

A PARAMETRIC DESCRIPTION OF ALGEBRAIC VARIETIES FOR ALGORITHMIC PURPOSES

JUAN SABIA

RÉSUMÉ. Dans l'exposé que nous avons fait au *XII Encuentro Rioplatense de Algebra y Geometría Algebraica*, nous avons présenté une vue d'ensemble de quelques aspects de la résolution efficace d'équations polynomiales. Dans cet article, nous nous concentrons sur une façon particulière de décrire les variétés algébriques dont nous avons parlé (la *résolution géométrique* d'une variété équidimensionnelle), laquelle était déjà connue de Kronecker (voir [19]) et a depuis prouvé son utilité pour la résolution algorithmique de systèmes d'équations polynomiales. Nous montrerons comment calculer cette représentation et nous en donnerons quelques applications.

ABSTRACT. In the talk we gave at the *XII Encuentro Rioplatense de Algebra y Geometría Algebraica*, we presented an overview of some aspects of efficient polynomial equation solving. In this paper, we focus our attention on a particular way of describing algebraic varieties we talked about (a *geometric resolution* of an equidimensional variety) that was already known to Kronecker (see [19]) and that has since proved to be very useful for solving systems of polynomial equations algorithmically. We will briefly show how this description can be attained and state some of its applications.

1. Introduction. A primary task we are faced with when dealing with a system of polynomial equations is to determine whether there are any solutions to the system or not. When the system is linear, algebraic tools can be used to this end (for instance the determinant or the rank of the matrices involved). Hilbert's *Nullstellensatz* can be seen also as a way of determining algebraically whether solutions of a system of multivariate polynomials exist or not.

Theorem 1. (*Hilbert's Nullstellensatz*) Let $f_1, \dots, f_s \in \mathbb{Q}[X_1, \dots, X_n]$. The following statements are equivalent:

- (1) $\{x \in \mathbb{C}^n \mid f_1(x) = \dots = f_s(x) = 0\} = \emptyset$;
- (2) There exist polynomials $g_1, \dots, g_s \in \mathbb{Q}[X_1, \dots, X_n]$ with $g_1 \cdot f_1 + \dots + g_s \cdot f_s = 1$.

Hilbert's *Nullstellensatz* translates in the language of linear algebra the problem of determining whether solutions to a polynomial system exist or not: if N is a bound for the degrees of the polynomials $g_1, \dots, g_s \in \mathbb{Q}[X_1, \dots, X_n]$, consider the coefficients of these polynomials as indeterminates and solve the linear system involved. If we try to apply Hilbert's *Nullstellensatz* directly, however, we may need to solve infinitely

many linear systems (one for each positive integer N), and this is impossible from an algorithmic point of view.

The first attempt to solve this problem was to give an upper bound for the degrees of some polynomials $g_1, \dots, g_s \in \mathbb{Q}[X_1, \dots, X_n]$ involved in the identity $g_1 \cdot f_1 + \dots + g_s \cdot f_s = 1$, taking into account the number n of variables, the number s of polynomials $f_1, \dots, f_s \in \mathbb{Q}[X_1, \dots, X_n]$ involved, and a bound on their degrees. That is why we call the following problem an *effective Hilbert's Nullstellensatz*:

Find an explicit function $\varphi : \mathbb{N}^3 \rightarrow \mathbb{N}$ satisfying the following property: let $f_1, \dots, f_s \in \mathbb{Q}[X_1, \dots, X_n]$ such that $\deg(f_i) \leq d$ for all $i \in \{1, \dots, s\}$. If $1 \in (f_1, \dots, f_s)$, there exist polynomials $g_1, \dots, g_s \in \mathbb{Q}[X_1, \dots, X_n]$ with $g_1 \cdot f_1 + \dots + g_s \cdot f_s = 1$ and $\deg(g_i) \leq \varphi(n, s, d)$ for each $i \in \{1, \dots, s\}$.

The first effective Hilbert's *Nullstellensatz* was given by Hermann [14] (whose proof was corrected in [21]), but the function she found was doubly exponential of order d^{2^n} . Evidently, this kind of bound is insufficient for algorithmic purposes. Brownawell [1] obtained the first single exponential bound, namely

$$\varphi(d, n, s) = 3 \min\{n, s\} n d^{\min\{n, s\}}.$$

The most precise bounds known to date for fields of any characteristic were given in [4] and [16] as

$$\varphi(d, n, s) = (\max\{3, d\})^n.$$

In [22], a better bound was obtained for the particular case $d = 2$, that is $\varphi(2, n, s) = n 2^{n+2}$. More precise bounds were also given in [24], [18] and [10] depending on the degrees of the polynomials appearing in the writing of 1 in the *Nullstellensatz*; they involve some geometric parameters apart from d , n and s .

A famous example by Masser and Philippon (see [1]) shows that the aforementioned bounds are optimal: these authors give a very simple example where the polynomials $g_1, \dots, g_s \in \mathbb{Q}[X_1, \dots, X_n]$ occurring in the writing of the 1 are all of degree at least $(d-1)d^{n-1}$.

If we give a fixed order to all the monomials in n variables and consider a polynomial (from the algorithmic point of view) as the vector of its coefficients, a polynomial of degree $D \geq 2$ will take $\binom{D+n}{D}$ coefficients. This number of coefficients is (asymptotically in D) of the same order as D^n . Therefore, in order to determine whether s rational polynomials in n variables and of degrees at most d have a common zero in $\mathbb{C}$, any general algorithm using an effective *Nullstellensatz* and the encoding of polynomials as the vectors of their coefficients will require at least $\mathcal{O}(sd^{n^2})$ steps.

At this point, there were at least two possibilities to try to design more effective algorithms: change the way of encoding polynomials, and decide whether there is a solution or not to a system of polynomial equations *without resorting to Hilbert's Nullstellensatz*.

In [8], Giusti and Heintz exploited both these possibilities to obtain a fundamental result related to the algorithmic solution of a system of polynomial equations. In that paper, a milestone in the development of algorithms solving polynomial equations, they designed an algorithm that can determine in *polynomial time*, in the size of the input, whether there exists a common complex zero or not for a given system of rational polynomial equations written as the vector of their coefficients.

Before going further, we have to explain the notion of time we use. An algorithm is a directed acyclic graph whose input nodes are the data we are given, and each internal node corresponds to a comparison or to an arithmetic operation that leads to the final result we are looking for. We will define the *time* or *complexity* of an algorithm as its number of nodes (that is, roughly speaking, the number of steps needed to obtain the output from the input).

In fact, the precise result Giusti and Heintz [8] obtained is the following.

Theorem 2. *Let $f_1, \dots, f_s \in \mathbb{Q}[X_1, \dots, X_n]$ be polynomials encoded as the vectors of their coefficients, with degrees bounded by d , and let $V \subset \mathbb{C}^n$ be the algebraic variety of their common zeros. Then there exists an algorithm which computes the dimension of V within complexity $s^{\mathcal{O}(1)} d^{\mathcal{O}(n)}$.*

Note that this result tells us more about the system than we have asked so far: if the dimension is -1 , the system has no solution but if the dimension is 0, for instance, the set of solutions consists only of finitely many isolated points.

Giusti and Heintz used a different way of encoding polynomials (*straight line programs*) to solve a problem in computer algebra for the first time. This encoding has to do with considering a polynomial as a function that can be evaluated rather than a formal expression (a vector of coefficients). As an illustration, this way of encoding would be very effective when dealing with the polynomial $P = (X + Y)^{1024}$ which, although it has 525,825 monomials considered as a polynomial in two variables of degree bounded by 1024, can be evaluated using only 11 operations. For precise definitions and elementary properties of straight line programs see, for instance, [2], [6] and [7].

Another key tool used by Giusti and Heintz in [8] was a particular way of defining zero-dimensional varieties that was already known by Kronecker; see [19]. This is a parametric way of presenting a variety which we will call a *geometric resolution* of the variety. This same description is being widely used nowadays in computer algebra; it is also known as *single variable representation*, *univariate representation* and *shape lemma*, among others.

In the following sections, we will define what is meant by a geometric resolution and we will show a possible algorithmic way to obtain it for a zero-dimensional variety defined by a family of polynomials.

2. Geometric resolution of zero-dimensional varieties.

2.1. Ideas and definitions. The idea of the presentation of a zero-dimensional variety by means of a geometric resolution is quite simple. Let $V \subset \mathbb{C}^n$ be a zero-dimensional variety consisting of D points:

$$V = \left\{ \xi^{(i)} := (\xi_1^{(i)}, \dots, \xi_n^{(i)}) \in \mathbb{C}^n \mid 1 \leq i \leq D \right\}.$$

Let $u_1, \dots, u_n \in \mathbb{Q}$ and assume that the linear form $\ell(X) := u_1 X_1 + \dots + u_n X_n$ is such that the numbers $\ell(\xi^{(i)})$ are all different from one another. In this case, we say that the linear form ℓ is a *primitive element* for V or that it *separates the points of V* . Consider the univariate polynomial $p \in \mathbb{C}$ defined by

$$p := \prod_{i=1}^D \left(T - \ell(\xi^{(i)}) \right).$$

Now, for each $j \in \{1, \dots, n\}$, use interpolation to find the unique polynomial $v_j \in \mathbb{C}[T]$ of degree bounded by $D - 1$ such that $v_j(\ell(\xi^{(i)})) = \xi_j^{(i)}$ for every $i \in \{1, \dots, D\}$. Then,

$$\begin{aligned} V &= \{x = (x_1, \dots, x_n) \in \mathbb{C}^n \mid p(\ell(x)) = 0, x_1 = v_1(\ell(x)), \dots, x_n = v_n(\ell(x))\} \\ &= \{(v_1(t), v_2(t), \dots, v_n(t)) \mid t \in \mathbb{C}, p(t) = 0\}. \end{aligned}$$

If we construct this description for a zero-dimensional variety included in $\mathbb{C}^n$ that is definable by rational polynomials, the polynomials $p, v_1, \dots, v_n$ will also be rational. Therefore, we can now define what is a geometric resolution for a zero-dimensional variety.

Definition 3. Let $V = \{\xi^{(1)}, \dots, \xi^{(D)}\} \subset \mathbb{C}^n$ be a zero-dimensional variety defined by polynomials in $\mathbb{Q}[X_1, \dots, X_n]$. A *geometric resolution* for V consists of a linear form $\ell(X) = u_1 X_1 + \dots + u_n X_n \in \mathbb{Q}[X_1, \dots, X_n]$ and of polynomials $p, v_1, \dots, v_n \in \mathbb{Q}[T]$ (where T is a new variable) such that:

- (1) $\ell(\xi^{(i_1)}) \neq \ell(\xi^{(i_2)})$ if $i_1 \neq i_2$;
- (2) $p(T) = \prod_{1 \leq i \leq D} (T - \ell(\xi^{(i)}))$;
- (3) For every $j \in \{1, \dots, n\}$, $\deg(v_j) \leq D - 1$ and $V = \{(v_1(t), \dots, v_n(t)) \mid t \in \mathbb{C}, p(t) = 0\}$.

Note that provided the linear form ℓ is given, this definition is unique. Thus we can call it the *geometric resolution of V* associated to the linear form ℓ .

2.2. A way to find geometric resolutions algorithmically. Although the previous construction is easy, it is theoretical; we should know the coordinates of the points of the variety V in advance in order to give its geometric resolution with respect to a linear form ℓ . Now suppose that we are given a zero-dimensional variety as the set of zeros of a family of polynomials. In this section, we will sketch a way of constructing the geometric resolution of V associated to ℓ following the ideas in [8] and [17].

Given a linear form, the first step will be to construct a univariate polynomial that vanishes over this linear form evaluated in the points of a zero-dimensional algebraic variety. To do so, we will use a result in [3].

Lemma 4. Let $f_1, \dots, f_s \in \mathbb{Q}[X_1, \dots, X_n]$ be polynomials of degrees bounded by d defining a zero-dimensional variety, and let $\ell \in \mathbb{Q}[X_1, \dots, X_n]$ be a linear form. Then there exists an algorithm which, within complexity $\mathcal{O}(sd^{n^2})$, computes the square-free polynomial $p \in \mathbb{Q}[T]$ such that its only roots are $\ell(\xi)$ for every $\xi \in V$.

Proof. Making a change of variables if necessary, we may suppose that the linear form is $\ell = X_1$. The polynomial $p(X_1)$ is an element of $\text{rad}(f_1, \dots, f_s)$ of degree bounded by d^n ; see Bézout's Theorem in [12]. Therefore, using Remark 1.6 in [3], we see that there exist polynomials $p_1, \dots, p_s \in \mathbb{Q}[X_1, \dots, X_n]$ such that

$$p^{d^n} = \sum_{i=1}^s p_i f_i, \quad \text{with } \deg(p_i f_i) \leq d^n(\deg p + 1) \leq d^n(d^n + 1).$$

Using this fact, we can find a non-zero polynomial $q \in \mathbb{Q}[T]$ such that its only roots are $\ell(\xi)$ for every $\xi \in V$. To do so, it is enough to find the minimum $d_0 \leq d^n(d^n + 1)$ such that a solution exists and can be identified for the linear system determined by the following conditions:

- (1) $q \in \mathbb{Q}[T]$ is a monic polynomial of degree d_0 ;
- (2) $q(X_1) = p_1 f_1 + \cdots + p_s f_s$, with $\deg(p_i f_i) \leq d^n(d^n + 1)$.

The polynomial p we are looking for is

$$p := \frac{q}{\text{GCD}(q, q')}.$$

The lemma now follows, because the computation of the GCD and the exact division of polynomials can be done in polynomial time in the degrees of the polynomials involved. $\square$

Note that although the version we have presented here is simpler than the one given by Giusti and Heintz [8], the complexity of our algorithm is still of order $\mathcal{O}(sd^{n^2})$. In the next subsection, we state the exact result shown in Section 3.4.5 of [8].

The next step towards the construction of a geometric resolution of a zero-dimensional variety will be to find a geometric resolution of a very particular zero-dimensional variety.

Lemma 5. *Let $f(X) \in \mathbb{Q}[X]$, $g(Y) \in \mathbb{Q}[Y]$ be non-zero square-free polynomials and let $V = \{(\xi, \eta) \in \mathbb{C}^2 \mid f(\xi) = 0, g(\eta) = 0\}$. Let $\delta := \deg(f) \cdot \deg(g)$. Then there exists an algorithm which, within complexity polynomial in δ , finds an element $\lambda \in \mathbb{Q}$ such that the linear form $\ell = Y + \lambda X$ is a primitive element of V and computes the geometric resolution of V associated to ℓ .*

Proof. Consider the polynomial $\hat{g} := g(T - \Lambda X) \in \mathbb{Q}[\Lambda][T, X]$, where Λ and T are new variables, and let $h := \text{Res}_X(f, \hat{g}) \in \mathbb{Q}[\Lambda][T]$. Observe that $\deg_T(h) = \deg(f) \cdot \deg(g)$ and for each $\lambda \in \mathbb{Q}$, let $\ell_\lambda := Y + \lambda X$.

Clearly, the roots of $h_\lambda(T) := h(\lambda, T) \in k[T]$ are exactly the elements $\ell_\lambda(\xi, \eta) = \eta + \lambda \xi$ with $(\xi, \eta) \in V$. Consequently, ℓ_λ is a primitive element for V if and only if h_λ is square-free. Thus it suffices to choose $\lambda \in \mathbb{Q}$ such that $\text{Res}_T(h, h')(\lambda) \neq 0$, where h' is the derivative of h with respect to T . As δ is the number of elements of V , there are at most $\delta(\delta - 1)/2$ values of λ such that ℓ_λ is not a primitive element for V . Hence it suffices to look for λ in the set $\{1, \dots, 1 + \delta(\delta - 1)/2\}$.

Once we have λ such that $\text{Res}_T(h, h')(\lambda) \neq 0$, the polynomial h_λ has to be the polynomial p of the geometric resolution of V associated to ℓ . To find the polynomials v_1 and v_2 , note that $\mathcal{B}_1 := \{\ell_\lambda^j \mid 0 \leq j < \deg(f) \cdot \deg(g)\}$ and $\mathcal{B}_2 := \{x^\alpha y^\beta \mid 0 \leq \alpha < \deg(f), 0 \leq \beta < \deg(g)\}$ are bases of the $\mathbb{Q}$ -linear space $\mathbb{Q}[X, Y]/(f, g)$. Therefore, we can use the change of bases to compute them. $\square$

Now, using the previous results recursively, we prove the following result.

Theorem 6. *Let $f_1, \dots, f_s \in \mathbb{Q}[X_1, \dots, X_n]$ be polynomials with degrees bounded by d which define a zero-dimensional variety V . Then there exists an algorithm of complexity polynomial in sd^{n^2} which computes a geometric resolution of V .*

Proof. The proof is done recursively, as in Section 3.4.6 in [8]. For every $i \in \{1, \dots, n\}$, a linear form $Y_i := u_1 X_1 + \cdots + u_i X_i$ and polynomials $v_1^{(i)}, \dots, v_i^{(i)} \in \mathbb{Q}[T]$ are computed so that, for each point $\xi := (\xi_1, \dots, \xi_n) \in V$, we have $\xi_j = v_j^{(i)}(Y_i(\xi))$ for $j \in \{1, \dots, i\}$.

For $i = 1$, take $Y_1 := X_1$ and $v_1^{(1)} := T$. Next, let $i \geq 2$ and assume that the variable Y_{i-1} and the polynomials $v_1^{(i-1)}, \dots, v_{i-1}^{(i-1)}$ fulfilling the required conditions are given.

We then compute two polynomials $f(X_i) \in \mathbb{Q}[X_i]$ and $g(Y_{i-1}) \in \mathbb{Q}[Y_{i-1}]$ that vanish over V ; see Lemma 4. Let

$$Z := \{(\xi, \eta) \in \mathbb{C}^2 \mid f(\xi) = 0, g(\eta) = 0\}.$$

Applying Lemma 5 to Z , we obtain an element $u_i \in \mathbb{Q}$ and polynomials $p, v_1, v_2 \in \mathbb{Q}[T]$ that yield the geometric resolution of Z associated to $Y_i := Y_{i-1} + u_i X_i$.

For the linear form Y_i , we can compute the polynomial $p_i \in \mathbb{Q}[T]$ of Lemma 4 whose zeros are exactly the values of Y_i evaluated in the points of V . The polynomial $v_i^{(i)}$ can be computed as the remainder of the division of v_1 by p_i . The polynomials $v_1^{(i)}, \dots, v_{i-1}^{(i)}$ are obtained by replacing the variable T by v_2 in the polynomials $v_1^{(i-1)}, \dots, v_{i-1}^{(i-1)} \in \mathbb{Q}[T]$ and reducing the result modulo p_i .

After the n th step, we get a linear form $Y_n := u_1 X_1 + \dots + u_n X_n$, the polynomial $p_n \in \mathbb{Q}[T]$ whose zeros are the values of Y_n at the points of V , and polynomials $v_1^{(n)}, \dots, v_n^{(n)}$ such that for every $\xi := (\xi_1, \dots, \xi_n) \in V$, the identity $\xi_j = v_j^{(n)}(Y_n(\xi))$ holds for every $j \in \{1, \dots, n\}$.

Taking into account the choice of the linear form in Lemma 5, and that the polynomials $f(X_i)$ and $g(Y_{i-1})$ in each step have degrees bounded by d^n , we deduce that the coefficients u_i can be chosen from the set $\{1, \dots, d^{4n}\}$.

Using Lemma 5 to estimate the complexity of each step of the recursion, we have that the total complexity of this algorithm is polynomial in sd^{n^2} . $\square$

2.3. A polynomial algorithm to compute the dimension of a variety. The exact version of Lemma 4 stated in Section 3.4.5 of [8] is as follows.

Lemma 7. *Let $f_1, \dots, f_s \in \mathbb{Q}[X_1, \dots, X_n]$ be polynomials of degrees bounded by d and let $V \subset \mathbb{C}^n$ be the variety they define. There exists an algorithm which, within complexity polynomial in sd^n , for a given linear form $\ell \in \mathbb{Q}[X_1, \dots, X_n]$, computes a polynomial $p \in \mathbb{Q}[T]$ of degree bounded by d^n such that $p(\ell(\xi)) = 0$ for all the isolated points of V .*

The proof of this lemma uses a homotopic deformation of the system of polynomials $f_1, \dots, f_s$ so that some regularity conditions are met. The polynomial p is computed by relating it to the characteristic polynomial of a suitable linear form associated to ℓ . By using this result, Giusti and Heintz [8] do not find a geometric resolution for the set of isolated points V_0 of a variety V , but they find it for a zero-dimensional variety Z_0 satisfying $V_0 \subseteq Z_0 \subseteq V$. Of course, if V is zero-dimensional, the geometric resolution obtained is exactly the one for V .

The manner in which Giusti and Heintz [8] compute the dimension of a variety V defined by polynomials $f_1, \dots, f_s$ is as follows. Consider generic affine linear forms $L_1, \dots, L_n \in \mathbb{Q}[X_1, \dots, X_n]$. Then a dimension argument states that $W_n := V \cap \{\xi \in \mathbb{C}^n \mid L_1(\xi) = 0, \dots, L_n(\xi) = 0\}$ is either empty or a zero-dimensional variety. By means of the previous lemma, fixing a linear form ℓ , we can compute the geometric resolution of this variety. If the polynomial p is not constant, this variety is not empty and therefore $\dim V = n$. If it is constant, W_n is empty and we can go on with the variety $W_{n-1} := V \cap \{\xi \in \mathbb{C}^n \mid L_1(\xi) = 0, \dots, L_{n-1}(\xi) = 0\}$ which will in turn be empty or zero-dimensional and will allow us to decide whether V has dimension $n-1$ or not. After at most n steps, either we have computed the dimension of V or we can say that $\dim V \leq 0$.

We therefore compute the geometric resolution associated to V and determine whether V is empty or not within complexity which is polynomial in sd^n .

3. Geometric resolution of equidimensional varieties. The definition of a geometric resolution given for a zero-dimensional variety can be adapted to the case of equidimensional varieties of any dimension.

Let $V \subset \mathbb{C}^n$ be an equidimensional variety of dimension r defined by the polynomials $f_1, \dots, f_s \in \mathbb{Q}[X_1, \dots, X_n]$. Suppose the variables $\{X_1, \dots, X_r\}$ are in *Noether position* with respect to the variety V ; that is $\mathbb{Q}[X_1, \dots, X_r] \cap (f_1, \dots, f_s) = \{0\}$ and, for each remaining variable X_i , there exists a polynomial in $\mathbb{Q}[X_1, \dots, X_r, X_i]$ monic in X_i vanishing over V . If we consider the field $\mathbb{Q}(X_1, \dots, X_r)$, then the variety $\tilde{V}$ defined by the polynomials $f_1, \dots, f_s$ over an algebraic closure of $\mathbb{Q}(X_1, \dots, X_r)$ turns out to be zero-dimensional. Given a linear form $\ell \in \mathbb{Q}[X_{r+1}, \dots, X_n]$ separating the points in $\tilde{V}$, we can then consider the geometric resolution $(p, \tilde{v}_{r+1}, \dots, \tilde{v}_n) \in \mathbb{Q}(X_1, \dots, X_r)[T]^{n-r+1}$ of $\tilde{V}$ associated to ℓ .

The Noether position hypothesis guarantees that $p \in \mathbb{Q}[X_1, \dots, X_r][T]$ and that it is a monic polynomial. Let $\rho \in \mathbb{Q}[X_1, \dots, X_r]$ be the GCD among the denominators of the coefficients of $\tilde{v}_{r+1}, \dots, \tilde{v}_n$ and let $v_{r+1} := \rho \tilde{v}_{r+1}, \dots, v_n := \rho \tilde{v}_n$. It can then be proved that

$$\begin{aligned} V \cap \{\rho \neq 0\} &= \{\xi \in \mathbb{C}^n \mid p(\ell(\xi)) = 0, \\ &\quad \rho(\xi_1, \dots, \xi_r) \cdot \xi_{r+1} - v_{r+1}(\xi_1, \dots, \xi_r, \ell(\xi)) = 0, \\ &\quad \dots, \\ &\quad \rho(\xi_1, \dots, \xi_r) \cdot \xi_n - v_n(\xi_1, \dots, \xi_r, \ell(\xi)) = 0\}. \end{aligned}$$

Under these conditions, we say that $p, \rho, v_{r+1}, \dots, v_n$ form a *geometric resolution* of V associated to ℓ .

4. A final remark. The description of equidimensional varieties by means of geometric resolutions, together with the straight-line program encoding, proved to be very useful when trying to obtain algorithms more effective than the ones using codification of polynomials by vectors of coefficients. The cornerstone of this family of algorithms is the aforementioned algorithm of Giusti and Heintz [8] which computes the dimension of an algebraic variety in polynomial time. These tools were later refined in [9], [10] and [17]. They were also used, for instance, to obtain the writing of the 1 in the *Nullstellensatz* (see [5] and [11]), to obtain the equidimensional decomposition of an algebraic variety in polynomial time (see [15] and [20]), and to solve parametric systems of polynomial equations (see [13] and [23]). These tools are still being used and will probably lead to new and more useful results in computer algebra in the future.

Acknowledgements. Funding in partial support of this work was provided by Argentinian research grants UBACyT (P. X112) and CONICET (PIP 2461). The author would like to thank Andrea Solotar and Marco Farinati for inviting him to take part in the *XII Encuentro Rioplatense de Algebra y Geometría Algebraica*. He is also indebted to Gabriela Jeronimo for her help in the transcription of these notes.

Résumé substantiel en français. Étant donnés $f_1, \dots, f_s \in \mathbb{Q}[X_1, \dots, X_n]$ des polynômes de degrés majorés par d , on considère d'abord la question de déterminer si le système $f_1(x) = \dots = f_s(x) = 0$ admet des solutions dans $\mathbb{C}^n$. Le théorème des zéros (*Nullstellensatz*) de Hilbert fournit une condition qui permet de traduire cette question en un problème d'algèbre linéaire.

La taille de la représentation classique d'un polynôme de degré $D \geq 2$ à n variables par le vecteur de ses coefficients (*représentation dense*) est d'ordre D^n . Par conséquent, l'usage de cette représentation et le théorème des zéros ne peuvent que conduire à des algorithmes de complexité polynomiale en sd^{n^2} à cause de la taille des sorties; voir [1], [4] et [16]. Pour obtenir de meilleures complexités, il faut alors changer la structure de données choisie ou la méthode employée.

Dans [8], Giusti et Heintz présentent un algorithme qui résout le problème en temps polynomial en la taille des entrées. Cette complexité est obtenue par une nouvelle méthode qui n'est pas basée sur le *Nullstellensatz* et un changement du codage des sorties et des résultats intermédiaires: un polynôme est vu comme une fonction et représenté par un *calcul d'évaluation* (ou *straight-line program*), c'est-à-dire par un programme permettant de calculer sa valeur en un point quelconque. L'algorithme calcule la dimension de la variété définie par le système donné, en se servant d'une description particulière des variétés de dimension zéro qui était déjà connue de Kronecker [19]: la résolution géométrique.

Une *résolution géométrique* d'une variété de dimension zéro $V \subset \mathbb{C}^n$ définie par un ensemble de polynômes à coefficients dans $\mathbb{Q}$ est composée d'une forme linéaire ℓ séparant les points de V ($\ell(\xi) \neq \ell(\xi')$ pour $\xi \neq \xi'$), son polynôme minimal $p = \prod_{\xi \in V} (T - \ell(\xi)) \in \mathbb{Q}[T]$, et des polynômes $v_1, \dots, v_n \in \mathbb{Q}[T]$ correspondant aux coordonnées des points de V . Il s'agit d'une paramétrisation de la variété sous la forme $V = \{(v_1(t), \dots, v_n(t)) \mid t \in \mathbb{C}, p(t) = 0\}$.

Dans cet article, nous décrivons un algorithme qui calcule une résolution géométrique d'une variété V de dimension zéro à partir de polynômes $f_1, \dots, f_s \in \mathbb{Q}[X_1, \dots, X_n]$ définissant V . Même si les bornes de complexité de cet algorithme ne sont pas les meilleures, nous le présentons ici pour illustrer les techniques qui sont exploitées dans ce cadre.

L'algorithme repose sur un lemme qui permet d'obtenir un polynôme en n'importe quelle forme linéaire qui s'annule sur chaque point de la variété. On trouve dans [8] un algorithme qui accomplit une tâche semblable en temps polynomial en la taille des entrées.

Lemme 4. Soient $f_1, \dots, f_s \in \mathbb{Q}[X_1, \dots, X_n]$ des polynômes de degrés au plus d qui définissent une variété algébrique V de dimension zéro et soit $\ell \in \mathbb{Q}[X_1, \dots, X_n]$ une forme linéaire. Il existe un algorithme qui calcule en temps $\mathcal{O}(sd^{n^2})$ un polynôme réduit (c'est-à-dire, sans racines multiples) $p \in \mathbb{Q}[T]$ dont l'ensemble des zéros est $\{\ell(\xi) \mid \xi \in V\}$.

Pour trouver une forme linéaire séparant et des polynômes qui donnent la paramétrisation de la variété, l'algorithme se base sur l'algorithme sous-jacent au lemme suivant.

Lemme 5. Soient $f(X) \in \mathbb{Q}[X]$, $g(Y) \in \mathbb{Q}[Y]$ des polynômes réduits non nuls et soit $V = \{(\xi, \eta) \in \mathbb{C}^2 \mid f(\xi) = 0, g(\eta) = 0\}$. Soit $\delta := \deg(f) \cdot \deg(g)$. On peut alors

trouver une valeur $\lambda \in \mathbb{Q}$ telle que $\ell = Y + \lambda X$ est une forme linéaire séparante pour V et calculer la résolution géométrique de V associée à ℓ en temps polynomial en δ .

Enfin, en utilisant les résultats précédents de manière itérative, on peut montrer le résultat suivant.

Théorème 6. Soient $f_1, \dots, f_s \in \mathbb{Q}[X_1, \dots, X_n]$ des polynômes de degrés majorés par d qui définissent une variété V de dimension zéro. On peut alors calculer une résolution géométrique de V par un algorithme de complexité polynomiale en sd^{n^2} .

L'algorithme de Giusti et Heintz [8] s'appuie sur un système d'équations définissant une variété V arbitraire et calcule une résolution géométrique d'un ensemble fini de points de V contenant les points isolés de la variété avec une complexité polynomiale en sd^n (la taille des entrées). À l'aide de cet algorithme, on peut calculer la dimension de la variété donnée en coupant successivement avec des hyperplans génériques (qui diminuent la dimension de un) jusqu'à ce que la variété soit vide en temps polynomial en sd^n . Nous renvoyons à [8] pour plus de précisions.

La notion de résolution géométrique d'une variété de dimension zéro s'étend au cas des variétés équidimensionnelles de dimension positive.

Depuis l'algorithme fondamental de Giusti et Heintz [8], de nombreuses méthodes efficaces pour la résolution d'équations polynomiales ont été proposées en utilisant la représentation des variétés par des résolutions géométriques et le codage de polynômes par des calculs d'évaluation; voir par exemple [5], [9], [13], [15], [20] et [23].

REFERENCES

1. W. D. Brownawell, *Bounds for the degrees in the Nullstellensatz*, Ann. of Math. (2) **126** (1987), 577–591.
2. P. Bürgisser, M. Clausen and M.A. Shokrollahi, *Algebraic Complexity Theory*, Grundlehren der Mathematischen Wissenschaften **315**, Springer, Berlin, 1997.
3. A. Dickenstein, N. Fitchas, M. Giusti and C. Sessa, *The membership problem for unmixed polynomial ideals is solvable in single exponential time*, Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes (Toulouse, 1989). Discrete Appl. Math. **33** (1991), 73–94.
4. N. Fitchas and A. Galligo, *Nullstellensatz effectif et conjecture de Serre (Théorème de Quillen–Suslin) pour le calcul formel*, Math. Nachr. **149** (1990), 231–253.
5. N. Fitchas, M. Giusti and F. Smietanski, *Sur la complexité du théorème des zéros*, Approx. Optim. **8**, Approximation and Optimization in the Caribbean, II (Havana, 1993), 274–329, Lang, Frankfurt am Main, Germany, 1995.
6. J. von zur Gathen, *Parallel arithmetic computations: a survey*, Mathematical foundations of computer science, 1986 (Bratislava, 1986), 93–112, Lecture Notes in Comput. Sci. **233** Springer, Berlin, 1986.
7. J. von zur Gathen, *Parallel linear algebra*, Synthesis of Parallel Algorithm, San Mateo, CA (1993), 573–617.
8. M. Giusti and J. Heintz, *La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial*, Computational Algebraic Geometry and Commutative Algebra (Cortona, 1991), 216–256, Sympos. Math., XXXIV, Cambridge University Press, Cambridge, 1993.
9. M. Giusti, J. Heintz, K. Hägele, J. E. Morais, L. M. Pardo and J. L. Montaña, *Lower bounds for Diophantine approximation*, J. Pure Appl. Algebra **117/118** (1997), 277–317.
10. M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern and L. M. Pardo, *Straight-line programs in geometric elimination theory*, J. Pure Appl. Algebra **124** (1998), 101–146.

11. M. Giusti, J. Heintz and J. Sabia, *On the efficiency of effective Nullstellensätze*, Comput. Complexity **3** (1993), 56–95.
12. J. Heintz, *Definability and fast quantifier elimination over algebraically closed fields*, Theoret. Comput. Sci. **24** (1983), 239–277. [Corrigendum: J. Heintz, Theoret. Comput. Sci. **39** (1985), 343.]
13. J. Heintz, T. Krick, S. Puddu, J. Sabia and A. Waissbein, *Deformation techniques for efficient polynomial equation solving*, J. Complexity **16** (2000), 70–109.
14. G. Hermann, *Zur Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95** (1926), 736–788.
15. G. Jeronimo and J. Sabia, *Effective equidimensional decomposition of affine varieties*, J. Pure Appl. Algebra **169** (2002), 229–248.
16. J. Kollár, *Sharp effective Nullstellensatz*, J. Amer. Math. Soc. **1** (1988), 963–975.
17. T. Krick and L. M. Pardo, *A computational method for diophantine approximation*, Progress Math. **143** (1996), 193–253.
18. T. Krick, J. Sabia and P. Solernó, *On intrinsic bounds in the Nullstellensatz*, Appl. Algebra Engrg. Comm. Comput. **8** (1997), 125–134.
19. L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, J. Reine Angew. Math. **92** (1882), 1–122.
20. G. Lecerf, *Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions*, Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation (St. Andrews), 209–216 (electronic), ACM, New York, 2000.
21. D. W. Masser and G. Wüstholz, *Fields of large transcendence degree generated by values of elliptic functions*, Invent. Math. **72** (1983), 407–464.
22. J. Sabia and P. Solernó, *Bounds for traces in complete intersections and degrees in the Nullstellensatz*, Appl. Algebra Engrg. Comm. Comput. **6** (1995), 353–376.
23. E. Schost, *Computing parametric geometric resolutions*, Appl. Algebra Engrg. Comm. Comput. **13** (2003), 349–393.
24. M. Sombra, *Bounds for the Hilbert function of polynomial ideals and for the degrees in the Nullstellensatz*, Algorithms for Algebra (Eindhoven, 1996). J. Pure Appl. Algebra **117/118** (1997), 565–599.

J. SABIA
 DEPARTAMENTO DE MATEMÁTICA,
 FACULTAD DE CIENCIAS EXACTAS Y NATURALES,
 UNIVERSIDAD DE BUENOS AIRES,
 BUENOS AIRES, ARGENTINA
 jsabia@dm.uba.ar