ for every i, $1 \le i \le 4N$ (if any).
- Then, M_1 takes the list $\mathbb{P} = \{p_1, \ldots, p_{4N}\}$ and looks for some prime number $p \in \mathbb{P}$, such that

  $$\tau \; mod \; p \neq 0.$$

  This last task is performed by using the straight–line program Γ that evaluates a_d and the obvious straight–line program Γ' that evaluates $\mathrm{disc}_T(f)$.

The error probability of this procedure is at most $\left(1 - \dfrac{1}{2N}\right)^{8N} < \dfrac{1}{e^4} < \dfrac{1}{2}$. ■

Task 2: Efficient factoring module a prime number It is a well-known that Berlekamp's factoring procedure in $\mathbb{Z}/p\mathbb{Z}[T]$ is deterministic, but its running time depends polynomially on the prime number p, and hence exponentially on the bit length of p. To avoid this drawback, P. Camion, D. Cantor and H. Zassenhauss ([CZ81, Cam, Cam83], for instance) have developed a probabilistic factoring procedure for polynomials $f \in \mathbb{Z}/p\mathbb{Z}[X]$ whose running time depends polynomially on $\deg(f)$ and the bit length of the prime number p. This method yields the following technical statement :

Lemma 56 *With the same assumptions as in Theorem 54 above, there exists a bounded error probabilistic Turing machine M_2 that performs the following task:*
The input of M_2 are polynomials $f \in \mathbb{Z}[T]$ as given in Theorem 54 above.
The output of M_2 is a prime number $p \in \mathbb{Z}$ as in Lemma 55 above and a list of polynomials

$$\{f_1, \ldots, f_s\} \in \mathbb{Z}/p\mathbb{Z}[T],$$

such that every $f_i \in \mathbb{Z}/p\mathbb{Z}[T]$ is an irreducible univariate polynomial for every i, $1 \leq i \leq s$ and

$$\bar{f} = \prod_{i=1}^{s} f_i,$$

where $\bar{f} \in \mathbb{Z}/p\mathbb{Z}[T]$ is the univariate squarefree polynomial obtained by taking residues modulo p of the coefficients of f. The running time of M_2 is polynomial in the following quantities :

$$L \; d \; \eta,$$

where d, L and η are as in Theorem 54 above.

Task 3 and 4: Newton–Hensel lifting and L^3 basis reduction From the output of the Turing machine M_2 of Lemma 56 above, we perform a Newton–Hensel lifting of each of the irreducible factors $f_i \in \mathbb{Z}/p\mathbb{Z}[T]$ of $\bar{f} \in \mathbb{Z}/p\mathbb{Z}[T]$ until we reach the bounds which allow us to apply the L^3 reduction procedure of [LLL82a].
However, the original bounds in [LLL82a] depend on the weight of the input polynomial $f \in \mathbb{Z}[T]$. Since we are not interested in computing all irreducible factors of f in $\mathbb{Q}[T]$, but just a few of them (those of weight bounded by H), we explain how the main statement of [LLL82a] can be modified for our purposes. The same proof of [LLL82a] yields our statement :
For every positive integer number $k \geq 1$, we shall denote by $\mathbb{Z}/p^k\mathbb{Z}$ the residue ring of integers modulo p^k. For every integer number $a \in \mathbb{Z}$, we denote by $\bar{a}^p \in \mathbb{F}_p$ and $\bar{a}^{p^k} \in \mathbb{Z}/p^k\mathbb{Z}$ the residual classes modulo p and p^k respectively. For every univariate polynomial g with integer coefficients

$$g = a_m X^m + \ldots + a_1 X + a_0$$

we denote by $\bar{g}^p \in \mathbb{F}_p[X]$ and $\bar{g}^{p^k} \in \mathbb{Z}/p^k\mathbb{Z}[X]$ the polynomials obtained respectively as :

$$\bar{g}^p := \bar{a}_m^p X^m + \ldots + \bar{a}_1^p X + \bar{a}_0^p \in \mathbb{F}_p[X], \text{ and } \bar{g}^{p^k} := \bar{a}_m^{p^k} X^m + \ldots + \bar{a}_1^{p^k} X + \bar{a}_0^{p^k} \in \mathbb{F}_{p^k}[X].$$

In the sequel we shall omit the superscripts ^{p} and $^{p^k}$ where no confusion may occur. From now on, let $f \in \mathbb{Z}[X]$ be a squarefree univariate polynomial with integer coefficients. Let $p \in \mathbb{N}$ be a prime number and let us assume that $\bar{f} \in \mathbb{F}_p[X]$ is also squarefree and that

$$\deg(f) := \deg(\bar{f}) = d.$$

Let us observe, that under these conditions $\bar{f}^{p^k} \in \mathbb{Z}/p^k\mathbb{Z}[X]$ is also squarefree and for every $k \geq 1$ holds :

$$\deg(f) = \deg(\bar{f}^{p^k}).$$

Let $h \in \mathbb{Z}[X]$ be a polynomial of degree $r \geq 0$ such that the following holds :

- the leading coefficient of h is 1,
- $\bar{h}$ divides $\bar{f}$ in $\mathbb{Z}/p^k\mathbb{Z}[X]$, and
- $\bar{h}$ is an irreducible polynomial in $\mathbb{F}_p[X]$.

Proposition 57 *[LLL82a] With the previous notations and assumptions, there exists one and only one irreducible factor $h_0 \in \mathbb{Z}[X]$ of f (in $\mathbb{Z}[X]$) such that $\bar{h}$ divides $\bar{h}_0$ in $\mathbb{F}_p[X]$.*

Now, we may define the following lattice (which depends only on h, p^k and $m \in \mathbb{N}$, $\leq m \leq d$):

$$L_{r,m}(h) := \{g \in \mathbb{Z}[X] : \deg(g) \leq m, \bar{h} \text{ divides } \bar{g} \text{ in } \mathbb{Z}/p^k\mathbb{Z}[X]\}$$

Finally, for every polynomial $g \in \mathbb{Z}[X]$, given as $g = a_mX^m + \ldots + a_1X + a_0$, we shall denote the norm of g as :

$$\|g\| := (a_m^2 + \ldots + a_1^2 + a_0^2)^{\frac{1}{2}}.$$

Let us observe that $\|g\| \leq WT(g) \leq (d+1)\|g\|$.
The following Theorem essentially states that the main statement in [LLL82b] depends principally on $\|h_0\|$ and not on $\|f\|$.

Theorem 58 *With the same notations and conventions as before, let $b_1, \ldots, b_{m+1}$ be a L^3–reduced basis of the lattice $L_{r,m}(h)$. Let us also assume that*

$$p^{kr} \geq 2^{\frac{dm}{2}} 2^{dm} \|h_0\|^{m+d}.$$

Thus, $h_0 \in L_{r,m}(h)$ if and only if $\|b_1\| \leq \left(\frac{p^{kr}}{\|h_0\|^m}\right)^{\frac{1}{d}}$.
Moreover, let $t \in \{1, \ldots, m+1\}$ be the maximal integer number such that :

$$\|b_j\| \leq \left(\frac{p^{kr}}{\|h_0\|^m}\right)^{\frac{1}{d}} \textit{ for every } i, \ 1 \leq j \leq t.$$

Then, $\deg(h_0) = m + 1 - t$ and $h_0 = \gcd(b_1, \ldots, b_t)$.

The proof of this Theorem follows step by step as that of Proposition 2.13 in [LLL82b]. ■

Now, we can show Theorem 54:

Proof.– [of Theorem 54] The machine M of Theorem 54 can be described as follows :
First of all, we apply the machine M_2 of Lemma 56 (which contains M_1) and yield the following list of items as output :

- a prime number $p \in \mathbb{Z}$ as in Lemma 56 above, and
- a list of polynomials $\{f_1, \ldots, f_s\} \subset \mathbb{Z}/p\mathbb{Z}[T]$, such that every $f_i \in \mathbb{Z}/p\mathbb{Z}[T]$ is an irreducible univariate polynomial for every i, $1 \leq i \leq s$ and

$$\bar{f} = \prod_{i=1}^{s} f_i.$$

For every $h \in \{f_1, \ldots, f_s\}$, the machine applies a Hensel Lifting procedure $\log_2 k$ times (as in [PZ89], for instance) to obtain a univariate polynomial $h_i \in \mathbb{Z}[X]$ satisfying :

- the leading coefficient of h, is 1 (and agrees with that of h),
- $\bar{h}$ and $\bar{h}_1$ agree in $\mathbb{F}_p[X]$, and
- $\bar{h}_1$ divides $\bar{f}$ in $\mathbb{Z}/p^k\mathbb{Z}[X]$.

The number k has been chosen such that holds : $p^{kr} \geq 2^{\frac{d^2}{2}} 2^{d^2} 2^{2dH}$.
Now, let $h_0 \in \mathbb{Z}[X]$ be the unique irreducible factor of f determined by Proposition 57.
Let r be the degree of h_1 and for every m, $r \leq m \leq d$, let $b_1^{(m)}, \ldots, b_{m+1}^{(m)}$ be a L^3–reduced basis of the lattice $L_{r,m}(h_1)$.
Now, if $\|b_1^{(m)}\| < \left(\frac{p^{kr}}{2^{mH}}\right)^{\frac{1}{d}}$, for some m, $r \leq m \leq d$, we conclude

- $h_0 \in L_{r,m}(h_1)$, and
- $\log_2 \|h_0\| \leq H$ (which, in particular, implies $wt(h_0) \leq \log_2(d+1) + H$).

Conversely, if $\|b_1^{(m)}\| \geq \left(\dfrac{p^{kr}}{2^{mH}}\right)^{\frac{1}{d}}$ for every m, $r \leq m \leq d$, we conclude that $wt(h_0) > H$, and we do not compute this irreducible factor.
Thus, we proceed by computing h_0 according to the strategy described by Theorem 58 above. ■

4.3 Computing binary encodings of suitable approximations

In the spite of the fast convergence of Newton's method, the bit length (i.e. the height) of the results obtained after several iterations may grow much faster than desirable. That is why we have to truncate the intermediate results obtained and this is the goal of the following statement :

Theorem 59 (Efficient Diophantine Approximation) *There exists a Turing machine M, which performs the following task :*
The input of M is the following list :

i) A list $F := (f_1, \ldots, f_n)$ of polynomials with integer coefficients of degree at most d and (logarithmic) weight at most w given by a division–free non–scalar straight–line program Γ of length L and depth ℓ and parameters in $\{-1, 0, 1\}$.

ii) The binary encoding of a point $z \in \mathbb{Q}[i]^n$ which is an approximate zero of the system $F := (f_1, \ldots, f_n)$ with associated zero $\zeta \in V_K(f_1, \ldots, f_n)$ with respect to the standard archimedean absolute value $|\cdot| : K \to \mathbb{R}$ induced by the standard inclusion $i : K \hookrightarrow \mathbb{C}$ satisfying the γ–Theorem, namely

$$\gamma(F, \zeta)\|z - \zeta\| \leq \frac{3 - \sqrt{7}}{2}.$$

iii) A positive rational $\epsilon \in \mathbb{Q}$, $\epsilon < 1$.

The machine M outputs the binary encoding of an approximation $\bar{z} \in \mathbb{Q}[i]^n$, such that

$$\|\bar{z} - \zeta\| \leq \epsilon.$$

The (logarithmic) height of $\bar{z}$ satisfies the following inequality :

$$ht(\bar{z}) \leq (n\ d\ w\ ht(z)(-\log_2 \epsilon))^{c_4}$$

where $c_4 > 0$ is a universal constant. The running time of M is polynomial in the following quantities :

$$n\ d\ L\ w\ ht(z)\ (-\log_2 \epsilon).$$

The proof of this statement will make use of several technical procedures which we are going to state now.

Rational Reconstruction of Newton Iteration.

Lemma 60 *With the same notations and assumptions as in Theorem 59 above, there is a universal constant $c_5 > 0$ such that the following holds : for every $z \in \mathbb{Q}[i]^n$:*

$$ht(N_F(z)) \leq (wdn)^{c_5} ht(z).$$

Due to the straight–line program encoding of the polynomials $f_1, \ldots, f_n$, we have to use the following Lemma which gives a well-suited version of Newton operator for this encoding.

Lemma 61 *[GHH+97, Mor97] Let $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ be polynomials as in Theorem 66. Then, there exists a straight–line program of length $O(d^2n^7L)$ and non-scalar depth $O(\log_2 n + \ell)$ which using the same parameters, computes the numerators $g_1, \ldots, g_n$ and a non–zero denominator h for $N_F(X_1, \ldots, X_n)\mathbb{Z}(X_1, \ldots, X_n)$.*

In order to obtain the binary encoding of $N_F(z)$, we use the following Lemma (as given in [HM97]) which is suitable for our particular straight–line program encoding of N_F. It is based on a rational reconstruction procedure due to J. Dixon (see [Dix82] or [Häg98, HM97] for details).

Lemma 62 *[HM97] There exists a Turing machine which, taking as input the straight–line program of $N_F(z_1, \ldots, z_n)$, outputs in time polynomial in*

$$d\ n\ w\ ht(z)\ L$$

a reduced binary encoding of $N_F(z_1, \ldots, z_n)$ (i.e. numerators and denominators have no common factors).

Effective Dirichlet Theorem. The first relevant statement is the following effective version of Dirichlet's Theorem due to [LLL82a].

Theorem 63 (Effective Dirichlet Theorem) *There exists a polynomial–time algorithm that, given a positive integer n and rational numbers $a_1, \ldots, a_n, \epsilon$ satisfying $0 < \epsilon < 1$, finds integers $p_1, \ldots, p_n, q$ satisfying*

$$|p_i - qa_i| \leq \epsilon \text{ for } 1 \leq i \leq n, \text{ and } 1 \leq q \leq \frac{2^{n(n+1)/4}}{\epsilon^{2n}}.$$

Proof.– [of Theorem 59] Let us denote by $EDT(z, \epsilon)$ the result of applying the Effective Dirichlet Theorem above to the point z and the rational number ϵ. Let us recursively define the following sequence of points in $\mathbb{Q}[i]$:

$$z^{(1)} := N_F(z), \text{ and } \bar{z}^{(1)} := EDT(z^{(1)}, \epsilon/4)$$

and for $k \geq 2$,

$$z^{(k)} := N_F(\bar{z}^{(k-1)}), \text{ and } \bar{z}^{(k)} := EDT(z^{(k)}, \epsilon/4).$$

Now, we have : $\|\bar{z}^{(k)} - \zeta\| < \|z^{(k)} - \zeta\| + \frac{\epsilon}{4}$. On the other hand, the following holds :

$$\|z^{(k)} - \zeta\| \leq \frac{1}{2}\|\bar{z}^{(k-1)} - \zeta\|.$$

From the previous inequalities we conclude :

$$\|\bar{z}^{(k)} - \zeta\| \leq \frac{1}{2^k}\|\zeta - z\| + \sum_{i=0}^{k-1} \frac{\epsilon}{2^{i+2}}.$$

In order to estimate $\|\zeta - z\|$, we apply Remark 41 to conclude :

$$\log \|\zeta - z\| \leq c \left(\frac{3}{d-1} \right) 2(\log n + w + d^2(ht(z))) + 1,$$

where c is a small universal constant $c > 0$. Therefore the following inequality holds :

$$\|\bar{z}^{(k)} - \zeta\| \leq \frac{1}{2^k} 2^{c(\log n + w + d^2 ht(z)} + \frac{\epsilon}{2}.$$

Thus, taking $k \in \mathbb{N}$ such that $k > (-\log_2 \epsilon)c(\log n + w + d^2 ht(z))$, the result follows. ■

Let us observe that the procedure described in the previous Theorem is essentially optimal due to the lower bound given in [GHH$^+$97].

4.4 From Kronecker's to Newton's solution

In this Subsection we prove Theorem 20 as stated in the Introduction. That statement is merely a consequence of the following Theorem we are going to show here.

Theorem 64 (From Kronecker's solution to Newton's solution) *There exists a bounded error probability Turing machine M which performs the following task :*
Given as input a positive integer $H \in \mathbb{N}$ in binary encoding and a sequence F of multivariate polynomials with integer coefficients $F := (f_1, \ldots, f_n)$ with $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ satisfying :

- *the polynomials $f_1, \ldots, f_n$ are of degree at most d and (logarithmic) weight at most w,*
- *the sequence $f_1, \ldots, f_n$ is given by a division–free non–scalar straight–line program Γ of length L, non–scalar depth ℓ and parameters in $\{-1, 0, 1\}$, and*
- *the sequence $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ is a smooth regular sequence,*

the machine M outputs approximate zeros with respect to the archimedean absolute value $|\cdot| : K \to \mathbb{R}$ induced on K by the canonical inclusion $i : K \hookrightarrow \mathbb{C}$ for all those zeros $\zeta \in V_K(f_1, \ldots, f_n)$, whose (logarithmic) height is at most H, i.e.

$$ht(\zeta) \leq H.$$

The running time of M is polynomial in the following quantities

$$(n\ d\ \delta(F)\ L\ w) + (n\ d\ D\ H\ [K : \mathbb{Q}]),$$

where $\delta(F) := \max\{\deg V(f_1, \ldots, f_i) : 1 \leq i \leq n\}$ and $D := \deg V(f_1, \ldots, f_n)$.

Proof.– This statement follows by giving a procedure that transforms a Kronecker description of the solution variety into a list of approximate zeros of bounded height.
First of all, let us recall how to relate $\mathbb{Q}$–definable irreducible components of bounded height and irreducible factors of bounded height of the minimal equation of the primitive element χ_u of the Kronecker solution.
A $\mathbb{Q}$–definable complex variety is an algebraic subset $\mathcal{W} \subset \mathbb{C}^n$, such that there exist polynomials $f_1, \ldots, f_s \in \mathbb{Z}[X_1, \ldots, X_n]$ with integer coefficients, such that

$$\mathcal{W} = \{\underline{x} \in \mathbb{C}^n : f_1(\underline{x}) = 0, \ldots, f_s(\underline{x}) = 0\}.$$

In particular, under our hypothesis the solution variety $V(f_1, \ldots, f_n) \subset C^n$ is $\mathbb{Q}$–definable. A $\mathbb{Q}$–definable algebraic subset $\mathcal{W} \subset \mathbb{C}^n$ is said to be $\mathbb{Q}$–definable irreducible if for any two $\mathbb{Q}$–definable algebraic subsets $\mathcal{W}_1, \mathcal{W}_2 \subset \mathbb{C}^n$, the following holds :

$$\mathcal{W} \subset \mathcal{W}_1 \cup \mathcal{W}_2 \Rightarrow [\mathcal{W} \subset \mathcal{W}_1] \vee [\mathcal{W} \subset \mathcal{W}_2].$$

In particular, the usual method shows that every $\mathbb{Q}$–definable algebraic subset $V \subset \mathbb{C}^n$ has a unique minimal description as a finite union of $\mathbb{Q}$–definable irreducible algebraic subsets $\mathcal{W}_1, \ldots, \mathcal{W}_s \subset \mathbb{C}^n$. Namely,

$$V = \mathcal{W}_1 \cup \ldots \cup \mathcal{W}_s.$$

These $\mathbb{Q}$–definable irreducible subsets $\mathcal{W}_1, \ldots, \mathcal{W}_s$ are called the $\mathbb{Q}$–definable irreducible components of V.
Let us observe that if $V \subset C^n$ is zero–dimensional (i.e. if V is a finite set) and if

$$V = \mathcal{W}_1 \cup \ldots \cup \mathcal{W}_s$$

is the decomposition of V into $\mathbb{Q}$–definable irreducible components, then this is a partition of V. Namely, $\mathcal{W}_i \cap \mathcal{W}_j = \emptyset$ for every $i \neq j$.
Let us assume now that K is a number field and that $\zeta \in V_K(f_1, \ldots, f_n)$ is a K–rational point of a zero–dimensional algebraic subset $V(f_1, \ldots, f_n) \subset \mathbb{C}^n$. Then, there exists a unique $\mathbb{Q}$–definable irreducible component $\mathcal{W}_\zeta \subset \mathbb{C}^n$ containing ζ. Moreover, as $\zeta \in K^n$, we easily conclude the following inequality :

$$\deg \mathcal{W}_\zeta = \deg(\zeta) = \# \mathcal{W}_\zeta \leq [K : \mathbb{Q}].$$

Let $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ be a sequence of polynomials defining a zero–dimensional $\mathbb{Q}$–definable affine algebraic variety $V := V(f_1, \ldots, f_n) := \{\underline{x} : f_1(\underline{x}) = 0, \ldots, f_n(\underline{x}) = 0\}$. Let us assume that the ideal $(f_1, \ldots, f_n)$ is a radical ideal in $\mathbb{Q}[X_1, \ldots, X_n]$. In particular all points in V are smooth.
As defined in the Introduction, a Kronecker solution of $V(f_1, \ldots, f_n)$ is the following list of items :

- The list of variables in Noether position $X_1, \ldots, X_n$.
- The primitive element $u := \lambda_1 X_1 + \cdots + \lambda_n X_n$ given by its coefficients in $\mathbb{Z}$. Let us recall that the linear form u is a primitive element u if and only if the polynomial mapping :

  $$\mathcal{U} : \mathbb{C}^n \longrightarrow \mathbb{C} : (x_1, \ldots, x_n) \mapsto u(x_1, \ldots, x_n)$$

  defines a birational isomorphism between $V(f_1, \ldots, f_n)$ and a hypersurface $H_u \subset \mathbb{C}$ (i.e. the set of roots of a univariate polynomials $\chi_u \in \mathbb{Z}[T]$).
- The minimal equation of the hypersurface H_u, namely $\chi_u \in \mathbb{Z}[T]$.
- A description of $(\mathcal{U} \mid_V)^{-1}$. This description is given by the following list :
  - a non–zero integer number $\rho \in \mathbb{Z}$,
  - a list of polynomials $v_j \in \mathbb{Z}[T]$, $1 \leq j \leq n$, such that $\deg(v_j) \leq \deg(\chi_u)$ for every j, $1 \leq j \leq n$,

  and such that the following holds for every $t \in H_u$:

  $$(\mathcal{U} \mid_V)^{-1}(t) := \left(\rho^{-1} v_1(t), \ldots, \rho^{-1} v_n(t)\right).$$

In particular, the birational isomorphism $\mathcal{U} : V \subset \mathbb{C}^n \to H_u \subset \mathbb{C}$ defines a biregular isomorphism that identifies the $\mathbb{Q}$–definable irreducible components of V and the $\mathbb{Q}$–definable irreducible components of H_u. Moreover, the $\mathbb{Q}$–definable irreducible components of H_u are completely determined by the prime factors of the univariate polynomial $\chi_u \in \mathbb{Z}[T]$.
This is explained in the following Lemma, whose elementary proof we omit.

Lemma 65 *With the previous notations and assumptions, let $\zeta := (\zeta_1, \ldots, \zeta_n) \in V_K(f_1, \ldots, f_n)$ be a smooth K–rational zero of the system $V = (f_1, \ldots, f_n)$. Let $\mathcal{W}_\zeta \subset V(f_1, \ldots, f_n)$ be the $\mathbb{Q}$–definable irreducible component of $V(f_1, \ldots, f_n)$ containing ζ. Then the following properties hold :*

- $\# \mathcal{W}_\zeta = \deg \mathcal{W}_\zeta \leq [K : \mathbb{Q}]$,
- *there exists a unique prime factor $g \in \mathbb{Q}[T]$ of $\chi_u \in \mathbb{Z}[T]$ such that :*
  - *$g \in \mathbb{Z}[T]$ is a primitive polynomial,*
  - *g vanishes on $\mathcal{U}(\mathcal{W}_\zeta)$,*
  - *g contains a zero in K,*
  - *$ht(g) \leq [K : \mathbb{Q}](ht(\zeta) + ht(u))$.*

Moreover, there exists a non–zero integer $\bar{\rho} \in \mathbb{Z} \setminus \{0\}$ and polynomials $w_1, \ldots, w_n$, such that the following holds :

- *the (logarithmic) height of $\bar{\rho}$,$w_1, \ldots, w_n$ is at most polynomial in*

$$[K : \mathbb{Q}] \deg(g)[ht(\zeta) + ht(u)]n,$$

- $\deg(w_i) \leq \deg(g) - 1$ *for all i, $1 \leq i \leq n$, and*
- $V_\zeta := \{(\bar{\rho}^{-1} w_1(t), \ldots, \bar{\rho}^{-1} w_n(t)) : t \in \mathbb{C}$ *and* $g(t) = 0\}$.

This univariate polynomial g is obviously the minimal polynomial over $\mathbb{Q}$ of the algebraic number :

$$u(\zeta) := u_1\zeta_1 + \ldots + u_n\zeta_n.$$

The polynomials $w_1, \ldots, w_n \in \mathbb{Z}[T]$ and the non–zero integer $\bar{\rho} \in \mathbb{Z}\setminus\{0\}$ introduced by the previous Lemma are given by the following rule. Let $q_1, \ldots, q_n \in \mathbb{Q}[T]$ be the remainders of the division of $\rho^{-1} v_i(T)$ by $g(T)$, i.e. $q_i := \mathrm{rem}(\rho^{-1} v_i, g)$ for every i, $1 \leq i \leq n$. Then, taking a minimal non–zero integer $\bar{\rho} \in \mathbb{Z} \setminus \{0\}$, such that $\bar{\rho} q_i \in \mathbb{Z}[T]$ for all i, $1 \leq i \leq n$ and defining $w_i := \bar{\rho} q_i \in \mathbb{Z}[T]$ for every i, $1 \leq i \leq n$, we obtain the desired polynomials.
In conclusion, to determine the list of smooth K–rational zeros of the system F of height bounded by H, we may determine the irreducible factors of χ_u such that

- K contains a root of g, and
- $ht(g) \leq [K : \mathbb{Q}](H + ht(u))$.

Thus, to prove Theorem 20, we start by using Theorem 17 (cf. [GHMP97]) as stated in the Introduction.
Let us recall that the output of the procedure described in Theorem 17 is a Kronecker solution of the variety $V(f_1, \ldots, f_n)$ with the following properties :

- the coefficients of the primitive element u have height at most $cn \log_2 d$,
- the coefficients of the polynomials $\chi_u, v_1, \ldots, v_n \in \mathbb{Z}[T]$ and the non–zero integer number $\rho \in \mathbb{Z} \setminus \{0\}$ are given by a straight–line program Γ satisfying the following properties :
  - size of $\Gamma \leq (nd\delta)^{c_6} L$,
  - non–scalar depth of $\Gamma \leq n^c(\log_2 \delta + \ell + \log_2 d)$,
  - the parameters used by Γ are in $\{-1, 0, 1\} \subset \mathbb{Z}$,

  where $c_6 > 0$ is some some "small" universal constant.

In order to conclude Theorem 20 from this data, we proceed as follows :

Task 1.- Computing irreducible factors of χ_u of bounded height Using the method described in Subsection 4.2 above, we compute all irreducible factors of χ_u of height bounded by

$$[K:\mathbb{Q}](H+ht(u)).$$

Let us observe that these factors are given by their coefficient lists and that the coefficients are given by their binary encoding.

Task 2.- Selecting factors with some zero in K We make use of the factoring procedures described in [Lan85, LM85] or [Len83]. Thus, from the output of Task 1, we choose just the factors g of χ_u satisfying :

- g contains a root in k, and
- $ht(g) \leq [K:\mathbb{Q}](H+ht(u))$.

Let us observe that the running time required to perform this task is polynomial in $c(K)[K:\mathbb{Q}](H+ht(u))D$, where D is the degree of the solution variety V, and $c(K)$ is the height of the field K. As the field K is fixed in our considerations, we will omit this quantity from now on.

Task 3.-Computing irreducible components of bounded height Let $\mathcal{F} := \{g_1, \ldots, g_s\} \subset \mathbb{Z}[T]$ be the output of Task 2, i.e. a list of irreducible factors of χ_u of bounded height having a root in K. Now, for every $g \in \mathcal{F}$, we apply the following procedure :
Let $C(g)$ be the companion matrix of g. For every i, $1 \leq i \leq n$, let us introduce the matrices

$$M_i := \rho^{-1} v_i(C(g)).$$

Let $q_1, \ldots, q_n \in \mathbb{Z}[T]$ be the characteristic polynomials of the matrices $M_1, \ldots, M_n$. Let $\zeta \in V_K(f_1, \ldots, f_n)$ be a smooth zero and $V_\zeta \subset V_K(f_1, \ldots, f_n)$ the $\mathbb{Q}$–definable irreducible component of $V_K(f_1, \ldots, f_n)$ that contains ζ. Let us assume that V_ζ is identified with the irreducible factor g of χ_u according to the rules described in Lemma 65 above. Let us finally assume $\zeta := (\zeta_1, \ldots, \zeta_n)$. Then, we obviously have the following property :
For every i, $1 \leq i \leq n$, the minimal polynomial of the matrix M_i is the minimal polynomial of ζ_i over $\mathbb{Q}$, and the characteristic polynomial of M_i is a power of the minimal polynomial of $\zeta_i \in K$ over $\mathbb{Q}$.
Now, we proceed as follows. Applying the factoring procedure described in Subsection 4.2 above, we verify for every i, $1 \leq i \leq n$, whether the polynomial q_i has any irreducible factor (the only one if any) of height at most H.
In the affirmative case, we have

$$ht(\zeta_i) \leq (\log_2(d+1)+H)[K:\mathbb{Q}] \text{ and } ht(\zeta) \leq n(\log_2(d+1)+H)[K:\mathbb{Q}].$$

Thus, we select all those irreducible factors g of the list $\mathcal{F}$ above, such that

- $ht(\zeta) \leq n(\log_2(d+1)+H)[K:\mathbb{Q}]$,
- $ht(g) \leq [K:\mathbb{Q}](H+ht(u))$, and
- K contains a root of g.

This can be done in time polynomial in the quantities :

$$[K:\mathbb{Q}]\; n\; d\; L\; \delta\; H.$$

Task 4.- Computing bounded height parametrizations Let $\mathcal{F}_1 := \{g_1, \ldots, g_{s_1}\}$ be the output of Task 3. Now, for every $g \in \mathcal{F}_1$ we perform the following task.
Using the technical tool described in [Dix82] (cf. also [Häg98, HM97]) and Lemma 65, we may compute

- a non–zero integer $\bar{\rho} \in \mathbb{Z} \setminus \{0\}$ and
- univariate polynomials $w_1, \ldots, w_n \in \mathbb{Z}[T]$,

such that the following holds :

i) $ht(\bar{\rho}), ht(w_1), \ldots, ht(w_n)$ are bounded by a polynomial in the quantities $[K : \mathbb{Q}]nd\deg(g)H$,

ii) $\deg(W_i) \leq \deg(g) - 1$ for all i, $1 \leq i \leq n$.

iii) Let $\zeta \in V_K(f_1, \ldots, f_n)$ be the smooth K–rational zero of the system F associated to the irreducible factor g according to Lemma 65 above. Let V_ζ be the $\mathbb{Q}$–definable irreducible component of $V_K(f_1, \ldots, f_n)$ that contains ζ. Then, the following is a biregular isomorphism :

$$\mathcal{U}|_{V_\zeta} : V_\zeta \subset \mathbb{C}^n \to \{t \in \mathbb{C} : g(t) = 0\} \text{ and } \left(\mathcal{U}|_{V_\zeta}\right)^{-1} := (\bar{\rho}^{-1}w_1(t), \ldots, \bar{\rho}^{-1}w_n(t)).$$

Task 5.- Computing approximate zeros of univariate polynomials For this task, we consider the univariate polynomial with integer coefficients

$$f(T) := \prod_{g \in \mathcal{F}} g \in \mathbb{Z}[T],$$

where $\mathcal{F}_1$ is the output of Task 3. Thus, we compute approximate zeros of the univariate polynomial f. This can be done by means of any of the procedures described for instance in [BCSS98a, Ren87, Sch86, Sch81, Sma81, Sma86a]. The running time of any of these procedures is polynomial in

$$n\ [K : \mathbb{Q}]\ D\ H.$$

Task 6.- Computing approximate zeros in the multivariate case Now, we recall Theorem 11 in Subsection 3.3 above, to conclude that for every smooth K–rational zero $\zeta \in V_K(f_1, \ldots, f_n)$ the following holds :

$$\log_2 \gamma(F, \zeta) \leq (nd)^3[K : \mathbb{Q}](h + ht(\zeta)).$$

Now, let $\mathcal{F}_1 := \{g_1, \ldots, g_{s_1}\}$ be the list of irreducible factors of χ_u computed after Task 3.
For every $g \in \mathcal{F}_1$, we apply :

i) Task 4 to compute the parametrization of bounded height,
i.e. $\bar{\rho} \in \mathbb{Z} \setminus \{0\}$ and $w_1, \ldots, w_n \in \mathbb{Z}[T]$.

ii) Task 5 to compute for every zero of g an approximate zero.

Let us assume $\zeta \in V_K(f_1, \ldots, f_n)$ be the smooth K–rational zero associated to g according to the rules of Lemma 65 above. Let V_ζ be the $\mathbb{Q}$–definable irreducible component of $V(f_1, \ldots, f_n)$ containing ζ.
Next, let $z \in \mathbb{Q}[i]$ be an approximate zero of $u(\zeta)$ computed by applying Task 5 to g. For sake of simplicity we may assume that $|u(\zeta) - z| < 1$ and that the height of z is polynomial in the following quantities : $ht(g)ht(\zeta)[K : \mathbb{Q}]\ n\ d$.
Finally, let us observe that $\zeta := (\bar{\rho}^{-1}w_1(u(\zeta)), \ldots, \bar{\rho}^{-1}w_n(u(\zeta)))$ and for every $x \in \mathbb{Q}[i]$, the following inequality holds :

$$\|\zeta - (\bar{\rho}^{-1}w_1(x), \ldots, \bar{\rho}^{-1}w_n(x))\| \leq n2^{wt(w_i)}\|x - u(\zeta)\|.$$

Then, we may apply the procedure described in Subsection 4.3 to compute a point $x \in \mathbb{Q}[i]$ satisfying

$$\|x - u(\zeta)\| < \epsilon,$$

where ϵ satisfies $n2^{wt(w_i)}\epsilon < \frac{3-\sqrt{7}}{2\gamma(F,\zeta)}$.
Using the previous bounds, we observe that there exists a universal constant $c_7 > 0$ such that if $\log_2 \epsilon < ([K : \mathbb{Q}]ndHw)^{c_7}$ holds, then the point $\bar{z} \in \mathbb{Q}[i]^n$ given by $\bar{z} := (\bar{\rho}^{-1}w_1(x), \ldots, \bar{\rho}^{-1}w_n(x))$ is an approximate zero of the system F with associated ζ, i.e.

$$\|\bar{z} - \zeta\| < \frac{3 - \sqrt{7}}{2\gamma(F, \zeta)}.$$

The running time of this task is polynomial in the following quantities :

$$[K : \mathbb{Q}] \; n \; d \; w \; H \; \log_2 \epsilon,$$

and the bounds above also show that $\log_2 \epsilon$ is polynomially bounded in the same quantities. ■

4.5 From Newton's to Kronecker's solution

In this Subsection we show Theorem 19 of the Introduction. This statement is a consequence of the following Theorem :

Theorem 66 (From Approximate Zeros to Geometric Solution) *There exists a bounded error probability Turing machine M which performs the following task :*
Suppose given as input a sequence $F := (f_1, \ldots, f_n)$ of multivariate polynomial with integer coefficients of degree at most d and (logarithmic) weight at most w satisfying the following properties :

- *the polynomials $f_1, \ldots, f_n$ are given by a division–free non–scalar straight–line program Γ of length L, non–scalar depth ℓ and parameters in $\{-1, 0, 1\}$,*
- *the sequence $f_1, \ldots, f_n \in \mathbb{Z}[X_1, \ldots, X_n]$ is a smooth regular sequence,*

and a point $z \in \mathbb{Q}[i]^n$ in binary encoding which is an approximate zero of the system F associated to some smooth K–rational zero $\zeta \in V_K(f_1, \ldots, f_n)$ with respect to the archimedean absolute value $\dot{||} : K \longrightarrow \mathbb{R}$ induced on K by the standard inclusion $i : K \hookrightarrow \mathbb{C}$. Let us also assume that z satisfies the γ–Theorem, namely

$$\|\zeta - z\| \leq \frac{3 - \sqrt{7}}{2\gamma(F, \zeta)}.$$

The machine M then outputs a Kronecker description of the $\mathbb{Q}$–definable irreducible component V_ζ of $V_K(f_1, \ldots, f_n)$ containing $\zeta \in V_\zeta$. The running time of M is polynomial in the following quantities :

$$w \; n \; d \; L \; ht(\zeta) \deg(V_\zeta) ht(z).$$

Proof.– The proof combines a method of reconstruction of minimal equations from diophantine approximations (cf. [KLL84, KLL88]) with a technical tool introduced in [KP94, KP96].
Let us introduced new variables $T_1, \ldots, T_n$. We denote by K_T the quotient field of the ring $\mathbb{Z}[T_1, \ldots, T_n]$ and by $\mathbb{K}_T$ an algebraic closure of it.
Let $\mathcal{U} := T_1X_1 + \ldots + T_nX_n \in \mathbb{Z}[T_1, \ldots, T_n, X_1, \ldots, T_n]$ be a generic projection. Let $V_\zeta \subset V(f_1, \ldots, f_n)$ be the $\mathbb{Q}$–definable irreducible component of $V(f_1, \ldots, f_n)$ containing the smooth

K–rational zero $\zeta \in V_K(f_1, \ldots, f_n)$. The Chow polynomial of V_ζ is the homogeneous polynomial of degree $\deg(V_\zeta)$ given by the following identity :

$$\chi_{\mathcal{U},\zeta}(T_1, \ldots, T_n, Z) := \prod_{\alpha \in \mathcal{V}_\zeta} (Z - (T_1\alpha_1 + \ldots + T_n\alpha_n)),$$

where $\alpha := (\alpha_1, \ldots, \alpha_n)$ runs over all complex points in V_ζ. For every $t := (t_1, \ldots, t_n) \in \mathbb{Z}^n$ and for every i, $1 \leq i \leq n$ we introduce the following polynomials :

$$p_i(t, Z) := \chi_{\mathcal{U},\zeta}(T_1, \ldots, T_{i-1}, 0, T_{i+1}, \ldots, T_n, Z) \text{ and } q_i := \chi_{\mathcal{U}}(0, \ldots, {}^{i)}\, 1, \ldots, 0, T) = \prod_{\alpha \in \mathcal{V}_\zeta} (Z - \alpha_i).$$

Finally, we introduce for every i, $1 \leq i \leq n$, and every $t := (t_1, \ldots, t_n) \in \mathbb{Z}^n$ the following family of planar algebraic sets :

$$V_i(t) := \{(x, y) \in \mathbb{K}^2 : q_i(x) = 0,\ p_i(t, y) = 0\}.$$

Now, we have the following two statement :

Lemma 67 *[KP94, KP96] With the same notations and assumptions as above, there exists a multivariate polynomial $F \in \mathbb{Z}[T_1, \ldots, T_n]$ of degree at most $n \deg(V_\zeta)^2$, such that the following holds :*
For every $t := (t_1, \ldots, t_n) \in \mathbb{Z}^n$ satisfying $F(t_1, \ldots, t_n) \neq 0$ holds : for every i, $1 \leq i \leq n$, the linear form $u_i := X + t_iY$ is a primitive element of the residue ring

$$\mathbb{Q}[X, Y]/\sqrt{p_i(t, X), q_i(Y)},$$

where $\sqrt{\ }$ stands for the radical of this ideal.

Moreover, the polynomial F can be computed from the coefficients of the polynomials $p_i(t, X)$ and $q_i(Y)$ in time polynomial in the following quantities :

$$ht(t) \deg(V_\zeta)\ n\ ht(\zeta).$$

Let us observe that for every $t := (t_1, \ldots, t_n) \in \mathbb{Z}^n$ satisfying $F(t) \neq 0$ the following linear form

$$\mathcal{U} := t_1X_1 + \ldots + t_nX_n \in \mathbb{Z}[X_1, \ldots, X_n]$$

is a primitive element of the residue ring

$$\mathbb{Q}[V_\zeta] := \mathbb{Q}[X_!, \ldots, X_n]/I(V_\zeta), \text{ where } I(V_\zeta) := \{g \in \mathbb{Q}[X_1, \ldots, X_n] : g|_{V_\zeta} \equiv 0\}.$$

Now, to find a point $t \in \mathbb{Z}^n$ that satisfies $F(t) \neq 0$, we can make use of any of the so–called probabilistic zero test for polynomials. We may apply for instance the following Lemma, due to [Sch79, Zip79].

Lemma 68 (Zippel–Schwartz) *Let $F \in \mathbb{Z}[T_1, \ldots, T_n]$ be as above and let*

$$\mathcal{A} := \{1, \ldots, (n \deg(\mathcal{V}_\zeta)^{c_8}\}^n \subset \mathbb{Z}^n$$

be a subset of integers of low height (where $c_8 > 0$ is a suitable universal constant). Then, choosing (at random) a point $t \in \mathcal{A}$, the probability that $F(t) = 0$ is strictly less than $\frac{1}{2}$.

Now we can exhibit a procedure which proves the claims made in Theorem 66.
First of all, let us choose at random a sequence of integer numbers $t := (t_1, \ldots, t_n) \in \mathbb{Z}^n$, such that

$$|t_i| \leq (n \deg(V_\zeta))^{c_8},\ \text{for all } i,\ 1 \leq i \leq n,$$

where $c_8 > 0$ is the universal constant of Lemma 68 above. For every i, $1 \leq i \leq n$, let us define the following algebraic numbers :

$$\alpha_i := t_1\zeta_1 + \ldots + t_{i-1}\zeta_{i-1} + t_{i+1}\zeta_{i+1} + \ldots + t_n\zeta_n \text{ and } \beta_i := \zeta_i,$$

where $\zeta := (\zeta_1, \ldots, \zeta_n) \in K^n$ is the actual smooth K–rational zero.
Now, we apply the method described in Subsection 4.3 above to compute an approximate zero $\bar{z} \in \mathbb{Q}[i]^n$ of the system F with associated zero ζ, such that the following holds :

$$\|\bar{z} - \zeta\| \leq \epsilon^{-1}.$$

Let us write $\bar{z} := (z_1, \ldots, z_n) \in \mathbb{Q}[i]^n$. For every i, $1 \leq i \leq n$, we define the following Gaussian rationals

$$x_i := t_1z_1 + \ldots + t_{i-1}z_{i-1} + t_{i+1}z_{i+1} + \ldots + t_nz_n \text{ and } y_i := z_i.$$

Then, we have $\|x_i - \alpha_i\| \leq n(n\deg(V_\zeta))_8^c\epsilon^{-1}$ and $\|y_i - \beta_i\| \leq \epsilon^{-1}$.
Now, choosing $\epsilon \in \mathbb{N}$, $\epsilon > 1$ such that $\log_2 \epsilon > [(10 + c_8)d\deg(V_\zeta)^2(n + ht(\zeta))]$, we conclude

$$\|x_i - \alpha_i\| \leq \frac{1}{2^{9\deg(\alpha_i)^2 ht(\alpha_i)}} \text{ and } \|y_i - \beta_i\| \leq \frac{1}{2^{9\deg(\beta_i)^2 ht(\beta_i)}}.$$

Then, we apply the procedure described in the following Theorem (see [KLL84] for details) :

Theorem 69 *Let $\alpha \in \mathbb{C}$ be an algebraic number of (logarithmic) height $ht(\alpha)$ and degree $d := [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and let $\bar{\alpha} \in \mathbb{Q}[i]$ be an approximation such that :*

$$|\alpha - \bar{\alpha}| < 2^{-2d^2+3d+4dh}.$$

Then, there exists a polynomial time algorithm which, taking as input the approximation $\bar{\alpha}$, computes the minimal polynomial of α.

Thus, we have computed for every i, $1 \leq i \leq n$, the following univariate polynomials :

- $p_i(X) \in \mathbb{Z}[X]$, the minimal polynomial of α_i over $\mathbb{Q}$, and
- $q_i(Y) \in \mathbb{Z}[Y]$, the minimal polynomial of β_i over $\mathbb{Q}$.

We apply a similar procedure to compute the minimal polynomial $p(Z) \in \mathbb{Q}[Z]$ of the algebraic number

$$u := t_1\zeta_1 + \ldots t_n\zeta_n \in K.$$

Next, we test whether for every i, $1 \leq i \leq n$, the linear form $X + t_iY$ is a primitive element of the residue ring

$$\mathbb{Q}[X, Y]/\sqrt{p_i(X), q_i(Y)}.$$

In the affirmative case, we apply the following Lemma, otherwise, we choose a different point $t \in \mathbb{Z}^n$.

Lemma 70 *[KP96, KP94] With the previous notations and assumptions, there exists a procedure that computes the following items :*

i) A non–zero integer $\rho \in \mathbb{Z}$, and

ii) univariate polynomials $v_1, \ldots, v_n \in \mathbb{Z}[T]$,

such that for every i, $1 \leq i \leq n$ holds :

$$\rho Y - v_i(X + Z_iY) \in \sqrt{(p_i, q_i)} \text{ in } \mathbb{Q}[X, Y].$$

The running time of this procedure is polynomial in the following quantities

$$ht(t)\max\{\deg(p_i), \deg(q_i)\}\max\{ht(p_i), ht(q_i)\}.$$

Finally, let us define the linear form $u := t_1X_1 + \ldots + t_nX_n \in \mathbb{Q}[X_1, \ldots, X_n]$ and the ideal $I := (p(u), \rho X_1 - v_1(u), \ldots, \rho X_n - v_n(u)) \subset \mathbb{Q}[X_1, \ldots, X_n]$.
The procedure outputs the above list if and only if $I \subset (f_1, \ldots, f_n)$. This inclusion can be tested by the following equivalence :

$$I \subset (f_1, \ldots, f_n) \text{ if and only if } p|f_i(\rho^{-1}v_1(u), \ldots, \rho^{-1}v_n(u)), \forall i, 1 \leq i \leq n.$$

The output is obviously the Kronecker encoding of the $\mathbb{Q}$–definable irreducible component of V containing ζ. ■

5 Lagrange resolvent

Let $f := a_dX^d + \cdots + a_0 \in \mathbb{Z}[X]$ be a squarefree univariate polynomial of degree d with integer coefficients. As f is square free, we obviously have $\alpha_i \neq \alpha_j$ for all i, j, $1 \leq i, j \leq d$ and $i \neq j$. Let $\alpha_1, \ldots, \alpha_d \in \mathbb{C}$ be the complex roots of the polynomial f. We obviously have the following identity :

$$f(X) = a_d \prod_{i=1}^{d} (X - \alpha_i) \in \mathbb{Z}[X].$$

Let $\sigma_0, \ldots, \sigma_{d-1} \in \mathbb{Z}[X_1, \ldots, X_d]$ be the elementary symmetric functions, i.e. the polynomial mappings satisfying the following identities :

$$\sigma_i(\alpha_1, \ldots, \alpha_d) = a_d^{-1}a_i, \quad \forall i, 0 \leq i \leq d-1.$$

The normal closure of f (also called the splitting field of f) is the smallest number field $K(f) \subseteq \mathbb{C}$ that contains all complex roots of f, i.e. the following holds :

$$K(f) = \mathbb{Q}(\alpha_1, \ldots, \alpha_d).$$

The Galois group of f is the group $\mathrm{Gal}_{\mathbb{Q}}(f)$ of all field automorphism $\tau : K(f) \to K(f)$ such that its restriction to $\mathbb{Q}$ is the identity. The order of the Galois group $\mathrm{Gal}_{\mathbb{Q}}(f)$ agrees with the dimension of $K(f)$ as a $\mathbb{Q}-$vectorspace, i.e. $\#\mathrm{Gal}_{\mathbb{Q}}(f) = [K(f) : \mathbb{Q}]$.
The Cayley–Lagrange resolvent of the polynomial f is a multivariate homogeneous polynomial which rational coefficients that represents both the Galois group $\mathrm{Gal}_{\mathbb{Q}}(f)$ and the normal closure $K(f)$. Namely, the Cayley–Lagrange resolvent is a polynomial $\mathrm{LAG}_f(T_1, \ldots, T_d, Z) \in \mathbb{Q}[T_1, \ldots, T_d, Z]$ of degree $[K(f) : \mathbb{Q}]$ given by the following identity :

$$\mathrm{LAG}_f(T_1, \ldots, T_d, Z) := \prod_{\tau \in \mathrm{Gal}_{\mathbb{Q}}(f)} (Z - (T_1\tau(\alpha_1) + \cdots + T_d\tau(\alpha_d)), \tau \in \mathrm{Gal}_{\mathbb{Q}}(f).$$

The polynomial $\mathrm{LAG}_f(T_1, \ldots, T_d, Z)$ is homogeneous and a monic polynomial with respect to the variable Z. The total degree of $\mathrm{LAG}_f(T_1, \ldots, T_d, Z)$ is the order of the Galois group $\mathrm{Gal}_{\mathbb{Q}}(f)$. The classical Lagrange resolvent is simply the univariate polynomial :

$$\gamma(Z) := \mathrm{LAG}_f(1, \alpha, \ldots, \alpha^{d-1}, Z),$$

where α is a root of unity. The Cayley–Lagrange resolvent satisfies the following additional property, which explains why LAG_f characterizes $K(f)$.

Proposition 71 *With the same assumptions and notations as above, let $D(T_1, \ldots, T_d) \in \mathbb{Q}[T_1, \ldots, T_d]$ be the discriminant of LAG_f with respect to the variable Z. Then, for every $\underline{t} := (t_1, \ldots, t_d) \in \mathbb{Z}^d$ satisfying $D(\underline{t}) \neq 0$, the following holds :*

- *The algebraic number $\theta := t_1\alpha_1 + \ldots + t_d\alpha_d$ is a primitive element of $K(f)$ over $\mathbb{Q}$, i.e. $K(f) = \mathbb{Q}(\theta)$.*
- *The univariate polynomial $p(Z) := LAG_f(t_1, \ldots, t_d, Z) \in \mathbb{Z}[Z]$ satisfies $K(f) := \mathbb{Q}[Z]/p(Z)$.*

In fact, using an strategy similar to that of [KP96] and Lemma 70 we may compute from the Cayley–Lagrange resolvent both a primitive element θ of $K(f)$ and a description of the roots $\alpha_1, \ldots, \alpha_d$ in terms of θ in time polynomial in $[K(f) : \mathbb{Q}]h$.
There is a more geometrical approach to the notion of Cayley–Lagrange resolvent. Let us consider the following zero–dimensional algebra (called the universal Resolution Algebra, cf. [Duc97]) :

$$\mathcal{U}(f) := \mathbb{Q}[X_1, \ldots, X_d]/I(f),$$

where $I(f)$ is the zero–dimensional ideal generated by the polynomials $I(f) := (F_0, \ldots, F_{d-1})$ where $F_0, \ldots, F_{d-1}$ are given by the following identity :

$$F_i := \sigma_i(X_1, \ldots, X_d) - a_d^{-1}a_0 \in \mathbb{Q}[X_1, \ldots, X_n] \text{ for every } i, 0 \leq i \leq d-1.$$

Let $V_f := V(F_0, \ldots, F_{d-1}) \subset \mathbb{C}^d$ be the set of all common zeros of the system of equations $F_0 = 0, \ldots, F_{d-1} = 0$. The algebraic set V_f is $\mathbb{Q}$–definable. Let us consider a $\mathbb{Q}$–definable irreducible component $\mathcal{W} \subset V_f$ of V_f. We denote by $CC_{\mathcal{W}}(T_1, \ldots, T_d, Z) \in \mathbb{Q}[T_1, \ldots, T_d, Z]$ the Cayley–Chow polynomial of the algebraic variety $\mathcal{W}$. Namely, the following identity holds :

$$CC_{\mathcal{W}}(T_1, \ldots, T_d, Z) := \prod_{\alpha \in \mathcal{W}} (Z - (T_1\alpha_1 + \ldots + T_n\alpha_n)),$$

where $\alpha := (\alpha_1, \ldots, \alpha_d) \in \mathbb{C}^n$. Then, the following Proposition holds :

Proposition 72 *With the same assumptions and notations as above, for every $\mathbb{Q}$–definable irreducible component $\mathcal{W}$ of V_f, the following holds :*

$$LAG_f(T_1, \ldots, T_d, Z) = CC_{\mathcal{W}}(T_1, \ldots, T_d, Z)$$

In particular, $\deg \mathcal{W} = \#Gal_{\mathbb{Q}}(f) = [K(f) : \mathbb{Q}]$.

Let us observe that a Kronecker description of any $\mathbb{Q}$–definable irreducible component of V_f immediately yields both the Cayley–Lagrange resolvent $\mathrm{LAG}_f(T_1, \ldots, T_d, Z)$ and a full description (via a primitive element) of the normal closure $K(f)$.
Now, we introduce a new collection of multivariate polynomial equations in $\mathbb{Q}[X_1, \ldots, X_d]$:

$$g_i(X_1, \ldots, X_d) := f(X_i), \text{ for every } i, 1 \leq i \leq d.$$

Let us consider now the zero–dimensional algebra : $B(f) := \mathbb{Q}[X_1, \ldots, X_d]/(g_1, \ldots, g_d)$.
Let $V'_f \subset \mathbb{C}^d$ be the $\mathbb{Q}$–definable algebraic set formed by all common complex zeros of the system of equations :

$$g_1 = 0, \ldots, g_d = 0.$$

Then, the following statement holds :

Lemma 73 *Let $\zeta := (\zeta_1, \ldots, \zeta_d) \in V'_f$ be a complex point such that $\zeta_i \neq \zeta_j$, $\forall i \neq j$, $1 \leq i, j \leq d$. Let $\mathcal{W}_\zeta \subset V'_f$ be the $\mathbb{Q}$–definable irreducible component of V'_f containing ζ. Then, $\mathcal{W}_\zeta$ is also a $\mathbb{Q}$–definable irreducible component of V_f.*

In particular, we conclude that $\mathrm{LAG}_f(T_1, \ldots, T_d, Z)$ and a primitive element of $K(f)$ can be easily computed from a Kronecker's description of any $\mathbb{Q}$–definable irreducible component $\mathcal{W}_\zeta$ of V'_f, where

$$\zeta := (\zeta_1, \ldots, \zeta_d) \in V'_f \subset \mathbb{C}^d \text{ and } \zeta_i \neq \zeta_j \ \text{ for all } i \neq j.$$

Moreover, we obviously have

$$\deg \mathcal{W}_\zeta = [K(f):\mathbb{Q}] = \#\mathrm{Gal}_{\mathbb{Q}}(f) \text{ and } ht(\zeta) \leq \log(d+1) + h.$$

Thus, applying the methods and techniques described in Subsection 4.5 above, we conclude that both the Cayley-Lagrange resolvent of f over $\mathbb{Q}$ and a description of $K(f)$ by a primitive element can be computed from an approximate zero $z \in \mathbb{Q}[i]^d$ of the system G with associated zero $\zeta := (\zeta_1, \ldots, \zeta_d) \in V'_f$, such that

$$\zeta_i \neq \zeta_j, \quad \text{for all } i \neq j.$$

The running time of this procedure is polynomial in

$$d\, h\, \#\mathrm{Gal}_{\mathbb{Q}}(f).$$

Now, we have the following statement.

Lemma 74 *With the same assumptions and notations as above, let $\zeta = (\zeta_1, \ldots, \zeta_d) \in V'_f$ be a zero of the system G. Then, for every $\underline{z} := (z_1, \ldots, z_d) \in \mathbb{Q}[i]^d$, the following are equivalent properties :*

i) For every $i, 1 \leq i \leq d$, z_i is an approximate zero of f with associate zero $\zeta_i \in \mathbb{C}$.

ii) The point $\underline{z} \in \mathbb{Q}[i]^d$ is an approximate zero of G with associate zero $\zeta := (\zeta_1, \ldots, \zeta_d)$.

Proof.– This is an obvious fact since the Newton operator N_G splits as a direct sum of the univariate Newton operators $N_{g_1}, \ldots, N_{g_d}$. Namely, the following holds :

$$N_G(\underline{x}) := \begin{pmatrix} N_{g_1}(x_1) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & N_{g_d}(x_d) \end{pmatrix}$$

for every $\underline{x} := (x_1, \ldots, x_d) \in \mathbb{C}^d$. ■

Thus, the Cayley–Lagrange resolvent of f over $\mathbb{Q}$ and the splitting field $K(f)$ can be computed just by computing a list $\underline{z} := (z_1, \ldots, z_d) \in \mathbb{Q}[i]^d$ of Gauss rationals, such that the following two properties hold :

- For every i, $1 \leq i \leq d$, z_i is an approximate zero of f with associated zero $\zeta_i \in \mathbb{C}$.
- For every i, j, $1 \leq i, j \leq d$, $i \neq j$, $\zeta_i \neq \zeta_j$.

This task can be performed in time polynomial in the degree d and the (logarithmic) weight $wt(f)$ of f.
Applying the method described in Subsection 4.5, Theorem 66, the next Theorem follows.

Theorem 75 *There exists a bounded error probability Turing machine M that performs the following task : Given as input a squarefree univariate polynomial $f := a_d X^d +, \ldots, +a_0 \in \mathbb{Z}[X]$ with integer coefficients, of degree d and height at most h, the machine M outputs :*

i) a description of the normal closure of f over $\mathbb{Q}$, $K(f)$, and

ii) the Cayley–Lagrange resolvent of f over $\mathbb{Q}$.

The running time of M is polynomial in the following quantities :

$$d\, h\, \#Gal_{\mathbb{Q}}(f).$$

References

[AH92] Leonard M. Adleman and Ming-Deh A. Huang. *Primality testing and abelian varieties over finite fields.* Springer-Verlag, Berlin, 1992.

[AM93] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, 1993.

[Art51] Emil Artin. *Algebraic numbers and algebraic functions. I.* Institute for Mathematics and Mechanics, New York University, New York, 1951.

[BCSS96] Blum, Cucker, Shub, and Smale. Algebraic settings for the problem "P <> NP?". In Renegar, Shub, and Smale, editors, *The Mathematics of Numerical Analysis: 1995 (25th) AMS-SIAM Summer Seminar in Applied Mathematics (Lectures in Applied Mathematics, Volume 32), American Mathematical Society.* 1996.

[BCSS98a] Lenore Blum, Felipe Cucker, Michael Shub, and Steve Smale. *Complexity and real computation.* Springer-Verlag, New York, 1998. With a foreword by Richard M. Karp.

[BCSS98b] Lenore Blum, Felipe Cucker, Mike Shub, and Steve Smale. Algebraic setting for the problem $P \neq NP$. preprint, 20 pages, 1998.

[BDG88] J. L. Balcázar, J. Díaz, and J. Gabarró. *Structural complexity I*, volume 11 of *EATCS*. Springer, 1988.

[Ber75] D. N. Bernstein. The number of roots of a system of equations. *Funkts. Anal. Pril.*, 9:1–4, 1975.

[BGS93] J.-B. Bost, H. Gillet, and C. Soulé. Heights of projective varieties and positive green forms. Manuscript I.H.E.S., 1993.

[BVdPV96] E. Bombieri, A. J. Van der Poorten, and J. D. Vaaler. Effective measures of irrationality for cubic extensions of number fields. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 23(2):211–248, 1996.

[Cam] Paul Camion. Factorisation des polynômes de $\mathbf{f}_q[X]$. *Rev. CETHEDEC Cahier*, 1981(2):5–21 (1982).

[Cam83] Paul F. Camion. Improving an algorithm for factoring polynomials over a finite field and constructing large irreducible polynomials. *IEEE Trans. Inform. Theory*, 29(3):378–385, 1983.

[Cas97] J. W. S. Cassels. *An introduction to the geometry of numbers.* Springer-Verlag, Berlin, 1997. Corrected reprint of the 1971 edition.

[CGH$^+$99] D. Castro, M. Giusti, J. Heintz, G. Matera, and L. M. Pardo. Data structures and smooth interpolation procedures in elimination theory. Manuscript, 1999.

[Cia82] Philippe G. Ciarlet. *Introduction à l'analyse numérique matricielle et à l'optimisation.* Masson, Paris, 1982.

[CZ81] David G. Cantor and Hans Zassenhaus. A new algorithm for factoring polynomials over finite fields. *Math. Comp.*, 36(154):587–592, 1981.

[Ded96] Jean-Pierre Dedieu. Approximate solutions of numerical problems, condition number analysis and condition number theorem. In *The mathematics of numerical analysis (Park City, UT, 1995)*, pages 263–283. Amer. Math. Soc., Providence, RI, 1996.

[Ded97a] Jean-Pierre Dedieu. Condition number analysis for sparse polynomial systems. In *Foundations of computational mathematics (Rio de Janeiro, 1997)*, pages 75–101. Springer, Berlin, 1997.

[Ded97b] Jean-Pierre Dedieu. Condition operators, condition numbers, and condition number theorem for the generalized eigenvalue problem. *Linear Algebra Appl.*, 263:1–24, 1997.

[Ded97c] Jean-Pierre Dedieu. Estimations for the separation number of a polynomial system. *J. Symbolic Comput.*, 24(6):683–693, 1997.

[Dem89] Demazure. *Catastrophes et Bifurcations.* Ellipses–X École Polytechnique, 1989.

[Dix82] J. Dixon. Exact solution of linear equations using p-adic expansions. *Numer. Math.*, 40:137–141, 1982.

[DSa] J. P. Dedieu and M. Shub. Newton's method for overdetermined systems of equations. *Math. Comp.*

[DSb] Jean-Pierre Dedieu and Mike Shub. On simple double zeros and badly conditioned zeros of analytic functions of n variables. *Math. Comp.*, page 0 (electronic).

[DS98] Jean-Pierre Dedieu and Steve Smale. Some lower bounds for the complexity of continuation methods. *J. Complexity*, 14(4):454–465, 1998.

[Duc97] L. Ducos. *Effectivité en Thréorie de Galois. Sous-resultants.* PhD thesis, Université de Poitiers, 1997.

[EY36] C. Eckardt and G. Young. The approximation of one matrix by another of lower rank. *Psichometruka*, 1:211–218, 1936.

[FGS95] N. Fitchas, M. Giusti, and F. Smietanski. Sur la complexité du théorème des zéros. In J. Guddat, editor, *Approximation and Optimization in the Caribbean II, Proceedings 2nd Int. Conf. on Non-Linear Optimization and Approximation*, volume 8 of *Approximation and Optimization*, pages 247–329. Peter Lange Verlag, Frankfurt am Main, 1995.

[Ful84] W. Fulton. *Intersection Theory.* Number 3 in Ergebnisse der Mathematik. Springer, 2 edition, 1984.

[GH91] M. Giusti and J. Heintz. Algorithmes - disons rapides - pour la décomposition d' une variété algébrique en composantes irréductibles et équidimensionelles. In T. Mora and C. Traverso, editors, *Proceedings of MEGA'90*, volume 94 of *Progress in Mathematics*, pages 169–194. Birkhäuser, 1991.

[GH93] M. Giusti and J. Heintz. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. In D. Eisenbud and L. Robbiano, editors, *Computational Algebraic Geometry and Commutative Algebra*, volume XXXIV of *Symposia Matematica*, pages 216–256. Cambridge University Press, 1993.

[GHH$^+$97] M. Giusti, K. Hägele, J. Heintz, J. E. Morais, J. L. Montaña, and L. M. Pardo. Lower bounds for diophantine approximation. In *Proceedings of MEGA'96*, volume 117,118, pages 277–317. Journal of Pure and Applied Algebra, 1997.

[GHM$^+$98] M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, and L. M. Pardo. Straight–line programs in geometric elimination theory. *J. of Pure and App. Algebra*, 124:101–146, 1998.

[GHMP95] M. Giusti, J. Heintz, J. E. Morais, and L. M. Pardo. When polynomial equation systems can be solved fast ? In G. Cohen, H. Giusti, and T. Mora, editors, *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings AAECC-11*, volume 948 of *LNCS*, pages 205–231. Springer, 1995.

[GHMP97] M. Giusti, J. Heintz, J. E. Morais, and L. M. Pardo. Le rôle des structures de données dans les problèmes d'élimination. *C. R. Acad. Sci. Paris*, 325:1223–1228, 1997.

[GS99] M. Giusti and E. Schost. Solving some over–determined systems. To appear in Proc. ISSAC, 1999.

[Häg98] K. Hägele. *Intrinsic height estimates for the Nullstellensatz.* PhD thesis, Universidad de Cantabria, Santander, Spain, 1998.

[Hei83] J. Heintz. Definability and fast quantifier elimination in algebraically closed fields. *Theor. Comput. Sci.*, 24(3):239–277, 1983.

[Hei89] J. Heintz. On the computational complexity of polynomials and bilinear mappings. A survey. In *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings of AAECC-5*, volume 356 of *LNCS*, pages 269–300. Springer, 1989.

[HM97] K. Hägele and J. L. Montaña. Polynomial random test for the equivalence problem of integers given by arithmetic circuits. Preprint 4/97 Depto. Matemáticas, Universidad de Cantabria, Santander, Spain, January 1997.

[HMPS00] K. Hägele, J.E. Morais, L.M. Pardo, and M. Sombra. On the intrinsic complexity of arithmetic nullstellensatz. *To appear in J. of Pure and App. Algebra*, Jan 2000.

[HS80] J. Heintz and C. P. Schnorr. Testing polynomials which are easy to compute. In *Proccedings of ACM 12th Symposium on Theory of Computing*, pages 262–272, 1980.

[HS82] J. Heintz and C. P. Schnorr. Testing polynomials which are easy to compute. In *Logic and Algorithmic*, volume 30 of *Monographie de l'Enseignement Mathématique*, pages 237–254, 1982.

[IM83] O. H. Ibarra and S. Moran. Equivalence of straight-line programs. *Journal of the ACM*, 30:217–228, 1983.

[Kal90] Erich Kaltofen. Polynomial factorization 1982–1986. In *Computers in mathematics (Stanford, CA, 1986)*, pages 285–309. Dekker, New York, 1990.

[Kal92] Erich Kaltofen. Polynomial factorization 1987–1991. In I. Simon, editor, *Proceedings of the 1st Latin American Symposium on Theoretical Informatics LATIN '92 (São Paulo, Brazil, April 1992)*, volume 583 of *LNCS*, pages 294–313, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong, 1992. Springer-Verlag.

[Kim] Myong Hi Kim. PhD thesis.

[KLL84] R. Kannan, A. K. Lenstra, and L. Lovasz. Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers. In *Proceedings of the 16th Ann. ACM Symposium on Theory of Computing (Washington, D.C.)*, pages 191–200, New York, 1984. ACM, ACM Press.

[KLL88] R. Kannan, A. K. Lenstra, and L. Lovász. Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers. *Math. Comp.*, 50(181):235–250, 1988.

[Kön03] J. König. *Einleitung in die allgemeine Theorie der algebraischen Grözen.* Druck und Verlag von B.G. Teubner,Leipzig., 1903.

[KP94] T. Krick and L. M. Pardo. Une approche informatique pour l' approximation diophantienne. *C. R. Acad. Sci. Paris*, 318(1):407–412, 1994.

[KP96] T. Krick and L. M. Pardo. A computational method for diophantine approximation. In L. González-Vega and T. Recio, editors, *Algorithms in Algebraic Geometry and Applications. Proceedings of MEGA'94*, volume 143 of *Progress in Mathematics*, pages 193–254. Birkhäuser Verlag, 1996.

[Kro82] L. Kronecker. Grundzüge einer arithmetischen theorie de algebraischen grössen. *J. reine angew. Math.*, 92:1–122, 1882.

[Kus76] A. G. Kushnirenko. Newton polytopes and the bezout theorem. *Funkts. Anal. Pril.*, 10(3), 1976.

[Lan83] S. Lang. *Fundamentals of Diophantine Geometry.* Springer, 1983.

[Lan85] S. Landau. Factoring polynomials over algebraic number fields. *SIAM J. Comp.*, 14:184–195, 1985.

[Len83] A. K. Lenstra. Factoring polynomials over algebraic number fields. In *Computer algebra (London, 1983)*, pages 245–254. Springer, Berlin, 1983.

[Len84] A. K. Lenstra. Polynomial factorization by root approximation. In John Fitch, editor, *Proceedings of the 3rd International Symposium on Symbolic and Algebraic Computation EUROSAM 84 (Cambridge, England, July 9-11, 1984)*, volume 174 of *LNCS*, pages 272–276, Berlin-Heidelberg-New York-London-Paris-Tokyo-Hong Kong, 1984. ACM SIGSAM, SAME, Springer-Verlag.

[LLL82a] A. K. Lenstra, H. W. Lenstra, and L. Lovasz. Factoring polynomials with rational coefficients. Technical Report 82-05, Mathematics Dept., University of Amsterdam, 1982.

[LLL82b] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Mathematische Ann.*, 261:513–534, 1982.

[LM85] S. Landau and G. L. Miller. Solvability by radicals is in polynomial time. *J. Comp. System Sci.*, 30:179–208, 1985.

[Mac16] F. S. Macauley. *The Algebraic Theory of Modular Systems.* Cambridge University Press, 1916.

[Mal93] G. Malajovich. *On the Complexity of Path-Following Newton Algorithms for Solving Systems of Polynomial Equations with Integer Coeficients.* PhD thesis, University of California at Berkeley, U.S.A., 1993.

[Mal94] G. Malajovich. On generalized newton algorithms: quadratic convergence, path-following and error analysis. *Theoretical Computer Science*, 133:65–84, 1994.

[Mal95] G. Malajovich. Worst possible condition number of polynomial systems. preprint 17 pages, 1995.

[McC76] P. J. McCarthy. *Algebraic Extensions of Fields.* Chelsea Publishing Comp., New York, 1976.

[Mig89] Maurice Mignotte. *Mathématiques pour le calcul formel.* Presses Universitaires de France, Paris, 1989.

[MMP96] J. L. Montaña, J. E. Morais, and L. M. Pardo. Lower bounds for arithmetic networks II: Sum of betti numbers. *Applicable Algebra in Engineering Communications and Computing*, 7:41–51, 1996.

[Mor90] François Morain. *Courbes elliptiques et tests de primalité.* Institut National de Recherche en Informatique et en Automatique (INRIA), Rocquencourt, 1990. Thèse, Université Claude Bernard-Lyon I, Lyon, 1990.

[Mor91] François Morain. Elliptic curves, primality proving and some titanic primes. *Astérisque*, (198-200):245–251 (1992), 1991. Journées Arithmétiques, 1989 (Luminy, 1989).

[Mor97] J. E. Morais. *Resolución eficaz de sistemas de ecuaciones polinomiales.* PhD thesis, Universidad de Cantabria, Santander, Spain, 1997.

[MP93] J. L. Montaña and L. M. Pardo. Lower bounds for arithmetic networks. In *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings of AAECC-4*, pages 1–24. Springer, 1993.

[MPR91] J. L. Montaña, L. M. Pardo, and T. Recio. The non-scalar model of complexity in computational geometry. In C. Traverso and T. Mora, editors, *Effective Methods in Algebraic Geometry, Proceedings of MEGA'90*, volume 94 of *Progress in Mathematics*, pages 347–361. Birkhäuser, 1991.

[Par95] L. M. Pardo. How lower and upper complexity bounds meet in elimination theory. In G. Cohen, H. Giusti, and T. Mora, editors, *Applied algebra, algebraic algorithms and error-correcting codes (Paris, 1995)*, volume 948 of *Lecture Notes in Computer Science*, pages 33–69. Springer, Berlin, 1995.

[Phi91] P. Philippon. Sur des hauteurs alternatives, I. *Math. Ann.*, 289:255–283, 1991.

[Phi94] P. Philippon. Sur des hauteurs alternatives, II. *Ann. Inst. Fourier, Grenoble*, 44(2):1043–1065, 1994.

[Phi95] P. Philippon. Sur des hauteurs alternatives, III. *J. Math. Pures Appl.*, 74:345–365, 1995.

[PZ89] M. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory.* Cambridge University Press, Cambridge, 1989.

[Ren87] James Renegar. On the worst-case arithmetic complexity of approximating zeros of polynomials. *Journal of Complexity*, 3(2):90–113, June 1987.

[Ros94] H. E. Rose. *A course in number theory.* The Clarendon Press Oxford University Press, New York, second edition, 1994.

[Sch79] J. T. Schwartz. Probabilistic algorithms for verification of polynomial identities. In *ISSAC '79: Proceedings of Int'l. Symp. on Symbolic and Algebraic Computation*, volume 72 of *Lecture Notes in Computer Science.* Springer-Verlag, 1979.

[Sch80] W. M. Schmidt. *Diophantine Approximation.* Springer Verlag, New York, 1980.

[Sch81] Arnold Schönhage. The fundamental theorem of algebra in terms of computational complexity. Preliminary report, Mathematisches Institut der Universität Tübingen, 1981.

[Sch86] Arnold Schönhage. Equation solving in terms of computational complexity. In *Proceedings of the International Congress of Mathematicians*, volume 3, page 40, 1986.

[SG86] J. Kilian S. Goldwasser. Almost all primes can be quickly certified. In *18th Annual ACM Symp. on Theory of Computing*, pages 316–329, 1986.

[Sma81] S. Smale. The fundamental theorem of algebra and complexity theory. *Bulletin of the Amer. Math. Soc.*, (4):1–36, 1981.

[Sma85] S. Smale. On the efficiency of algorithms of analysis. *Bull. of the AMS*, 13(2):87–121, 1985.

[Sma86a] S. Smale. Algorithms for solving equations. In *Proceedings of the International Congress of Mathematicians*, pages 172–195, Berkeley, California, USA, 1986.

[Sma86b] S. Smale. *Newton's method estimates from data at one point.* Springer, 1986.

[Som98] M. Sombra. *Estimaciones para el teorema de ceros de Hilbert.* PhD thesis, Universidad de Buenos Aires, Argentina, 1998.

[SS85] M. Shub and S. Smale. Computational complexity: on the geometry of polynomials and a theory of cost. I. *Ann Sci. École Norm. Sup.*, 18:107–142, 1985.

[SS86] M. Shub and S. Smale. Computational complexity: on the geometry of polynomials and a theory of cost. II. *SIAM Journal on Computing*, 15(1):145–161, 1986.

[SS93a] M. Shub and S. Smale. Complexity of Bézout's theorem I: Geometric aspects. *J. of the AMS*, 6(2):459–501, 1993.

[SS93b] M. Shub and S. Smale. Complexity of Bézout's theorem II: Volumes and probabilities. In *Proceeding effective methods in Algebraic Geometry*, volume 109 of *Progress in Mathematics*, pages 267–285. MEGA '92, Niece, Birkhäuser, 1993.

[SS93c] M. Shub and S. Smale. Complexity of Bézout's theorem III: Condition number and packing. *J. of Complexity*, 9:4–14, 1993.

[SS94a] M. Shub and S. Smale. Complexity of Bézout's theorem IV: Probability of success, extensions. *SIAM J. of Numer. Anal.*, to appear, 1994.

[SS94b] M. Shub and S. Smale. Complexity of Bézout's theorem V: Polynomial time. *Theor. Comp. Sci.*, 133:141–164, 1994.

[SS96] Michael Shub and Steve Smale. Complexity of Bezout's theorem. IV. probability of success and extensions. *SIAM Journal on Numerical Analysis*, 33(1):128–148, February 1996.

[Str90] V. Strassen. Algebraic complexity theory. In *Handbook of Theoretical Computer Science*, chapter 11, pages 634–671. Elsevier, 1990.

[Stu96] B. Sturmfels. *Gröbner bases and Convex Polytopes*, volume 8 of *University Lecture Series*. American Mathematical Society, 1996.

[Tyl94] S. Tyler. *The Lagrange Spectrum in Projective Space over a Local Field.* PhD thesis, University of Texas at Austin, 1994.

[Vog84] W. Vogel. *Results on Bézout's Theorem.* Tata Institute of Fundamental Research. Springer, 1984.

[Yak95a] Jean-Claude Yakoubsohn. Une constante universelle pour la convergence de la méthode de Newton. *C. R. Acad. Sci. Paris Sér. I Math.*, 320(3):385–390, 1995.

[Yak95b] Jean-Claude Yakoubsohn. A universal constant for the convergence of Newton's method and an application to the classical homotopy method. *Numer. Algorithms*, 9(3-4):223–244, 1995.

[Zar95] O. Zariski. *Algebraic Surfaces.* Classics in Mathematics. Springer, 1995.

[Zip79] R. Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings EUROSAM' 79*, number 72 in LNCS, pages 216–226. Springer, 1979.

[ZS58] Oscar Zariski and Pierre Samuel. *Commutative Algebra*, volume 1. D. Van Nostrand Co., Inc., Princeton, 1958. with the co-operation of I. S. Cohen.