Straight-line Programs
in Polynomial Equation Solving

Teresa Krick[1]

Département de Mathématique, Université de Limoges, France
Departamento de Matemática, Universidad de Buenos Aires, Argentina.
`teresa.krick@unilim.fr, krick@dm.uba.ar`

Abstract. Solving symbolically polynomial equation systems when intermediate and final polynomials are represented in the usual dense encoding turns out to be very inefficient: the sizes of the systems one can deal with do not respond to realistic needs. Evaluation representations appeared in this frame a decade ago as a new possibility to treat new families of problems.

We present a survey of the most recent complexity results for different polynomial problems when polynomials are encoded by evaluation (straight-line) programs. We also show surprising mathematical by-products, such as new mathematical invariants and results, that appeared as a consequence of the search of good algorithms.

Keywords. Computer algebra, polynomial equation systems, algebraic varieties, straight-line programs, Nullstellensatz, geometric resolutions, Chow forms, equidimensional decomposition, symbolic Newton method.

MSC 2000. *Primary:* 14Q15, *Secondary:* 68W30.

Contents

Introduction

There are several geometric questions that naturally arise when we are faced to a system of polynomial multivariate equations: do the given equations have at least a common root in an algebraic closure of the base field? If this is so, is there a finite or infinite number of them? What is the dimension of the solution variety? How to describe it in a more tractable manner?

Two major lines have been proposed to answer this kind of questions: numerical analysis which responds with approximate solutions, and computational algebra with its symbolic procedures giving exact solutions. In this paper we deal with this second aspect, although the evaluation methods we describe tend a natural bridge to the numerical point of view.

Nowadays most usually applied symbolic algorithms rely on rewriting techniques where the input is given by the number of variables, degree bounds and the list of polynomials with (implicitly) all their possible coefficients: this is the case for Gröbner bases computations and for characteristic set descriptions (and also with some minor changes for the more recently considered sparse systems). Unfortunately for the usual case when the degree d of the polynomials is greater than the number n of variables, the size of the input system is typically large, essentially of order d^n, and the degree of the polynomials describing the output can reach d^n as well, which means that writing the output requires at least $(d^n)^n$ symbols, a quantity that is exponential in the size of the input. Moreover, it is a well-known fact that the worst-case complexity of Gröbner bases computations is doubly exponential in n. This behavior prevents us from considering large polynomial equation systems with rewriting techniques.

Evaluation representations began to be strongly considered as an alternative a decade ago. A first and quite naïve motivation of this point of view is that there are polynomials that nobody writes (in dense representation) but everybody computes for specific values, like for example the determinant of a matrix of indeterminates. As another motivation, for the first question raised above —the effective Nullstellensatz— there is a classic example (which gives the well-known lower bound for the degrees of the polynomials arising in a Bézout identity, see Section 2 below) that suggested that there are always for this question Bézout identities composed by polynomials that behave better than expected with respect to evaluation, in the sense that they can be evaluated faster than they should. A careful development of new techniques, that I partially describe here, proved that this intuition was right.

The consideration through evaluation methods (straight-line programs) of the stated geometric questions allows to classify their complexity with respect not only to the usual parameters given by the number n of variables and the number s and degree d of the input polynomials, but also to less usual parameters like the length L of the straight-line program representation of the input and the size δ of the underlying linear algebra structure (this parameter, more precisely defined in Sections 1.3 and 1.5 below, is nowadays called the *geometric degree of the input polynomial system*). It is shown that all considered geometric questions behave polynomially with respect to these parameters, more precisely there are probabilistic algorithms and straight-line program representations for the output polynomials whose complexity and lengths are polynomial in s, n, d, δ and L.

Here is an example of such a statement, for the case of a zero-dimensional variety, which represents a core result in this philosophy (see Section 3.1 below):

Theorem *Let $f_1, \ldots, f_n \in \mathbb{Q}[x_1, \ldots, x_n]$ be polynomials of degree bounded by d and encoded by straight-line programs of length L, which define a zero-dimensional variety $Z \subset \mathbb{C}^n$. Set δ for the geometric degree of the input polynomial system.*
Then there is a bounded probability algorithm which computes (slp's for) a simple and tractable presentation of Z (a geometric resolution*) within complexity $(nd\delta L)^{\mathcal{O}(1)}$.*

As the parameters L and δ are in the worst case (and also in a random case) equal to sd^n (for $d \geq n$) and d^n respectively, but may be in some specific cases polynomial in n, s and d, the result

can be read as giving an exponential bound in the worst case but a polynomial bound for certain subfamilies of input polynomials.

Also, another consequence of this result is that when the input is codified in the dense representation and its size is measured by sd^n (for $d \geq n$), the length of the straight-line program representation of the output is polynomial in this quantity instead of being exponential as it happens with its dense representation. Since from a straight-line program one clearly (but not rapidly) recovers a dense representation through interpolation, the result implies that the exponential behavior of the complexity of these questions (when considering them classically) is all contained in the final interpolation: there is no exponentiality needed before.

Another research line suggested by this classification is related to the Bézout number: it is usual to associate to a family of s polynomials of degrees $d_1, \ldots, d_s$ in n variables such that $d_1 \geq \cdots \geq d_s$, the Bézout number $D := d_1 \cdots d_{\min\{n,s\}}$. The main property of this Bézout number is that it bounds the geometric degree of the variety defined by the input polynomials. However a precise definition of such a Bézout number D should depend intimately on the representation of the input polynomials: for polynomials of degree d encoded in dense representation, $D := d^n$ seems to be a natural choice, while for sparse polynomials with support in $\mathcal{A}$, $D := \mathrm{Vol}(\mathcal{A})$ seems to be the right notion of Bézout number, as this quantity also controls the degree of the variety. This digression is motivated by the following crucial observation: in the computation of the resultant, the length of the input L together with the associated Bézout number D and the number of variables n controls the complexity. In the case of dense representation of the input and $d \geq 2$, the typical length L equals $\mathcal{O}(nd^n)$ and $D = d^n$ while for the sparse representation, we have $L \geq 1$ and $D = \mathrm{Vol}(\mathcal{A})$. In both cases, the complexity of computing the resultant is $(nD)^{\mathcal{O}(1)}L$. The optimal complexity estimate should in fact be linear in D as well, although it is not clear what is the exact dependence on n: in the linear case, that is for $n+1$ dense linear forms, $L = \mathcal{O}(n^2)$ and $D = 1$ hold and the resultant equals the determinant, which is conjectured —but still not proved— to be computable in $\mathcal{O}(n^2)$. In an even more general framework, the conjecture is that the computation of (a slp representation of) any geometric object associated to a family of polynomials in n variables represented in a given encoding, with associated Bézout number D and associated length of the input L, should be linear in both D and L, and (possibly) quadratic in n. Here the associated Bézout number D could be the geometric degree of the input polynomial system.

A final comment on the contents of this paper: I only treat here results concerning *upper bounds* for the sequential complexity of *geometric* questions. I do not consider algebraic questions like for instance the ideal membership problem since their complexity is usually accepted to behave essentially worse. Also, all bounds depend on the size of the underlying linear algebra structure which is in the worst case of order d^n independently from the fact $d \geq n$ or not. In case $d = 2$ and n arbitrary, the size of the input is of order n^2 instead of 2^n while our algorithms are in the generic case polynomial in 2^n. A completely different analysis and novel approach are needed to deal with this case. Finally, concerning *lower bounds* —a task of a different order of complexity as everybody knows— there is a deep research actually going on: we refer to [12] and the references given there for an outview of the most recent and striking results on the matter.

This paper is deliberately written in a non-technical style: for each subject I tried to priorize ideas and natural developments over precise definitions, proofs or full generality of results: references where these can be found are always given. The paper is divided in 6 chapters. Chapter 1 gives a very quick and intuitive introduction on data structures and algorithms, priorizing properties of the straight-line program encodings with respect to other encodings, and also with some preliminaries needed for the sequel. Chapter 2 presents the effective Nullstellensatz as a motivation of the spirit of the paper. It contains a presentation of classic upper and lower (degree and arithmetic) bounds and a discussion on the utility of evaluation methods with a succint idea of an algorithm. In particular it shows how a good evaluation method combined with a deep and non-trivial arithmetic analysis yield optimal bounds for the arithmetic Nullstellensatz. Chapter 3 concentrates on zero-dimensional varieties, presenting geometric resolutions (shape lemmas descriptions) and Chow forms and comparing both characterizations of these varieties. Chapter 4 gives the generalizations of

these notions to equidimensional varieties of arbitrary dimension, and introduces Newton's method to lift the information on a good zero-dimensional fibre to the corresponding positive-dimensional component. Chapter 5 shows an outline of a general algorithm which describes each equidimensional component of a variety from a set description. This algorithm is mainly the result of many other algorithms performing related tasks that were developed and improved during the last 5 years and are somewhat discussed during the whole paper. Finally Chapter 6 gives a couple of applications that are interesting on their own, even in a more classical frame.

Many of the ideas and algorithms surveyed in this paper are implemented in a MAGMA package, called *Kronecker*, developed by Grégoire Lecerf [49].

Acknowledgments. I wish to thank FoCM organizers for their invitation to give this talk at FoCM'02 great conference, held at the IMA, Minneapolis, during August 2002, and for making my presence possible there. Also, I would like to say that the results presented here would not have been obtained without any of the members of TERA group (http://tera.medicis.polytechnique.fr/) and especially without Joos Heintz. Finally, I am grateful to Juan Sabia and Martín Sombra for their help and comments, and to David Cox for his careful reading.

1 Preliminaries

1.1 Data structures

The objects we deal with are polynomials in n variables with coefficients in a field k of characteristic zero. That is

$$f = \sum_{\alpha} a_{\alpha} x^{\alpha} \quad \text{with} \quad a_{\alpha} \in k,$$

where $\alpha := (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$ and $x^{\alpha} := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.

We insist on the fact that the characteristic of the base field k is zero, for some of the techniques and results we present do not apply for positive characteristic. The notation $\mathbb{A}^n$ always refers to $\mathbb{A}^n(\overline{k})$, where $\overline{k}$ is an algebraic closure of k, unless otherwise specified.

The usual *dense encoding* for representing such a polynomial f is given by an a priori bound d for the degree of f and an array of the $\binom{d+n}{d} = \binom{d+n}{n}$ coefficients a_{α} (zero coefficients as well as non-zero ones) in a pre-established order.

In opposition the *sparse encoding* only represents the non-zero coefficients by means of couples $(\alpha; a_{\alpha})$ indicating the exponent α corresponding to a non-zero coefficient a_{α}. (Another classic way of defining sparsity is fixing the Newton polytope allowed, that is the convex hull of the exponents corresponding to non-zero coefficients, we only consider it here in the applications.)

In this paper we deal with a third way of representing a polynomial f, which is called the *straight-line program encoding* (*slp* for short). The idea of using slp as short encodings of special families of polynomials goes back to the seventies, when it appeared in questions concerning the probabilistic testing of polynomial identities. The first applications to computer algebra dealt with the elimination of one variable problems ([35, 41, 42]. Later there were extended to multivariate elimination problems by Marc Giusti, Joos Heintz and their collaborators, in works that are partly reviewed here.

There are many different slp approaches. We refer to [8] for the standard definition or to [35, 45] for other models. We only describe here the simplest one, in a non-rigurous manner that we hope is enough for the readability of this paper:

Definition 1.1 *Given a polynomial $f \in k[x_1, \ldots, x_n]$, a slp encoding of f is an evaluation circuit γ for f, where the only operations allowed belong to $\{+, -, \cdot\}$ (no divisions) and the constants $a \in k$ can be used freely.*

More precisely: $\gamma = (\gamma_{1-n}, \ldots, \gamma_0, \gamma_1, \ldots, \gamma_L)$ *where* $f = \gamma_L$, $\gamma_{1-n} := x_1, \ldots, \gamma_0 := x_n$ *and for* $k > 0$, γ_k *is of one of the following forms:*

$$\gamma_k = a * \gamma_j \quad or \quad \gamma_k = \gamma_i * \gamma_j \quad where\ a \in k,\ * \in \{+, -, \cdot\}\ and\ i, j < k.$$

For example, the dense encoding of the polynomial $f = x^{2^d}$ (in 1 variable) is $(1, 0, \ldots, 0)$ for the decreasing order of monomials, its sparse encoding equals $(2^d; 1)$ and a straight-line program encoding is for instance given by the following slp γ:

$$\gamma_0 = x\ ,\ \gamma_1 = \gamma_0 \cdot \gamma_0 = x^2\ ,\ \gamma_2 = \gamma_1 \cdot \gamma_1 = x^{2^2}\ , \ldots ,\ \gamma_d = \gamma_{d-1} \cdot \gamma_{d-1} = x^{2^d}.$$

We specify now the *lengths* associated to these encodings: here we assume that each constant of the field k has length 1. (In many concrete situations the input polynomials have integer or rational coefficients and thus a more realistic measure of the input is given by taking also into account a bound for the maximum bit length of every integer allowed to appear.) Thus the dense encoding of a polynomial f of degree bounded by d like above has length $\binom{d+n}{d} = \mathcal{O}(d^n)$ (at least if $d \geq n$ as it is usually the case), while the sparse encoding has length $(n+1)N$ where N is a bound for the number of non-zero coefficients of f. Finally the length of a slp γ like above is defined as $L(\gamma) = L$ (note that $\gamma_{1-n}, \ldots, \gamma_0$ are added to the list only to handle with the variables and therefore have no cost), and the length $L(f)$ of f is the minimum of the lengths of γ for γ a slp encoding f.

Coming back to the example, the length of the dense encoding of x^{2^d} is $2^d + 1$, the length of its sparse encoding is 2 while the length of its slp encoding is bounded by d since we exhibited a slp γ for f such that $L(\gamma) = d$. However, note that for $(x+y)^{2^d}$ (in 2 variables) one can produce immediately a slp γ' of length $d+1$ defining $\gamma'_1 := x + y$ and then squaring like in γ, while both the dense and the sparse encodings have length $\binom{2^d}{2} = \mathcal{O}(2^{2d})$. This observation is an example of the following crucial fact:

Remark 1.2 *Straight-line programs behave well under linear changes of variables (while sparsity does not).*

Now let us compare dense encoding and slp encoding lengths. Every polynomial has a standard slp encoding given essentially by its dense encoding:

Remark 1.3 *Let* $f \in k[x_1, \ldots, x_n]$ *be a polynomial of degree d, then*

$$L(f) \leq 3\binom{d+n}{d}.$$

Proof.– One shows inductively that for any $r \in \mathbb{N}$, there is a slp of length bounded by $\binom{n+r}{r}$ whose intermediate results are all monomials x^α with $|\alpha| \leq r$ (once one has a list of all the monomials of degree bounded by $r - 1$, each one of the $\binom{n+r-1}{r}$ homogeneous monomials of degree r is simply obtained from one of the list multiplying by a single variable). Finally we multiply all monomials of f by their coefficients and add them up, that is we add $2\binom{d+n}{d}$ instructions to obtain a slp encoding for f. □

Also, it is clear that a sparse polynomial has a "short" slp (if one knows in advance a bound for the degree): Let $f \in k[x_1, \ldots, x_n]$, $\deg f \leq d$, be a polynomial with at most N non-zero coefficients, then $L(f) \leq Nd + N - 1$.

Reciprocally, if a polynomial $f \in k[x_1, \ldots, x_n]$ is represented by a slp of length L and *a bound for its degree d is known*, its dense encoding is trivially obtained within $d^{\mathcal{O}(n)}L(f)$ operations, simply interpolating in a grid of $(d+1)^n$ points. Of course this is not very satisfactory since we loose the possible benefit we had of having a short slp for f. However, it is important to notice that polynomials with short slp's are very rare. This is an important classification fact:

Fix a bound d for the degree of the polynomials. In the same way that sparse polynomials (we mean polynomials with at least one prescribed zero coefficient) belong to the union of closed hyperplanes

of the set of all polynomials, polynomials with slp's essentially shorter that the length given by the standard dense encoding belong to a closed hypersurface of the set of all polynomials (see [35] or [34, Th. 3.2]):

Proposition 1.4 *For every $c \in \mathbb{N}$, and for every $n, d \in \mathbb{N}$ big enough, there exists a hypersurface $\mathcal{H} \subset \mathbb{A}^{\binom{n+d}{d}}$ such that*

$$\{f \in k[x_1, \ldots, x_n], \deg f \leq d \text{ and } L(f) \leq (nd)^c\} \Rightarrow f = \sum a_\alpha x^\alpha \text{ with } (a_\alpha)_\alpha \in \mathcal{H}.$$

Roughly speaking this fact says that a random polynomial of degree d takes essentially as much time to be evaluated than its whole number of (zero and non-zero) monomials. Polynomials like in the statement of Proposition 1.4 are very special, and are nowadays called *smart polynomials.* We will show that quite amazingly the polynomials that naturally appear when dealing with geometric questions related to polynomial equations are smart.

A bad feature of slp encodings is that two different slp's may encode the same polynomial, or more simply a slp can encode the zero polynomial, without our noticing. Of course, even if we know the degree of f, evaluating in a grid of $(d+1)^n$ points is forbidden for too expensive. There is in this line a remarkable result due to Heintz and Schnorr ([34, Th. 4.4]) that shows that there exist test grids (*correct test sequences*) whose cardinality depend polynomially on the slp length of the polynomial:

Lemma 1.5 *Let $\mathcal{F} := \{f \in k[x_1, \ldots, x_n] : \deg f \leq d, L(f) \leq L\}$. There exists in any big enough set of k (whose size depends polynomially on d and L) a subset $\mathcal{A}$ with $\#\mathcal{A} = (nL)^{\mathcal{O}(1)}$ such that:*

$$\forall f \in \mathcal{F}, \ f(a) = 0 \ \forall a \in \mathcal{A}^n \Rightarrow f = 0.$$

This is an existence result and nobody knows until now how to exhibit economically such correct test sequences. However, one can replace it by the Zippel-Schwartz zero test for the design of probabilistic algorithms ([68, 59]):

Lemma 1.6 *Let $\mathcal{A} \subset k$ be a finite set. For any $f \in k[x_1, \ldots, x_n]$, $f \neq 0$, the probability that a randomly chosen $a \in \mathcal{A}^n$ annihilates f verifies*

$$\mathrm{Prob}(f(a) = 0) \leq \frac{\deg f}{\#\mathcal{A}}.$$

1.2 Algorithms

The formalization of our algorithms is given by the Blum-Shub-Smale machine over k with the restriction that the only branches allowed are comparisons to zero. Roughly speaking the algorithm is a finite sequence of instructions performed on the input, where each instruction can be an arithmetic operation $(+, -, \cdot)$ on elements of k or a comparison to zero and a selection of how to continue depending on the result of the comparison. We refer to [5, Ch. 3 and 4]. The special feature here is that most of the algorithms we refer to compute as their output slp encodings instead of lists of coefficients (dense or sparse encodings). For many of them, the input is also encoded by slp's, see [37, Sec. 1.2] for a more formal presentation.

In some cases we refer to *bounded probability algorithms*, algorithms with special nodes that flip coins (these nodes randomly choose the following instruction between two possible ones with probability $1/2$ for each of them ([5, Sec. 17.1], [37, Sec. 1.2]) so that the error probability of the result of the algorithm is bounded by $1/4$. In our setting probability is introduced by choosing a random element a with equidistributed probability in a set $\{0, 1, \ldots, N-1\}^n$ where a certain polynomial f of known degree will be specialized in order to apply the Zippel-Schwartz zero-test.

The complexity or time of the algorithm is equal to the number of arithmetic operations performed (each arithmetic operation on k has unit cost), comparisons, selections and flipping coins can be considered with no cost since if they are meaningful their number is bounded by the number of operations. Again this model can be adapted to more realistic needs, e.g. counting bit operations in an integer setting.

1.3 Parameters

We adopt the following parameters to measure an input polynomial system $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$: the number of variables n, a bound for the degrees d, the number of polynomials s, the maximum length L of slp's computing $f_1, \ldots, f_s$ and also a parameter δ which measures the maximum dimension of the underlying linear algebra structures. This new parameter appeared naturally during the search of good algorithms with slp encodings, and is mentioned for the first time in [25]. It is associated to the input polynomials and is called the *geometric degree of the input polynomial system*. It is in the worst case bounded by the Bézout number d^n although it can be substantially smaller.

In case $s \le n + 1$ and $f_1, \ldots, f_s$ is a reduced weak regular sequence, that is, for $1 \le i \le s - 1$, f_{i+1} is not a zero-divisor modulo the ideal $(f_1, \ldots, f_i)$ which is a radical ideal (this implies in particular that for $1 \le i \le s$, the variety $V(f_1, \ldots, f_i)$ is pure of codimension i), we define here the parameter δ as

$$\delta := \max_{1 \le i \le s} \deg(V(f_1, \ldots, f_i))$$

where deg denotes the usual geometric affine degree of the variety.

For instance if $V \subset \mathbb{A}^3$ is the variety defined by the reduced regular sequence $f_1 = x(z-1), f_2 = z, f_3 = y(z-1)$, one obtains $\delta = 2$ (note that δ does not coincide with the cardinality of this finite variety, but measures the biggest degree attained by successively adding the equations).

In case the input polynomials $f_1, \ldots, f_s$ do not define a reduced weak regular sequence, we perturb them performing a sufficiently generic scalar combination: for a *good choice* of $a_1, \ldots, a_{n+1} \in k^s$ (the meaning of good choice is explained in Section 1.5 below), we define the polynomials $\tilde{f}_1, \ldots, \tilde{f}_{n+1}$ as

$$\tilde{f}_1 := a_{11} f_1 + \cdots + a_{1s} f_s, \ldots, \tilde{f}_{n+1} := a_{n+11} f_1 + \cdots + a_{n+1s} f_s,$$

and we define a geometric degree δ (associated to $a := (a_1, \ldots, a_{n+1})$) of the input polynomial system as

$$\delta(a) := \max_{1 \le i \le n+1} \deg(V(\tilde{f}_1, \ldots, \tilde{f}_i)).$$

For instance the value of δ associated to the system of polynomials $f_1 = x^2, f_2 = x - y^2, f_3 = 1 - yz$ is not 1 as this is not a reduced sequence, but 2.

The definition given here is a simplified version of the many different definitions of geometric degree of the input polynomial system that appear in different papers, each time adapted to their context (see for instance [25, 47, 61, 50, 28, 37]). In particular we only choose *a* geometric degree depending of the good choice a, which is enough for our purpose, and skip the definition of *the* geometric degree which is an intrinsic quantity that does not depend on the choice of a.

1.4 Basic linear algebra ingredients

Our algorithms rely on the possibility of performing the usual linear algebra operations by means of algorithms behaving well with slp's. For instance the computation of (slp's for) the coefficients of the characteristic polynomial of a $D \times D$ matrix, as well as the computation of its adjoint and its determinant, can be done within $\mathcal{O}(D^4)$ arithmetic operations with no divisions and no branches [3].

Another useful fact is that a slp of length L for the computation of a polynomial $f \in k[x_1, \ldots, x_n]$ of degree bounded by d produces easily slp's of length $\mathcal{O}(d^2 L)$ for the homogeneous components of any given degree of f ([45, Lem. 13], [8, Lem. 21.25].

Also, there is a classic division free algorithm known as Strassen's Vermeidung von Divisionen [64] which computes a slp for the quotient of two polynomials provided it is a polynomial. More precisely

Proposition 1.7 *Let $f, g \in k[x_1, \ldots, x_n]$ be polynomials encoded by slp's of length L such that $f(0) = 1$. Assume that f divides g in $k[x_1, \ldots, x_n]$ and that $\deg g/f \le d$. Then there is an algorithm which computes a slp for g/f within complexity $\mathcal{O}(d^2(d + L))$.*

7

The idea is simply to use that

$$f^{-1} = \frac{1}{1 - (1 - f)} = \sum_{k \geq 0} (1 - f)^k$$

and to truncate all operations and the result at order d. This algorithm is easily adapted to more general situations when $f(a) \neq 0$ for $a \in k^n$, or when $f \neq 0$ and one looks probabilistically for $a \in k^n$ such that $f(a) \neq 0$.

Finally there is a bounded probability algorithm to compute the greatest common divisor of two multivariate polynomials encoded by slp's [41].

1.5 Input preparation

Given $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ which define an arbitrary variety $V := V(f_1, \ldots, f_s) \subset \mathbb{A}^n$, as many authors do we replace the original input system by taking a linear combination of the polynomials and a change of variables, in order to attain the good underlying linear algebra structure we discussed partly in Section 1.3.

- In case $f_1, \ldots, f_s$ are not (known to be) a reduced regular sequence we replace them by $\tilde{f}_1, \ldots, \tilde{f}_{n+1}$ as explained in Section 1.3, for a choice of $a = (a_1, \ldots, a_{n+1}) \in k^{(n+1) \times s}$ such that:

  - $V(\tilde{f}_1, \ldots, \tilde{f}_{n+1}) = V$.
  - For $0 \leq r \leq n - 1$, if $V(\tilde{f}_1, \ldots, \tilde{f}_{n-r}) \neq V$, then $I_r := (\tilde{f}_1, \ldots, \tilde{f}_{n-r})$ is a radical ideal of dimension r outside V (that is every primary component $\mathcal{Q}$ of I_r such that $V(\mathcal{Q}) \not\subset V$ is prime of dimension r).

  These conditions imply that if a minimal equidimensional decomposition of V is given by

  $$V = V_0 \cup \cdots \cup V_{n-1}$$

  where for $0 \leq r \leq n - 1$, V_r is either empty or equidimensional of dimension r, then

  $$V(I_r) = V_r' \cup V_r \cup \cdots \cup V_{n-1}$$

  where V_r' is either empty or an equidimensional variety of dimension r (that contains in particular all the components of lower dimension of V).

  In case the original variety $V := V(f_1, \ldots, f_s)$ is empty, the perturbed polynomials $\tilde{f}_1, \ldots, \tilde{f}_{n+1}$ verify that for a certain $t \leq n$, $(\tilde{f}_1, \ldots, \tilde{f}_t)$ is a reduced regular sequence and $V(\tilde{f}_1, \ldots, \tilde{f}_{t+1}) = \emptyset$.

  An important fact is that Bertini's theorem insures that for a generic choice of such a matrix a, the desired conditions are always attained (see for instance [1, Sec. 4], [27, Sec. 3.2], [58, Prop. 18 and proof of Th. 19]). Moreover, the coefficients of the matrices a giving bad choices belong to a hypersurface of degree bounded by $4(d+1)^{2n}$ ([50, Lem. 1 and 2] or [46, Prop. 4.3 and Cor. 4.4]). This enables us to apply the Zippel-Schwartz zero test.

- We replace the variables $x_1, \ldots, x_n$ by new variables $y_k = b_{k1}x_1 + \cdots b_{kn}x_n$, $1 \leq k \leq n$, such that for $0 \leq r \leq n - 1$, the variables $y_1, \ldots, y_r$ are in Noether normal position with respect to the equidimensional component W_r of $V(I_{n-r})$ of dimension r, that is, the morphism $\pi : W_r \to \mathbb{A}^r$, $y \mapsto (y_1, \ldots, y_r)$ is finite of degree $\deg W_r$.

  In fact we look for a more technical condition (see Assumption 4.1 below) which implies this Noether position one. Again the important fact is that a generic choice of the new variables insures the desired conditions. Moreover, the coefficients of the matrices b giving bad choices belong to a hypersurface of degree bounded by $n(n-1)d^{2n}$ ([46, Prop. 4.5]), which enables us to apply the Zippel-Schwartz zero test again.

2 The Nullstellensatz

This section discusses results on the effective Nullstellensatz that motivate the spirit of this survey paper. It also presents some complexity aspects in more detail.

The (weak) Nullstellensatz states (for a field k with algebraic closure $\overline{k}$):

> Let $f_1, \ldots, f_s$ be polynomials in $k[x_1, \ldots, x_n]$. The equation system
>
> $$f_1(x) = 0, \ldots, f_s(x) = 0$$
>
> has no solution in $\overline{k}^n$ if and only if there exist $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ satisfying the Bézout identity
>
> $$1 = g_1 f_1 + \cdots + g_s f_s. \tag{1}$$

Upper bounds

Bounds for the degrees of polynomials g_i's satisfying Identity (1) immediately yield a linear system of equations. Showing such bounds is what is nowadays called *Effective Nullstellensätze*.

In 1926, Hermann [36] (see also [31], [54]) proved that in case Identity (1) holds, there exist $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ with $\deg g_i f_i \leq 2 \, (2d)^{2^{n-1}}$. After a conjecture of Keller and Gröbner, this estimate was dramatically improved by Brownawell [7] to $\deg g_i f_i \leq n^2 d^n + n \, d$ in case $\mathrm{char}\,(k) = 0$, while Caniglia, Galligo and Heintz [9] showed that $\deg g_i f_i \leq d^{n^2}$ holds in the general case.

These results were then independently refined by Kollár [43] and by Fitchas and Galligo [19] to

$$\deg g_i f_i \leq \max\{3, d\}^n, \tag{2}$$

which is optimal in case $d \geq 3$. For $d = 2$, Sombra [62] showed that the bound $\deg g_i f_i \leq 2^{n+1}$ holds.

A lower bound

We turn now to a lower bound estimate. The following well-known example due to Masser and Philippon yields a lower bound for any general degree estimate. Set

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

for any positive integers n and d. These are polynomials of degree d in n variables. Let $g_1, \ldots, g_n \in \mathbb{Q}[x_1, \ldots, x_n]$ be polynomials satisfying Bézout identity (1). Specializing it at

$$x_1 := t^{(d-1)d^{n-2}}, x_2 := t^{(d-1)d^{n-3}}, \ldots, x_{n-1} := t^{d-1}, x_n := 1/t \quad \text{for} \quad t \neq 0$$

one obtains

$$1 = g_1(t^{(d-1)d^{n-2}}, \ldots, t^{d-1}, 1/t) \, t^{(d-1)d^{n-1}}$$

which implies that $\deg_{x_n} g_1 \geq (d-1)d^{n-1}$.

In fact here is a Bézout identity with optimal degrees for these polynomials:

$$1 = x_n^{(d-1)d^{n-1}} x_1^d - x_n^{(d-1)d^{n-1}} \left(x_1^d - (x_2^d)^d\right) - \cdots - x_n^{(d-1)d^{n-1}} \left(x_{n-2}^{d^{n-2}} - (x_{n-1}^d)^{d^{n-2}}\right) + \left(1 - (x_{n-1}x_n^{d-1})^{d^{n-1}}\right)$$

i.e. $g_1 = x_n^{(d-1)d^{n-1}}, g_2 = -g_1\left(x_1^{d-1} + \cdots + (x_2^d)^{d-1}\right), \ldots, g_n = 1 + x_{n-1}x_n^{d-1} + \cdots + (x_{n-1}x_n^{d-1})^{d^{n-1}-1}$.

This example immediately shows that the dense encoding of any output $g_1, \ldots, g_n$ has length at least $\binom{d^n - d^{n-1} + n}{n}$, which is exponential in the length $\binom{d+n}{n}$ of the dense encoding of the input. Moreover,

a slight perturbation of this example —replacing x_n by a linear combination of the variables— destroys all the sparsity of the output.

However in this case there is at least one choice of *smart* polynomials since a coarse computation shows that $L(g_1) \leq n(d-1)$ and $L(g_i) \leq (n+5i)(d-1)$. Here we have used the identity:

$$x^{d^i-1}+x^{d^i-2}y+\cdots+y^{d^i-1} = \left(x^{d-1}+x^{d-2}y+\cdots+y^{d-1}\right) \cdots \left(x^{d^{i-1}(d-1)}+x^{d^{i-1}(d-2)}y+\cdots+y^{d^{d-1}(d-1)}\right).$$

Arithmetic bounds

Now let us consider the arithmetic aspects of the Nullstellensatz, that is when the input polynomials have integer coefficients (or more generally coefficients in a number ring). In the case of integer coefficients, the Nullstellensatz takes the following form:

> Let $f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_n]$ be polynomials such that the equation system
>
> $$f_1(x) = 0, \ldots, f_s(x) = 0$$
>
> has no solution in $\mathbb{C}^n$. Then there exist $a \in \mathbb{Z} \setminus \{0\}$ and $g_1, \ldots, g_s \in \mathbb{Z}[x_1, \ldots, x_n]$ satisfying the Bézout identity
>
> $$a = g_1 f_1 + \cdots + g_s f_s.$$

Let $h(f)$ denote the *height* of an arbitrary polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$, defined as the logarithm of the maximum absolute value of its coefficients, and for the sequel set $h := \max_i h(f_i)$. A slight modification of Masser and Philippon example yields the lower bound $h(a) \geq d^n h$.

On the other hand the bound (2) reduces Bézout identity (1) to a system of $\mathbb{Q}$-linear equations, which by application of Cramer rule gives an estimate for the height of a and the polynomials g_i of type $s\, d^{n^2}\, (h + \log s + d)$.

It was soon conjectured that the optimal height bound should be closer to the mentioned lower bound than to this trivial upper bound.

Philippon [55] obtained the first sharp estimate for the denominator a in a Bézout identity: $\deg g_i \leq (n+2)\, d^n$, $h(a) \leq \kappa(n)\, d^n(h+d)$, where $\kappa(n)$ depends exponentially on n. Then the first essential progress on height estimates for all the polynomials g_i was achieved by Berenstein and Yger who, from 1991 to 1999 [1, 2], obtained $\deg g_i \leq n\,(2\,n+1)\,d^n$, $h(a), h(g_i) \leq \lambda(n)\, d^{4n+3}\,(h+\log s+d \log d)$, where $\lambda(n)$ is a (non-explicit) constant which depends exponentially on n. Their proof relies on the previous work of Philippon and on techniques from complex analysis. Using the algebraic techniques described in Paragraph "Idea of an algorithm" below, the author and Pardo [44, 45] obtained the same kind of estimates though less precisely. In 1998 Sombra convinced us that the techniques were better than the obtained results and that what was lacking was a deeper height analysis. This lead to the nowadays best and essentially optimal arithmetic bound [46] stated in Paragraph "Computational results" below.

Idea of an algorithm

Since 1993, Heintz, Giusti and their collaborators initiated a strong current area of research on computational issues related to the Nullstellensatz [27, 20, 45, 25, 24, 30]. The fact that the polynomials g_i's satisfying the Bézout identity in the Masser and Philippon counterexample were smart did not seem to be a coincidence. They searched for arguments and tools behaving well under specializations in order to generalize this fact. A good algorithmic answer is given by the application of the duality theory for Gorenstein algebras to this setting. We refer to E. Kunz [48, Appendix F] for a complete mathematical presentation of the duality theory.

The initial spirit of the algorithm is quite simple. It works by successive divisions:

$$1 \in (f_1, \ldots, f_s) \iff f_s \text{ is invertible } \pmod{(f_1, \ldots f_{s-1})}$$

and more generally, once $g_s, \ldots, g_{i+1}$ are determined

$$1 - g_s f_s - \cdots - g_{i+1} f_{i+1} \in (f_1, \ldots, f_i) \iff \exists g_i : 1 - g_s f_s - \cdots - g_{i+1} f_{i+1} \equiv g_i f_i \pmod{(f_1, \ldots f_{i-1})}.$$

To illustrate the algorithm assume now that $(f_1, \ldots, f_s)$ defines the empty variety, that $s = n + 1$ and that $I_r := (f_1, \ldots, f_{n-r})$ is an ideal of dimension r for $0 \le r \le n - 1$. Thus $I_0 := (f_1, \ldots, f_n)$ is a zero-dimensional ideal, and the first step is straightforward: $B := k[x_1, \ldots, x_n]/I_0$ is a finite-dimensional k-vector space. Therefore an inverse g_{n+1} for f_{n+1} in B can be obtained for instance using the characteristic polynomial χ_{n+1} of (the multiplication by) f_{n+1} in B and the Cayley-Hamilton theorem: $\chi_{n+1}(t) = t^D + c_{D-1} t^{D-1} + \cdots + c_0$ (with $c_0 \in k^*$ since f_{n+1} is invertible) implies that we can define

$$g_{n+1} := -\frac{1}{c_0}(f_{n+1}^{D-1} + c_{D-1} f_{n+1}^{D-2} + \cdots + c_1). \tag{3}$$

For the second recursion step, even if one can mimic the finite-dimensional vector space argument, in the best case the framework is a finite-rank free module $B := k[x_1, \ldots, x_n]/I_1$ over $A := k[x_1]$, and the argument above fails since here $c_0 \in k[x_1]$ does not necessarily divide the expression in the numerator of the corresponding formula (3).

The trace formula giving the duality theory of Gorenstein algebras is the tool which enables us to generalize the previous argument to the case when we are not in a finite vector space frame. It performs effective divisions modulo complete intersection ideals. It was introduced in the context of the effective Nullstellensatz in [20], and then refined in [58, 45, 47, 24, 30]. The latest optimal results for the arithmetic aspects when the base ring is a number ring are obtained in [46].

Here we describe only the basic aspects of the theory we need to sketch the proof.
Let $I_r = (f_1, \ldots, f_{n-r}) \subset k[x_1, \ldots, x_n]$ be a reduced complete intersection ideal (of dimension r), such that $B := k[x_1, \ldots, x_n]/I_r$ is a finite-rank free module over $A := k[x_1, \ldots, x_r]$.
The dual A-module $B^* := \mathrm{Hom}_A(B, A)$ can be seen as a B-module with scalar multiplication defined by $f \cdot \tau(g) := \tau(f g)$ for $f, g \in B$ and $\tau \in B^*$. It happens to be a free B-module of rank 1. Any of its generators is called a *trace* of B. There is a canonical trace σ associated to the complete intersection I_i, and particular polynomials $a_m, b_m \in k[x_1, \ldots, x_n]$ verifying the following *trace formula*:

$$\forall g \in k[x_1, \ldots, x_n], \ g \equiv \sum_m \sigma(g a_m) b_m \pmod{I_r}.$$

The canonical trace σ is related to the usual trace Tr of B/A by the equality $\mathrm{Tr}(g) \equiv \sigma(Jg)$ $\pmod{I_r}$ where J is the Jacobian determinant of the complete intersection I_r with respect to the variables $x_{i+1}, \ldots, x_n$.

Now we are able to describe —at least theoretically— the second recursion step. All steps follow the same pattern.
Let $I_1 = (f_1, \ldots, f_{n-1})$, $B = k[x_1, \ldots, x_n]/I_1$ and $A := k[x_1]$ be in the hypothesis of the duality theory. Let $\chi_n(t) := t^D + c_{D-1} t^{D-1} + \cdots + c_0$ be the characteristic polynomial of f_n in B/A. Observe that $c_0 \in A \setminus \{0\}$ since f_n is not a zero-divisor modulo I_1. We define

$$\begin{aligned}
f_n^* &:= f_n^{D-1} + c_{D-1} f_n^{D-2} + \cdots + c_1, \\
g_n &:= -\frac{1}{c_0} \sum_m \sigma(f_n^*(1 - g_{n+1} f_{n+1}) a_m) b_m.
\end{aligned}$$

Fact: g_n *belongs to* $k[x_1, \ldots, x_n]$ (*i.e.* c_0 *divides the numerator*) *and* $g_n f_n \equiv 1 - g_{n+1} f_{n+1} \pmod{I_1}$.
Proof.–

- In fact $c_0 \mid \sigma(f_n^*(1 - g_{n+1} f_{n+1}) a_m)$ in $A = k[x_1]$ for every m:

11

Since by hypothesis there exists $q \in k[x_1, \ldots, x_n]$ such that $1 - g_{n+1} f_{n+1} \equiv q\, f_n \pmod{I_1}$ and on the other hand $f_n^* f_n \equiv -c_0 \pmod{I_1}$, we infer that $f_n^*(1 - g_{n+1} f_{n+1}) \equiv -c_0 q \pmod{I_1}$. Therefore

$$\sigma(f_n^*(1 - g_{n+1} f_{n+1}) a_m) = \sigma(-c_0 q\, a_m) = -c_0 \sigma(q\, a_m)$$

since σ is a A-morphism and $c_0 \in A$.

- By the trace formula, $-c_0\, g_n \equiv f_n^*(1 - g_{n+1} f_{n+1}) \equiv -c_0 q \pmod{I_1}$. Thus $c_0\, g_n\, f_n \equiv c_0\,(1 - g_{n+1} f_{n+1}) \pmod{I_1}$. Since c_0 is not a zero-divisor modulo I_1 we conclude that $g_n f_n \equiv 1 - g_{n+1} f_{n+1} \pmod{I_1}$.

We finally observe that the relationship between this trace σ and the canonical trace Tr allows us to replace in the computations σ that one does not know by Tr which is computable as a coefficient of the characteristic polynomial. The polynomials a_m, b_m are also easily computable.

Computational results

The foundational paper of this computational current of research on the Nullstellensatz is the one of Giusti, Heintz and Sabia [27] followed by [20]:

Theorem 2.1 *Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ be polynomials of degree bounded by d. Then there is a bounded probability algorithm of size $s^{\mathcal{O}(1)} d^{\mathcal{O}(n)}$ which decides whether the ideal $(f_1, \ldots, f_s)$ is trivial or not, and in case it is, produces slp's of the same length for polynomials $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ satisfying the Bézout identity $1 = g_1 f_1 + \cdots + g_s f_s$. The degree of these polynomials was first bounded by $d^{\mathcal{O}(n^2)}$ [27, Sec. 2, Th.] and then by $d^{\mathcal{O}(n)}$ [20, Th. 2].*

This result follows after an input preparation of the kind of the one described in Section 1.5 in order to place the input in the hypothesis of the duality theory, and a recursive application of the division procedure. The canonical trace is computed as a coefficient of the characteristic polynomial of the multiplication map in B/A. A suitable basis of the natural zero-dimensional vector space associated to B/A is obtained reducing to the two variables case.

Later on, the input polynomials were no longer considered in their dense encoding: the complexity bounds are now given in terms of the lengths of the slp encoding and of the geometric degree of the input polynomials [25, Th. 20], [24, Th. 4, Th. 21], that is what is called *intrinsic Nullstellensatz*:

Theorem 2.2 *Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ be polynomials of degree bounded by d given by slp's of length bounded by L with no common zeroes in $\overline{k}^n$. Let δ be a geometric degree of the input equation system. Then there is a bounded probability algorithm of size $(snd\delta L)^{\mathcal{O}(1)}$ which produces slp's of the same length for polynomials $g_1, \ldots, g_s \in k[x_1, \ldots, x_n]$ satisfying the Bézout identity $1 = g_1 f_1 + \cdots + g_s f_s$. The degree of these polynomials are bounded by $n^2 d\delta$.*

The proof of this theorem is based on the techniques of [27] in what concerns the recursive divisions. The dependence on δ is due to the precise results on the degrees of [58] and [47, 61] where bounds in terms of δ were first computed. In order to obtain a final bound depending polynomially on L (and not on d^n) the authors introduced a formal version of Newton's method which produces with good complexity good bases of the complete intersection ideals recursively considered. This method is essential in all further developments and will be introduced in a simple frame in Section 4.1.

Now let us add the arithmetic aspects of the Nullstellensatz.
The duality technique introduced above also yields arithmetic bounds. That was done in [44, 45]: the slp produces an integer a and polynomials g_i's such that $\deg g_i \leq (n\, d)^{c\, n}$, $h(a), h(g_i) \leq (n\, d)^{c\, n}(h + \log s + d)$, where c is a universal constant. Then an arithmetic analogue of the intrinsic Nullstellensatz was obtained in [30, 29]. To this aim the authors introduced the notion of *height of a polynomial system*, the arithmetic analogue of the geometric degree of the system. In [46] these results are generalized and brought to an optimal form. As a consequence of this intrinsic statement, a sparse version is obtained, recently improved by Sombra in [63].
More precisely, the main result of [46] in its simplest form is the following:

Theorem 2.3 *Let $f_1, \ldots, f_s \in \mathbb{Z}[x_1, \ldots, x_n]$ be polynomials without common zeros in $\mathbb{C}^n$. Set $d := \max_i \deg f_i$ and $h := \max_i h(f_i)$.*
Then there exist $a \in \mathbb{Z} \setminus \{0\}$ and $g_1, \ldots, g_s \in \mathbb{Z}[x_1, \ldots, x_n]$ such that

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

- $\deg g_i \leq 4 \, n \, d^n,$

- $h(a), h(g_i) \leq 4 \, n \, (n+1) \, d^n \, (h + \log s + (n+7) \, \log(n+1) \, d).$

The proof of this arithmetic Nullstellensatz also relies on the trace formula. However there is another key ingredient which is the notion of local height of a variety defined over a number field K introduced there:
For $V \subset \mathbb{A}^n(\overline{\mathbb{Q}})$ an equidimensional affine variety defined over K and for an absolute value v over K, the *local height* $h_v(V)$ of V at v is defined —inspired by results of Philippon— as a Mahler measure of a suitable normalized Chow form of V. This definition is consistent with the Falting's height $h(V)$ of V, namely:

$$h(V) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} N_v \, h_v(V),$$

where M_K denotes the set of canonical absolute values of K, and N_v the local degree of K at v. Then the authors obtained estimations of the local height of the trace and the norm of a polynomial $f \in K[x_1, \ldots, x_n]$ with respect to an integral extension $K[\mathbb{A}^r] \hookrightarrow K[V]$. There are also local analogues of many of the global results of Bost, Gillet and Soulé [6] and Philippon [56].

3 Zero-dimensional varieties

We devote this section to the description of a zero-dimensional variety by means of two different presentations: a classic description that we call here, following [24, Sec. 2.1], a geometric resolution of the variety (also known as a shape lemma presentation or a rational univariate representation), and its Chow form (also known as the u-resultant when associated to a system of equations). We compare both approaches.
For the whole section, $Z \subset \mathbb{A}^n$ denotes a 0-dimensional variety (that is a finite variety) of cardinality D.

3.1 Geometric Resolutions

Geometric resolutions were first introduced in the works of Kronecker and König in the last years of the XIX century. Nowadays they are widely used in computer algebra. We refer to [23] for a complete historical account.

A *geometric resolution* of Z consists of an affine linear form $\ell(x) = u_0 + u_1 x_1 + \cdots + u_n x_n \in k[x_1, \ldots, x_n]$ and of polynomials $q \in k[t]$ and $w = (w_1, \ldots, w_n) \in k[t]^n$ (where t is a new single variable) such that:

- The affine linear form ℓ is a *primitive element* of Z, that is $\ell(\xi) \neq \ell(\xi')$ for all $\xi \neq \xi'$ in Z.

- The polynomial q is monic of degree D and $q(\ell(\xi)) = 0$ for all $\xi \in Z$; that is,

$$q(t) = \prod_{\xi \in Z} (t - \ell(\xi))$$

is the minimal polynomial of ℓ over Z.

- For $1 \leq i \leq n$, $\deg w_i < D$ and

$$Z = \{(w_1(\ell(\xi)), \ldots, w_n(\ell(\xi)))\,;\ \xi \in Z\} = \left\{(w_1(\tau), \ldots, w_n(\tau))\,;\ \tau \in \overline{k}\ /\ q(\tau) = 0\right\};$$

   that is, w parametrizes Z by the zeroes of q.

Observe that the minimal polynomial q and the parametrization p are uniquely determined by the variety Z and the affine linear form ℓ. We say that (q, w) is *the geometric resolution of Z associated to ℓ.*

The existence of such a geometric resolution of Z (at least with coefficients in $\overline{k}$) is simple to show: Let $\ell(x) = 0$ be any projection hyperplane that separates the zeroes of Z (any generic enough hyperplane will do), and define $q(t) = \prod_{\xi \in Z}(t - \ell(\xi))$. Thus q is a polynomial of degree $D := \#Z$ that vanishes on Z. Now for $1 \leq i \leq n$, let $w_i(t)$ be the unique polynomial of degree strictly bounded by D which verifies that $w_i(\ell(\xi)) = \xi_i$ for every $\xi = (\xi_1, \ldots, \xi_n) \in Z$. Then the polynomial $x_i - w_i(\ell(x))$ also vanishes on Z and it is easy to show that in fact

$$Z = V\left(q(\ell(x)), x_1 - w_1(\ell(x)), \ldots, x_n - w_n(\ell(x))\right).$$

The computation of a geometric resolution

The algorithm that we describe here has its beginning in [26] and the ideas were then refined in [25] with the introduction of Newton's method and in [24] where the use of computable companion matrices replaced theoretical algebraic roots. Further improvements were then developed independently in [51, 28] and [33] where a significant speed-up is obtained by a technique called deforestation.

Here, in order to simplify the presentation we assume that the zero-dimensional variety Z is given as the zero set of a reduced regular sequence $f_1, \ldots, f_n$ in $k[x_1, \ldots, x_n]$.

Theorem 3.1 *([24, Th. 19]) Let $f_1, \ldots, f_n \in k[x_1, \ldots, x_n]$ be polynomials of degree bounded by d and encoded by slp's of length L. Assume that the polynomials are a reduced regular sequence and set δ for a geometric degree of the input polynomial system.*
Then there is a bounded probability algorithm which computes (slp's for) a separating linear form ℓ and a geometric resolution (q, v) of Z associated to ℓ within complexity $(nd\delta L)^{\mathcal{O}(1)}$.

The algorithm has n recursive steps: it adds one equation at a time. For simplicity one assumes that $x_1, \ldots, x_n$ are in Noether normal position with respect to the ideals $(f_1, \ldots, f_i)$, $1 \leq i \leq n$.
The i-th step computes from a geometric resolution of the zero-dimensional variety

$$Z_i := V(f_1, \ldots, f_i) \subset \mathbb{A}^i(\overline{k(x_1, \ldots, x_{n-i})})$$

a geometric resolution of the zero-dimensional variety

$$Z_{i+1} := V(f_1, \ldots, f_{i+1}) \subset \mathbb{A}^{i+1}(\overline{k(x_1, \ldots, x_{n-i-1})}).$$

The first input is given by the geometric resolution $(q(t) := f_1(x_1, \ldots, x_{n-1}, t), w_1(t) := t)$ of $Z_1 := V(f_1)$ associated to the separating linear form $\ell := x_n$, and the last $(n-1)$ step computes a geometric resolution of the zero dimensional variety $Z_n = Z$.

The crucial point here is that the input of step $i+1$ cannot be simply the output of step i, where the natural length of this output would be $L_{i+1} = (nd\delta_i)^{\mathcal{O}(1)} L_i$ (where δ_i is the size of the underlying linear algebra at step i), since in that case the recursion would yield an output length

$$L_n = (nd)^{\mathcal{O}(n)}(\delta_0 \cdots \delta_{n-1})^{\mathcal{O}(1)} L = (nd\delta)^{\mathcal{O}(n)} L$$

which does not represent any improvement with respect to other known algorithms.

The alternative was for the first time addressed in [26] where the authors dealt with the necessity of a compression of the input data at each recursive step that enabled them to add L_i instead

14

of multiplying it : $L_{i+1} = (nd\delta_i)^{\mathcal{O}(1)}L + L_i$. Another principal breakthrough of this paper is that it adapted the concept of geometric resolution to a positive dimension context, rediscovering Kronecker's approach.

The general form of an algorithm like this one is considered in more detail for the computation of Chow forms in Section 5, after the introduction of Newton's method and the use of companion matrices in some simple cases.

3.2 Chow forms

Set $L(U,x) := U_0 + U_1 x_1 + \cdots + U_n x_n$ for a generic (affine) linear form where $U := (U_0, \ldots, U_n)$ denotes a new group of variables. Typically a specialized linear form $\ell(x) := L(u,x)$ does not meet any of the points of Z unless $u \in \mathbb{A}^n$ is a root of the following polynomial

$$\mathcal{C}h_Z(U) = \prod_{\xi \in Z} L(U,\xi).$$

This polynomial is called the (normalized) *Chow form* of Z. It happens to be a homogeneous polynomial in $k[U]$ of degree D. We refer to [60, Section I.6.5] for the proof of this fact.

Thus, the main feature of the Chow form is that for any $u \in k^{n+1}$,

$$\mathcal{C}h_Z(u) = 0 \iff Z \cap \{L(u,x) = 0\} \neq \emptyset.$$

Chow forms → geometric resolutions

A Chow form gives straightforward a "generic" geometric resolution and hence, by specialization, families of geometric resolutions. We describe here the procedure, essentially due to Kronecker:

The polynomial $\mathcal{P}_Z(U,t) \in k[U,t]$ (where t is a single variable like before) defined by

$$\mathcal{P}_Z(U,t) := (-1)^D \mathcal{C}h_Z(U_0 - t, U_1, \ldots, U_n) = \prod_{\xi \in Z}(t - L(U,\xi))$$

verifies that $P(U,x) := \mathcal{P}_Z(U, L(U,x)) = \sum_\alpha a_\alpha(x)U^\alpha$ vanishes clearly on every $\xi \in Z$. Thus, for every α, $a_\alpha(\xi) = 0$ for every $\xi \in Z$, which implies in particular that $\frac{\partial P(U,x)}{\partial U_i}$ also vanishes on every $\xi \in Z$.

Now for $1 \leq i \leq n$,

$$\frac{\partial P}{\partial U_i}(U,x) = \frac{\partial \mathcal{P}_Z}{\partial U_i}(U, L(U,x)) + \frac{\partial \mathcal{P}_Z}{\partial t}(U, L(U,x))x_i$$

implies that for every $\xi \in Z$,

$$\frac{\partial \mathcal{P}_Z}{\partial U_i}(U, L(U,\xi)) + \frac{\partial \mathcal{P}_Z}{\partial t}(U, L(U,\xi))\xi_i = 0.$$

This last equality means that for every $u \in \overline{k}^{n+1}$ such that both $\ell(x) := L(u,x)$ verifies that $\ell(\xi) \neq \ell(\xi')$ for all $\xi \neq \xi'$ in Z and $\frac{\partial \mathcal{P}_Z}{\partial t}(u, \ell(\xi)) \neq 0$ for all $\xi \in Z$ (these conditions are fulfilled in a non-empty open Zariski subset of $\overline{k}^{n+1}$), one has that

$$\xi_i = -\frac{\frac{\partial \mathcal{P}_Z}{\partial U_i}(u, \ell(\xi))}{\frac{\partial \mathcal{P}_Z}{\partial t}(u, \ell(\xi))}.$$

A proper geometric resolution of Z associated to ℓ is then given by $q(t) := \mathcal{P}_Z(u,t)$ and the polynomials $w_i(t)$ that one can obtain using the discriminant $\rho(U)$ of $\mathcal{P}_Z(U,t)$ with respect to t to eliminate the polynomial $\frac{\partial \mathcal{P}_Z}{\partial t}(u, \ell(\xi))$ appearing in the denominator (replacing it by the non-zero constant $\rho(u)$).

Geometric resolutions → Chow forms:

Now let us show how to derive the Chow form from a given geometric resolution of Z with respect to a linear form ℓ. This simple and beautiful construction relies on the fact that even if we do not know the coordinates of each zero ξ of Z, a geometric resolution gives the information of the zeroes altogether:

We are looking for

$$\mathcal{C}h_Z(U) = \prod_{\xi \in Z} L(U, \xi) = |\mathrm{Diag}_{\xi \in Z}\big(L(U, \xi)\big)|,$$

where $|\mathrm{Diag}(\ )|$ denotes the determinant of the diagonal matrix with the entries under the brackets in the diagonal. But the information we have is that of $q(t) = \prod_{\xi \in Z}(t - \ell(\xi))$ whose companion matrix C_q is similar ($\sim$) to $\mathrm{Diag}_{\xi \in Z}\big(\ell(\xi)\big)$ since $\ell(\xi) \neq \ell(\xi')$ for $\xi \neq \xi'$. For $1 \leq i \leq n$, we also have w_i such that $\xi_i = w_i(\ell(\xi))$. Thus

$$w_i(C_q) \ \sim \ w_i\big(\mathrm{Diag}_{\xi \in Z}(\ell(\xi))\big) \ \sim \ \mathrm{Diag}_{\xi \in Z}\big(w_i(\ell(\xi))\big) \ \sim \ \mathrm{Diag}_{\xi \in Z}\big(\xi_i\big).$$

We infer that

$$L\big(U, (\mathrm{Id}, w_1(C_q), \dots, w_n(C_q))\big) \ \sim \ \mathrm{Diag}_{\xi \in Z}\big(L(U, \xi)\big)$$

and we conclude by taking the determinant of the left hand side.

This beautiful application of companion matrices is a crucial tool that was introduced in this context in [24, pp. 285-286] to replace each zero in Z by their "all-together information".

4 Equidimensional varieties

A variety is said to be equidimensional if all its irreducible components have the same dimension. We recall that the degree of an equidimensional variety V is defined as the number of points in the intersection of V with a generic linear variety of codimension equal to the dimension of V.

To simplify the presentation, we set $n = r + m$ and we distiguish the variables in two groups: the set of free variables $y = (y_1, \dots, y_r)$ and the set of dependent variables $x = (x_1, \dots, x_m)$ of the extension $k[V]$: for that purpose we assume for the whole section that $V \subset \mathbb{A}^n = \mathbb{A}^{r+m}$ is an equidimensional variety of dimension r and degree D, defined by polynomials in $k[y_1, \dots, y_r, x_1, \dots, x_m]$, which satisfies the following assumption:

Assumption 4.1 *We assume that $Z := V \cap \{y_1 = 0, \dots, y_r = 0\}$ is a zero-dimensional variety of cardinality $\#Z = \deg V = D$.*

Assumption 4.1 implies that the variables $y_1, \dots, y_r$ are in Noether normal position with respect to V [46, Lem. 2.14]. That means that if we set $A := k[y_1, \dots, y_r]$, $A \cap I(V) = \{0\}$ holds, and that for $1 \leq i \leq m$, there is an integral dependence equation for x_i over A modulo $I(V) \subset A[x_1, \dots, x_m]$: there exists a non-zero and monic polynomial $p_i \in A[x_i] \cap I(V)$. We remark that the previous condition is satisfied by any variety under a generic linear change of variables.

4.1 Geometric resolutions

We present here the notions of geometric resolution of an equidimensional variety of positive dimension.

Under Assumption 4.1 we can reduce easily to the zero-dimensional case: we invert the variables $y_1, \dots, y_r$. We set $K := k(y_1, \dots, y_r)$ for the field of fractions of $A = k[y_1, \dots, y_r]$ and we consider the following objects:

$$
\begin{aligned}
I^e &:= K[x_1, \dots, x_m] \cdot I(V) \ \subset K[x_1, \dots, x_m]\\
V^e &:= V(I^e) \ \subset \overline{K}^m,
\end{aligned}
$$

where $I(V)$ is the ideal of V and $V(I^e)$ is the variety defined by I^e. V^e is a zero-dimensional variety of cardinality $D = \deg V$ and a geometric resolution of V is (essentially) given by a geometric resolution of V^e. It does not describe the whole variety V but describes it outside a given hypersurface. It consists of an affine linear form $\ell = u_0 + u_{r+1}x_1 + \cdots + u_{r+m}x_m \in k[x_1, \ldots, x_m]$ and of polynomials $q \in A[t]$ and $w = (w_1, \ldots, w_m) \in A[t]^m$ such that:

- The affine linear form ℓ is a *primitive element* of V^e, that is $\ell(\xi) \neq \ell(\xi')$ for all $\xi \neq \xi'$ in V^e.

- The polynomial q, of degree D in t, is the monic minimal polynomial of ℓ with respect to the extension $K \hookrightarrow K[V^e]$. The Noether position assumption guarantees that the coefficients of q belong to A and also that the *total* degree of q equals D (see for instance [58, Cor. 2]).

- For $1 \leq i \leq m$, $\deg_t w_i < D$ and $\rho\, x_i = w_i(\ell)$ in $K[V^e]$, where $\rho \in A$ is the discriminant of q with respect to t. The polynomial w_i also belongs to $A[t]$ [28, Sec. 3.2].

Thus, we infer that

$$V^e = \{\, (\frac{w_1(\ell(\xi))}{\rho}, \ldots, \frac{w_m(\ell(\xi))}{\rho})\, ;\, \xi \in V^e \,\} = \{\, (\frac{w_1(\tau)}{\rho}, \ldots, \frac{w_m(\tau)}{\rho})\, ;\, \tau \in \overline{K} \,/\, q(\tau) = 0 \,\}.$$

In particular, since q is monic in t, for every $\eta = (\eta_1, \ldots, \eta_r) \in \mathbb{A}^r$ such that $\rho(\eta) \neq 0$, $\#(V \cap \{y_1 = \eta_1, \ldots, y_r = \eta_r\}) = D$ and the D roots $(\eta, \xi_\eta) \in \mathbb{A}^{r+n}$ are obtained via the D different roots τ_η of $q(\eta, t) = 0$:

$$V \cap \{y_1 = \eta_1, \ldots, y_r = \eta_r\} = \{\, (\eta_1, \ldots, \eta_r, \frac{w_1(\eta, \tau_\eta)}{\rho(\eta)}, \ldots, \frac{w_m(\eta, \tau_\eta)}{\rho(\eta)})\ \text{ for } \tau_\eta \text{ s.t. } q(\eta, \tau_\eta) = 0 \,\}.$$

For simplicity of notation, we say that outside the hypersurface $\{\rho = 0\} \subset \mathbb{A}^{r+m}$ the variety $V \subset \mathbb{A}^{r+m}$ coincides with

$$\{\, (y, \frac{w(y, \tau_y)}{\rho(y)})\ \text{ for } \tau_y \text{ s.t. } q(y, \tau_y) = 0 \,\}.$$

We say that (q, w) is the geometric resolution of V associated to ℓ. It gives a simple description of V outside the discriminant variety. There is another equivalent approach, more suitable algorithmically, where the geometric resolution of V is defined outside the variety $\{q' = 0\}$ where $q' = \partial q / \partial t$ instead of outside the discriminant variety (cf. Section 3.2).

Observe that Assumption 4.1 implies that

$$Z = V \cap \{y_1 = 0, \ldots, y_r = 0\} = \{(0, \frac{w(0, \tau_0)}{\rho(0)})\ \text{ for } \tau_0 \text{ s.t. } q(0, \tau_0) = 0 \,\}.$$

The next section is crucial: it shows how the tractable information of the r-dimensional equidimensional variety V is encoded in the arbitrary input equations plus the information of the zero-dimensional fibre Z. In other terms it shows how to recover a geometric resolution of V from a geometric resolution of Z, lifting the points $(0, \xi_0) \in Z$ to the corresponding $(y, \xi_y) \in V$.

4.2 Dimension zero → positive dimension

Let $V \subset \mathbb{A}^{r+m}$ be an equidimensional variety of dimension r satisfying Assumption 4.1 and set as usual $Z := V \cap \{y_1 = 0, \ldots, y_r = 0\}$. Supppose we are given a geometric resolution (q_Z, w_Z) of Z associated to a separating linear form ℓ. How can we derive from it a geometric resolution (q_V, w_V) of V?

The major tool here is the application of Newton's method to lift an "approximate zero", that is a geometric resolution of the zero-dimensional fibre Z, to the geometric resolution of V. Newton's method has been applied in a similar way to recover the exact factorization of multivariate polynomials from factorization algorithms for univariate polynomials by E. Kaltofen in [40]. For polynomial

systems it has been previously used by W. Trinks [66] and by F. Winkler [67]. In our specific frame it has been re-introduced by J. Heintz et al. in [25].

First let us recall Hensel's lifting, that is, the algebraic version of Newton's method, in its classic presentation:

Proposition 4.2 *Let p be a prime integer number, $f \in \mathbb{Z}[x]$ and $\xi_0 \in \mathbb{Z}$ such that*

$$f(\xi_0) \equiv 0 \pmod{p}, \quad f'(\xi_0) \not\equiv 0 \pmod{p}.$$

Then, for all $k \in \mathbb{N}$, there exists $\xi_k \in \mathbb{Z}$ such that

$$f(\xi_k) \equiv 0 \pmod{p^{2^k}}, \quad \xi_k \equiv \xi_0 \pmod{p}.$$

The existence (and also uniqueness mod p^{2^k}) of this sequence of integers is given by the recursive application of Newton's operator

$$N_f(x) = x - \frac{f(x)}{f'(x)}$$

to the input approximate zero ξ_0:

$$\text{for all } k \geq 1, \ \xi_k \equiv N_f(\xi_{k-1}) \pmod{p^{2^k}}.$$

Hensel's lifting translates directly to a constructive implicit function theorem, that is the version we use here:

Proposition 4.3 *Set $A := k[y_1, \ldots, y_r]$ and $A[x] := A[x_1, \ldots, x_m]$. Let $V \subset \mathbb{A}^{r+m}$ be an equidimensional variety of dimension r defined by a reduced regular sequence $f_1, \ldots, f_m \subset A[x]$, and assume moreover that V satisfies Assumption 4.1.*
Set $\mathcal{M} = (y_1, \ldots, y_r) \subset A$ for the maximal ideal associated to 0, $F(y,x) := (f_1(y,x), \ldots, f_m(y,x))$ and $D_x F := (\partial f_i / \partial x_j)_{1 \leq i,j \leq m}$.
Let $\xi_0 \in \mathbb{A}^m$ be such that $F(y, \xi_0) \in \mathcal{M}$ (i.e. $F(0, \xi_0) = 0$, that is $(0, \xi_0) \in Z$) and $|D_x F|(y, \xi_0) \notin \mathcal{M}$.
Then the recursive application of

$$N_F(x^t) := x^t - (D_x F(y,x))^{-1} F(y,x)^t$$

initialized at ξ_0 approximates the corresponding fiber root $(y, \xi_y) \in V$ with quadratic precision. That is, if N_F^k denotes the application of k times the Newton operator, $N_F^k(\xi_0)$ tends quadratically to a m-tuple of formal power series $\xi_y \in \overline{k}[[y]]^m$ verifying:

- $F(y, \xi_y) = 0$

- $\xi_y(0) = \xi_0$.

where "tends quadratically" means that $F(y, N_F^k(\xi_0)) \in \mathcal{M}^{2^k}$.

Next section gives an idea of how to derive the polynomial q_V of a geometric resolution of V from a geometric resolution of Z:

Idea of the algorithm
We adopt the abusive notation $N_F^\infty(\xi_0) := \xi_y$.

For the rest of the section, let $V = V(f_1, \ldots, f_m) \subset \mathbb{A}^{r+m}$ be an equidimensional variety of dimension r satisfying Assumption 4.1 which is in the hypothesis of Proposition 4.3. We will recover the polynomial q_V of a geometric resolution of V from a geometric resolution of Z associated to a linear form ℓ, lifting the roots $(0, \xi_0) \in Z$ to their corresponding fiber roots $(y, \xi_y) \in V$ (via the inmersion $\overline{k}[[y]] \hookrightarrow \overline{K}$).
Without loss of generality we identify Z with $\{\xi_0 : f_1(0, \xi_0) = \cdots = f_m(0, \xi_0) = 0\} \subset \mathbb{A}^m$.

We know that the total degree of $q_V \in A[t]$ equals D, and we observe that $\ell \in k[x_1, \ldots, x_m]$ is also a separating linear form for V^e.

The information we have is $q_Z(t) = \prod_{\xi_0 \in Z}(t - \ell(\xi_0)) \in k[t]$ and $w := w_Z \in k[t]$ such that for every $\xi_0 \in Z$, $\xi_0 = w(\ell(\xi_0)) = (w_1(\ell(\xi_0)), \ldots, w_1(\ell(\xi_0)))$.

Here is a very informal sketch of how things work:

By Proposition 4.3 we know that for every $\xi_0 \in Z$, $N_F^\infty(\xi_0) = \xi_y \in \overline{k}[[y]]^m$. Thus we are looking for

$$q_V(y, t) = \prod_{(y, \xi_y)}(t - \ell(\xi_y)) = \prod_{(y, \xi_y)}(t - \ell(N_F^\infty(\xi_0))).$$

As we have the a priori bound D for the degree of q_V in the variables y as well, to obtain it *exactly* it is enough to approximate each root ξ_y by a n-tuple of power series up to order D, that is to compute $\lceil \log_2 D \rceil$ iterations of Newton operator on ξ_0 and then to truncate the obtained polynomial at degree D.

Of course we don't know the roots $\xi_0 \in Z$, but we are looking in fact for the characteristic polynomial of the diagonal matrix $\mathrm{Diag}_{\xi_y}(\ell(\xi_y))$, and —as at the end of Section 3— we have the information of all $\xi_0 \in Z$ together via the companion matrix $C = C_{q_Z}$ of q_Z: for $1 \le i \le m$,

$$
\begin{aligned}
w_i(C) &\sim \mathrm{Diag}_{\xi_0 \in Z}((\xi_0)_i) \implies \\
N_F^\infty(w(C)) &\sim \left(\mathrm{Diag}_{\xi_0}((N_F^\infty(\xi_0))_1), \ldots, \mathrm{Diag}_{\xi_0}((N_F^\infty(\xi_0))_m)\right) \\
&\sim \left(\mathrm{Diag}_{\xi_y}((\xi_y)_1), \ldots, \mathrm{Diag}_{\xi_y}((\xi_y)_m)\right) \implies \\
\ell(N_F^\infty(w(C))) &\sim \mathrm{Diag}_{\xi_y}(\ell(\xi_y)),
\end{aligned}
$$

and we should conclude taking its characteristic polynomial which is exactly the polynomial q_V we are looking for.

Again, as we have the a priori bound D for the degree of q_V, it is enough to compute all approximations up to order D and then to truncate the obtained characteristic polynomial at degree D as well.

Let us conclude with a word on the computational aspects:

We set $k := \lceil \log_2 D \rceil$ and we compute formally polynomials $g_1, \ldots, g_m$ and h corresponding to the numerators and a single denominator of the k-th iteration of Newton operator on a m-tuple of indeterminate variables $(x_1, \ldots, x_m)$. We apply them on the matrices $w_1(C), \ldots, w_m(C)$. Using the Cayley-Hamilton theorem we invert the matrix $h(w(C))$ modulo its determinant in $k[y]$, which is invertible as a power series. We approximate the inverse by a formal power series truncated at order D. All remaining computations are truncated at order D. The details of this procedure can be found for instance in [32, Proof of Th. 2], which deals with a generalization of what is presented here.

Generalizations of Newton-Hensel symbolic lifting where the strong hypothesis made here are weakened, allowing multiplicities, are being deeply studied by Grégoire Lecerf ([51, 28, 52, 53] and work in progress).

4.3 Chow forms

For a detailed mathematical account of Chow forms we refer to [60, Sec. I.6.5], [21, Chap. 3], [15], and to [46, Sec. 1.2.2] for the specific normalization introduced here.

Let $V \subset \mathbb{A}^n = \mathbb{A}^{r+m}$ be as before an equidimensional variety of dimension r and degree D satisfying Assumption 4.1 (although unnecessarily heavy, the notation $y = (y_1, \ldots, y_r)$ for the free variables and $x = (x_1, \ldots, x_m)$ for the dependent ones is kept here for the sake of coherence).

Generically a linear variety of codimension $r+1$ does not meet V. Like in the zero-dimensional case, the condition on the coefficients of these linear varieties to meet V is given by a polynomial called a Chow form of V. We formalize that: For $i = 0, \ldots, r$, let $U_i = (U_{i0}, U_{i1}, \ldots, U_{in})$ be a group of

$n + 1$ variables and set $U := (U_0, \ldots, U_r)$, and $L(U_i, (y, x)) := U_{i0} + U_{i1} y_1 + \cdots + U_{in} x_m$ for the associated generic linear form in the variables (y, x).
Define

$$\Phi_V = \{(u_0, \ldots, u_r; \xi), \, \xi \in V, \, L(u_0, \xi) = 0, \ldots, L(u_r, \xi) = 0\} \subset (\mathbb{A}^{n+1})^{r+1} \times \mathbb{A}^n,$$

and denote by $\pi : (\mathbb{A}^{n+1})^{r+1} \times \mathbb{A}^n \to (\mathbb{A}^{n+1})^{r+1}; \, (u, \xi) \mapsto u$ the canonical projection. Then the Zariski closure of the image of Φ_V, $\overline{\pi(\Phi_V)} \subset (\mathbb{A}^{n+1})^{r+1}$, is a closed hypersurface [60, p.66]. We define the *Chow form of* V as any squarefree defining equation $\mathcal{F}_V \in k[U_0, \ldots, U_r]$ of $\overline{\pi(\Phi_V)}$.

The main feature of the Chow form is that for every $u_0, \ldots, u_r \in \mathbb{P}^n$,

$$\mathcal{F}_V(u_0, \ldots, u_r) = 0 \iff \overline{V} \cap \{L^h(u_0, (y, x)) = 0\} \cap \cdots \cap \{L^h(u_r, (y, x)) = 0\} \neq \emptyset.$$

Here $L^h(U_i, (y, x)) = U_{i0} y_0 + U_{i1} y_1 + \cdots + U_{in} x_m$ stands for the homogeneization of L and $\overline{V} \subset \mathbb{P}^n$ for the projective closure of V.

A Chow form $\mathcal{F}_V$ is a multihomogeneous polynomial of degree D in each group of variables U_i ($0 \leq i \leq r$). The projective closure $\overline{V} \subset \mathbb{P}^n$ is uniquely determined by a Chow form of V ([60, p. 66]). Moreover, it is possible to derive equations for the variety $\overline{V}$ from a Chow form of V ([21, Chap. 3, Cor. 2.6]). In case V is irreducible, $\mathcal{F}_V$ is a irreducible polynomial and, in the general case, a Chow form of V of the equidimensional variety V is the product of the Chow forms of its irreducible components.

Observe that the Chow form of an equidimensional variety is uniquely determined up to a scalar factor. Here we follow [46, Sec. 1.2.2] and define *the (normalized) Chow form* $\mathcal{C}h_V$ by fixing the choice of this scalar factor through the condition

$$\mathcal{C}h_V(e_0, \ldots, e_r) = 1,$$

where e_i denotes the $(i + 1)$-vector of the canonical basis of k^{n+1}. That is the coefficient of the monomial $U_{00}^D \cdots U_{rr}^D$ (the fact that this coefficient is not zero follows from Assumption 4.1).

Chow forms → geometric resolutions:
The procedure described in Section 3.1 is generalizable to any dimension:
We define

$$\mathcal{P}(U_0, t, y) := (-1)^{\deg V} \mathcal{C}h_V((U_{00} - t, U_{01}, \ldots, U_{0n}); e_1 - y_1 e_0; \ldots; e_r - y_r e_0)$$

For every $\xi = (y, \xi_y) \in V$, we observe that $\mathcal{P}(U_0, L(U_0, \xi), y_1, \ldots, y_r) = 0$ since

$$V \cap \{L(U_0, (y, x)) = L(U_0, (y, \xi_y))\} \cap \{y_1 = y_1\} \cap \cdots \cap \{y_r = y_r\} \neq \emptyset.$$

Thus $\mathcal{P}(U_0, L(U_0, \xi), y_1, \ldots, y_r)$ vanishes on V^e. Moreover $\deg_t \mathcal{P} = \deg V$ since $\deg_{U_0} \mathcal{C}h_V = \deg V$ and for a generic u_0, $\ell(y, x) := L(u_0, (y, x))$ separates the zeroes of V^e. Finally $\mathcal{P}$ is monic in t since it can be shown that its leading coefficient is independent from y, and $\mathcal{C}h_V(-e_0, e_1, \ldots, e_r) = (-1)^{\deg V}$. Then we conclude as in Section 3.1.

Geometric resolutions → Chow forms

If we proceed exactly as in the pure zero-dimensional case we obtain $\mathcal{C}h_{V^e}(U_0) \in K[U_0]$ in a single set of variables U_0 and with extraneous coefficients depending on the free variables y (cf. the Chow form of [50, Sec. 3.3]).
The first polynomial although probabilistic algorithm to compute the Chow form of an equidimensional variety satisfying Assumption 4.1 from a geometric resolution is given in [37, Prop. 3.5]. It follows from the main technical result Main Lemma 2.3 of that paper that we discuss here in a simplified form:

Proposition 4.4 *Set $A := k[y_1, \ldots, y_r]$ and $A[x] := A[x_1, \ldots, x_m]$. Set $n := r + m$ and let $V \subset \mathbb{A}^n$ be an equidimensional variety of dimension r defined by a reduced regular sequence $f_1, \ldots, f_m \subset A[x]$. Assume moreover that V satisfies Assumption 4.1. Suppose that a geometric resolution (q, w) of $Z = V \cap \{y_1 = 0, \ldots, y_r = 0\}$ associated to a linear form ℓ is given, and that $f_1, \ldots, f_m$ are polynomials of degrees bounded by d encoded by slp's of length L.*

Then there is a deterministic algorithm which computes (a slp for) the Chow form Ch_V within complexity $(ndD)^{\mathcal{O}(1)}L$.

Idea of the proof.–

The computation of the Chow form relies on a way of writing it as a quotient of products of Chow forms of zero-dimensional varieties with respect to different base fields [37, Prop. 2.5]:

$$Ch_V(U_0, \ldots, U_r) = \frac{\prod_{i=0}^r Ch_{Z_i}(U_i)}{\prod_{i=1}^r Ch_{Z_i}(e_i)}, \tag{4}$$

where $Z_0, \ldots, Z_r$ denote the zero-dimensional varieties of degree D defined as

$$
\begin{aligned}
Z_0 &:= Z = V(y_1, \ldots, y_r, f_1, \ldots, f_m) \subset \mathbb{A}^n(\overline{k}) \\
Z_1 &:= V(L(U_0, (y,x)), y_2, \ldots, y_r, f_1, \ldots, f_m) \subset \mathbb{A}^n(\overline{k(U_0)}) \\
&\quad\vdots \\
Z_r &:= V(L(U_0, (y,x)), \ldots, L(U_{r-1}, (y,x)), f_1, \ldots, f_m) \subset \mathbb{A}^n(\overline{k(U_0, \ldots, U_{r-1})})
\end{aligned}
$$

and $Ch_{Z_i}(e_i)$ consists on specializing the group of variables U_i on the $(i+1)$-vector of the canonical basis of k^{n+1} (which corresponds to the hyperplane y_i).

Now fix $0 \le i \le r$. Remember that as Z_i is zero-dimensional, $Ch_{Z_i} = \prod_{\xi_U \in Z_i} L(U_i, \xi_U)$.

It can be shown that for each $(0, \xi_0) \in Z$, Proposition 4.3 centered at $(e_1, \ldots, e_i)$ holds and gives back from ξ_0 (an approximation of) the unique $\xi_U \in \overline{k}[[U_0 - e_1, \ldots, U_{i-1} - e_i]]^m$ such that $\xi_U \in Z_i$ and $\xi_U(e_1, \ldots, e_i) = \xi_0$.

Then we proceed as in Section 4.2 (Idea of the algorithm) to recover Ch_{Z_i} which is the determinant of the diagonal matrix $\mathrm{Diag}_{\xi_U \in Z_i}\big(L(U_i, \xi_U)\big)$ from the companion matrix C_q of q which is similar to $\mathrm{Diag}_{\xi_0 \in Z}\big(\ell(\xi_0)\big)$.

A final comment concerning the algorithm: in order to avoid divisions in the computation of the polynomial Ch_V, we need to invert the denominator in the right hand side of Identity 4 and replace it by a formal power series. However as it is not directly invertible we need to compute its order and its graded component of lowest degree. This information also decides up to which order the approximations of the numerator and the denominator have to be computed. This is done in [37, Lem. 2.10].

Similar lifting ideas could seem to lead to a simpler algorithm to compute the Chow form of the variety: the Chow form can be written as the numerator of the independent term of a certain characteristic polynomial, which can be approximated from a good fiber using Newton method. However it is important to observe that up to now an algorithm that approximates the power series corresponding to a quotient does not yield an approximation of the numerator. That is the reason why the product formula above is so useful.

5 Arbitrary varieties

In this section $V \subset \mathbb{A}^n$ is an arbitrary variety. Thus V can be decomposed in the following manner:

$$V = V_0 \cup \cdots \cup V_n$$

where for $0 \le r \le n$, V_r is either empty or an equidimensional variety of dimension r. The degree D of V is defined, following [31], as the sum of the degrees of its irreducible, or equivalently equidimensional, components.

We suppose that V is described as the zero set of $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ of degrees bounded by d and described by slp's of size bounded by L. In this section we deal with the question of producing an algorithm which determines (slp's for) the equidimensional components of V. These can be described by means of equations, or of geometric resolutions, or by their Chow forms.

Set theoretic descriptions of the equidimensional components can be found for instance in [14, 22] where the algorithms are for dense input representation and deterministic, with complexity of order $(sd^{n^2})^{\mathcal{O}(1)}$, or in [38, 39] for a probabilistic algorithm for slp input representation of complexity $(sd^n)^{\mathcal{O}(1)} L$. Geometric resolution algorithms and similar ones are given in [17] for the classic point of view and in [50, 51] for evaluation methods.

The evaluation methods algorithms have all more or less the same recursive structure, as in the zero-dimensional case. First they need a preparation of the input as described in Section 1.5 or similar in order to produce a good linear algebra underlying structure. Then the algorithms adds one equation at the time, computing at each level in the same manner equations for what they want modulo some extraneous factors (a consequence of the input preparation) that need to be cleaned at some point. Here we describe roughly the algorithm of [37] which computes probabilistically (a slp for) a Chow form of each equidimensional component of V.

Idea of the algorithm

The algorithm relies on three major ingredients:

- *Ingredient 1*: the generalization of Proposition 4.4 presented in [37, Main Lemma 2.3], where instead of being given a reduced regular sequence $f_1, \ldots, f_m$ we assume the weaker condition that $f_1, \ldots, f_m \in I(V)$ and that for every $\xi_0 \in Z$, the localized ideals $I(V)_{\xi_0}$ and $(f_1, \ldots, f_m)_{\xi_0}$ coincide.

- *Ingredient 2*: a bounded probability algorithm which given a Chow form of V and a polynomial f which is not a zero-divisor modulo $I(V)$ returns a Chow form of $V \cap V(f)$ [37, Lem. 3.8].

- *Ingredient 3*: a bounded probability algorithm which given a Chow form of an equidimensional variety with some components contained in a given hypersurface returns separated Chow forms for both parts [37, Lem. 3.9].

Let $V = V_0 \cup \cdots \cup V_n$ be the variety defined by the input polynomials. If $V \neq \mathbb{A}^n$, the input preparation (Section 1.5) enables us to assume that

$$V(f_1) = V_{n-1} \cup V'_{n-1} \quad , \quad V(f_1, f_2) = (V_{n-2} \cup V_{n-1}) \cup V'_{n-2}$$

where the varieties V'_{n-1}, V'_{n-2} are equidimensional varieties of codimension 1 and 2 respectively containing all other components of V, and that f_1 satisfies the hypothesis of Ingredient 1 for V'_{n-1}. Also $V'_{n-1} \cap V(f_2) = (V_{n-2} \cup \tilde{V}_{n-2}) \cup V'_{n-2}$ where $\tilde{V}_{n-2}$ is the remaining equidimensional part of codimension 2 included in V_{n-1}.

The input of the first step is $\mathcal{C}h_{V(f_1)} = \mathcal{C}h_{V_{n-1} \cup V'_{n-1}}$ from which we compute $\mathcal{C}h_{V_{n-1}}$ and $\mathcal{C}h_{V'_{n-1}}$ by Ingredient 3 since $V_{n-1} \subset V(f_2)$ and no component of V'_{n-1} does.

The latter should be the input of next step: from the Chow form of V'_{n-1} one can compute, by Ingredient 2, the Chow form of $V'_{n-1} \cap V(f_2) = (V_{n-2} \cup \tilde{V}_{n-2}) \cup V'_{n-2}$ and then apply again Ingredient 3 to separate the Chow form of $V_{n-2} \cup \tilde{V}_{n-2}$ from that of V'_{n-2} (the Chow form of $V_{n-2} \cup \tilde{V}_{n-2}$ will be broken up in its two parts at the end by another application of Ingredient 3). However the complexity considerations introduced after Theorem 3.1 prevent that since the complexity would explode due to the recursion.

What we do is to compress the information of V'_{n-1}: from its Chow form we obtain probabilistically a geometric resolution of the zero-dimensional variety $Z_{n-1} = V'_{n-1} \cap V(x_1, \ldots, x_{n-1})$ associated to a certain linear form, and these arrays of coefficients will be the input of next step together with f_1.

The second step begins computing *again* $\mathcal{C}h_{V'_{n-1}}$ from the geometric resolution of Z_{n-1} and f_1 by application of Ingredient 1. Then it follows as explained in the previous paragraph computing

the Chow forms of $V_{n-2} \cup \tilde{V}_{n-2}$ and of V'_{n-2}, and again keep aside the former and compress the information of the latter replacing it by a geometric resolution of $Z_{n-2} = V'_{n-2} \cap V(x_1, \ldots, x_{n-2})$.

All steps follow now the same pattern. At the end of this part of the algorithm one obtains a list of Chow forms of V_{n-1}, $V_{n-2} \cup \tilde{V}_{n-2}, \ldots, V_0 \cup \tilde{V}_0$ where $\tilde{V}_r$ is either empty or an equidimensional variety of dimension r included in $V_{r+1} \cup \cdots \cup V_{n-1}$ while no irreducible component of V_r is. The algorithm concludes extracting from these Chow forms the Chow forms of $V_{n-2}, \ldots, V_0$ by application of Ingredient 3.

The final result is in a simplified form:

Theorem 5.1 *[37, Th. 1] Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ be polynomials of degree bounded by d encoded by straight-line programs of length bounded by L. Set $V := V(f_1, \ldots, f_s) \subset \mathbb{A}^n$ and let $V = V_0 \cup \cdots \cup V_n$ be its minimal equidimensional decomposition. Set δ for a geometric degree of the input polynomial system.*
Then there is a bounded probability algorithm which computes (slp's for) Chow forms of $V_0, \ldots, V_n$ within (expected) complexity $s(n\,d\,\delta)^{\mathcal{O}(1)}L$. Its worst case complexity is $s(n\,d^n)^{\mathcal{O}(1)}L$.

An analogous result for the description of the equidimensional components of V by means of geometric resolutions is obtained in [50].

6 Applications

6.1 The computation of the sparse resultant

We take this application concerning the computation of a class of sparse resultants from [37].

The classical resultant $\mathrm{Res}_{n,d}$ of a system of $n+1$ generic homogeneous polynomials $f_0, \ldots, f_n$ of degree d in $n+1$ variables is a polynomial in the indeterminate coefficients $U_i = (U_{i\alpha}, \alpha), 0 \leq i \leq n$, of the polynomials f_i, that characterizes for which coefficients the system has a non-trivial solution. This polynomial is homogeneous of degree d^n in each set of indeterminate coefficients (U_i). Clearly the number of variables and the degree bound make it prohibitively expensive to write (the dense encoding of) this polynomial, unless very specific cases like the resultant of two homogeneous polynomials in two variables. However a direct application of the computation of the Chow form, more precisely of Proposition 4.4 above, shows that a straight-line program for $\mathrm{Res}_{n,d}$ can be deterministically computed within complexity $(nd^n)^{\mathcal{O}(1)}$. This can be extended to compute some classes of sparse resultants.

The sparse resultant is the basic object in sparse elimination theory and has been used extensively as a tool for the resolution of polynomial equation systems (see for instance [65], [57], [18]). Several effective procedures were proposed to compute it (see e.g. [65], [10], [11]). Recently, C. D'Andrea has obtained an explicit determinantal formula which extends Macaulay's formula to the sparse case ([16]).

From the algorithmic point of view, the main assumption of sparse elimination theory is that computations should be substantially faster when the input polynomials are sparse (in the sense that their Newton polytopes are restricted). Basically, the parameters which control the sparsity are the number of variables n and the normalized volume $\mathrm{Vol}(\mathcal{A})$ of the convex hull of the set $\mathcal{A}$ of exponents (that is $n!$ times its volume with respect to the Euclidean volume form of $\mathbb{R}^n$). None of the previous algorithms computing sparse resultants is completely satisfactory, as their predicted complexity is exponential in all or some of these parameters (see [11, Cor. 12.8]).

The precise definition of the (unmixed) sparse resultant is as follows:
Let $\mathcal{A} = \{\alpha_0, \ldots, \alpha_N\} \subset \mathbb{Z}^n$ be a finite set of integer vectors. We assume here that $\mathbb{Z}^n$ is generated by the differences of elements in $\mathcal{A}$. For $i = 0, \ldots, n$, let U_i be a group of variables indexed by the elements of $\mathcal{A}$, and set

$$f_i := \sum_{\alpha \in \mathcal{A}} U_{i\alpha}\, x^\alpha \ \in k[U_i][x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$$

23

for the generic Laurent polynomial with support equal to $\mathcal{A}$. Let $W_{\mathcal{A}} \subset (\mathbb{P}^N)^{n+1} \times (\overline{k}^*)^n$ be the incidence variety of $f_0, \ldots, f_n$ in $(\overline{k}^*)^n$, that is

$$W_{\mathcal{A}} = \{(\nu_0, \ldots, \nu_n; \xi); \ \ F_i(\nu_i, \xi) = 0 \ \ \forall 0 \leq i \leq n\},$$

and let $\pi : (\mathbb{P}^N)^{n+1} \times (\overline{k}^*)^n \to (\mathbb{P}^N)^{n+1}$ be the canonical projection. The variety $\overline{\pi(W_{\mathcal{A}})}$ happens to be an irreducible variety of codimension 1 (see [21, Chapter 8, Prop.-Defn. 1.1]), and the sparse $\mathcal{A}$-resultant $\mathrm{Res}_{\mathcal{A}}$ is defined as the unique —up to a sign— irreducible polynomial in $\mathbb{Z}[U_0, \ldots, U_n]$ which defines it. It is a multihomogeneous polynomial of degree $\mathrm{Vol}(\mathcal{A})$ in each group of variables U_i.

As this resultant coincides with the Chow form of the toric variety associated to the input set $\mathcal{A}$, the result one can obtain is the following:

Proposition 6.1 *([37, Cor. 4.2] Let $\mathcal{A} \subset (\mathbb{N}_0)^n$ be a finite set which contains $\{0, e_1, \ldots, e_n\}$. Then there is a bounded probability algorithm which computes (a slp for) a scalar multiple of the $\mathcal{A}$-resultant $\mathrm{Res}_{\mathcal{A}}$ with (expected) complexity $(n \mathrm{Vol}(\mathcal{A}))^{\mathcal{O}(1)}$. Its worst case complexity is $(nd^n)^{\mathcal{O}(1)}$, where $d := \max\{|\alpha|\, ; \, \alpha \in \mathcal{A}\}$.*

In fact, this expected polynomial behavior of the complexity is out of reach of the known and usual matrix formulations, as in all of them the involved matrices have an exponential size.
As an example, the $\mathcal{A}$-resultant $\mathrm{Res}_{\mathcal{A}}$ for

$$\mathcal{A} := \mathcal{A}(n, d) = \{0, e_1, \ldots, e_n, e_1 + \cdots + e_n, 2e_1 + \cdots + 2e_n, \ldots, de_1 + \cdots + de_n\}$$

can be computed with (expected) complexity $(nd)^{\mathcal{O}(1)}$ since $\mathrm{Vol}(\mathcal{A}) = nd$.

It would be desirable to extend this result in order to compute general mixed resultants.

6.2 The computation of the ideal of a variety

We take this application from [4]. It is a well-known fact that unless for very particular situations there is not yet a good complexity algorithm to compute generators for the ideal of a variety from a set theoretic description of the variety, that is to compute generators of the radical of an ideal from generators of the ideal. Most of the known algorithms rely on Gröbner basis computations, whose worst-case complexity is doubly exponential in the number of variables or at least in the dimension of the variety. The result here is the following:

Theorem 6.2 *[4, Th. 17] Let $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ be polynomials of degree bounded by d which define a smooth irreducible variety $V \subset \mathbb{A}^n$ of dimension r.*
Then there is a bounded probability algorithm which computes (slp's for) a set of $(n - r)(r + 1)$ generators for $I(V)$, of degree bounded by $\deg V$ and within complexity $s(nd^n)^{\mathcal{O}(1)}$.

To give a rough idea of the algorithm we recall the notion of characteristic polynomial of an equidimensional, in our case moreover irreducible, variety $V \subset \mathbb{A}^n$ of dimension r and degree D:
Let as usual $U_0, \ldots, U_r$ be $r + 1$ groups of $n + 1$ variables $U_i := (U_{ij})_{0 \leq j \leq n}$, and $L(U_i, x) := U_{i0} + U_{i1}x_1 + \cdots + U_{in}x_n$. Also let $(t_0, \ldots, t_r)$ be a group of $r + 1$ single variables. A *characteristic polynomial* $\mathcal{P}_V \in k[U_0, \ldots, U_r][t_0, \ldots, t_r]$ of V is defined as any defining equation of the Zariski closure of the image of the map

$$\varphi_V : \mathbb{A}^{(r+1)(n+1)} \times V \to \mathbb{A}^{(r+1)(n+1)} \times \mathbb{A}^{r+1}, \quad (u_0, \ldots, u_r; \xi) \mapsto (u_0, \ldots, u_r; \, L(u_0, \xi), \ldots, \, L(u_r, \xi))$$

which is a hypersurface. This is a multihomogeneous polynomial of degree D in each group of variables $U_i \cup \{t_i\}$. Its degree in the group of variables $(t_0, \ldots, t_r)$ is also bounded by D.
By a result of [13], the ideal $I(V)$ of the smooth irreducible variety V is generated by the set of polynomials (of degree D) $\mathcal{P}_V(u, L(u_1, x), \ldots, L(u_r, x))$ for $u := (u_0, \ldots, u_r) \in \mathbb{A}^{(r+1)(n+1)}$. Moreover as $I(V)$ is locally a complete intersection (generated thus by $n - r$ polynomials), one can show that $I(V)$ can globally be generated by $(n - r)(r + 1)$ of these polynomials.

The algorithmic aspects of this construction rely on the fact that the characteristic polynomial can be derived from the Chow form by a simple composition of variables ([46, Lem. 2.13]), and on a careful choice of the localizations in order to recover a global description with bounded probability.

References

[1] C. A. BERENSTEIN, A. YGER, *Effective Bézout identities in* $\mathbb{Q}[x_1, \ldots, x_n]$, Acta Math. **166** (1991) 69–120.

[2] C. A. BERENSTEIN, A. YGER, *Residue calculus and effective Nullstellensatz,* Amer. J. Math. **121** (1999) 723–796.

[3] S.J. BERKOWITZ, *On computing the determinant in small parallel time using a small number of processors,* Inform. Process. Lett. **18** (1984) 147-150.

[4] C. BLANCO, G. JERONIMO, P. SOLERNÓ, *Computing generators of the ideal of a smooth algebraic variety,* In preparation, University of Buenos Aires (2002).

[5] L. BLUM, F. CUCKER, M. SHUB, S. SMALE, *Complexity and real computation,* Springer (1998).

[6] J.-B. BOST, H. GILLET, C. SOULE, *Height of projective varieties and positive Green forms,* J. Amer. Math. Soc. **7** (1994) 903–1027.

[7] W. D. BROWNAWELL, *Bounds for the degrees in the Nullstellensatz,* Ann. of Math. **126** (1987) 577–591.

[8] P. BÜRGISSER, M. CLAUSEN, M.A. SHOKROLLAHI, *Algebraic complexity theory,* Springer (1997).

[9] L. CANIGLIA, A. GALLIGO, J. HEINTZ, *Borne simplemente exponentielle pour les degrés dans le théorème des zéros sur un corps de charactéristique quelconte,* C. R. Acad. Sci. Paris **307** (1988) 255–258.

[10] J.F. CANNY, I.Z. EMIRIS, *An efficient algorithm for the sparse mixed resultant,* Lect. Notes Comput. Sci. **263** (1993) 89-104.

[11] J.F. CANNY, I.Z. EMIRIS, *A subdivision-based algorithm for the sparse resultant,* J. ACM **47** (2000) 417-451.

[12] D. CASTRO, M. GIUSTI, J. HEINTZ, G. MATERA, L. M. PARDO, *The hardness of polynomial equation solving ,* to appear in Foundations of Computational Mathematics (2002).

[13] F. CATANESE, *Chow varieties, Hilbert schemes and moduli spaces of surfaces of general type,* J. Alg. Geometry **1** (1992) 561-595.

[14] A.L. CHISTOV, D.Y. GRIGORIEV, *Subexponential time solving systems of algebraic equations.* LOMI preprint E-9-83, E-10-83, Steklov Institute, Leningrad, 1983.

[15] J. DALBEC, B. STURMFELS, *Introduction to Chow forms,* Invariant methods in discrete and computational geometry (Curaçao, 1994), Kluwer (1995) 37-58.

[16] C. D'ANDREA, *Macaulay's style formulas for sparse resultants,* E-print: `math.AG/0107181`.

[17] M. ELKADI, B. MOURRAIN, *A new algorithm for the geometric decomposition of a variety,* Proc. ISSAC'1999 (ACM) (1999), 9-16.

[18] M. ELKADI, B. MOURRAIN, *Matrices in elimination theory,* J. Symb. Comput. **28** (1999), 3-44.

[19] N. FITCHAS, A. GALLIGO, *Nullstellensatz effectif et conjecture de Serre (théorème de Quillen–Suslin) pour le Calcul Formel,* Math. Nachr. **149** (1990) 231-253.

[20] N. FITCHAS, M. GIUSTI, F. SMIETANSKI, *Sur la complexité du théorème des zéros,* in J. Gudat et. al., eds., Approximation and optimization **8**, Peter Lange Verlag (1995) 247-329.

[21] I.M. GELFAND, M.M. KAPRANOV, A.V. ZELEVINSKY, *Discriminants, resultants, and multidimensional determinants,* Birkhäuser (1994).

[22] M. GIUSTI, J. HEINTZ, *Algorithmes —disons rapides— pour la décomposition d'une varieté algébrique en composantes irréductibles et équidimensionelles,* Progress in Math. **94**, Birkhäuser (1991) 164-194.

[23] M. GIUSTI, J. HEINTZ, *Kronecker's smart, little black-boxes,* Proceedings of Foundations of Computational Mathematics, Oxford 1999 (FoCM'99), A. Iserles and R. DeVore, eds., Cambridge University Press **284** (2001) 69-104.

[24] M. GIUSTI, J. HEINTZ, K. HÄGELE, J.E. MORAIS, L.M. PARDO, J.L. MONTAÑA, *Lower bounds for Diophantine approximations,* J. Pure Appl. Algebra **117 & 118** (1997) 277-317.

[25] M. GIUSTI, J. HEINTZ, J.E. MORAIS, J. MORGENSTERN, L.M. PARDO *Straight-line programs in geometric elimination theory,* J. Pure Appl. Algebra **124** (1998) 101-146.

[26] M. GIUSTI, J. HEINTZ, J.E. MORAIS, L.M. PARDO, *When polynomial equation systems can be solved fast?,* Proc. 11th. International Symposium Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-11, Paris 1995, G. Cohen, M. Giusti and T. Mora, eds., Lecture Notes in Comput. Sci. **948** (1995) 205-231.

[27] M. GIUSTI, J. HEINTZ, J. SABIA, *On the efficiency of effective Nullstellensätze,* Comput. Complexity **3** (1993) 56-95.

[28] M. GIUSTI, G. LECERF, B. SALVY, *A Gröbner free alternative for polynomial system solving,* J. Complexity **17** (2001) 154-211.

[29] K. HÄGELE, *Intrinsic height estimates for the Nullstellensatz,* Ph.D. dissertation, Univ. Cantabria (1998).

[30] K. HÄGELE, J. E. MORAIS, L. M. PARDO, M. SOMBRA, *On the intrinsic complexity of the arithmetic Nullstellensatz,* J. Pure Appl. Algebra **146** (2000) 1083-183.

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

[32] J. HEINTZ, T. KRICK, S. PUDDU, J. SABIA, A. WAISSBEIN, *Deformation techniques for efficient polynomial equation solving,* J. Complexity **16** (2000) 70-109.

[33] J. HEINTZ, G. MATERA, A. WAISSBEIN, *On the time-space complexity of geometric elimination procedures,* Applicable Algebra in Engineering, Communication and Computing 11(4) (2001) 239-296.

[34] J. HEINTZ, C. P. SCHNORR, *Testing polynomials which are easy to compute,* Proc. 812h Annual ACM Symp. on Computing (1980) 262-268. Also in Logic and Algorithmic. An International Symposium held in honour of Ernst Specker, Monographie No. **30** de l'Enseignement de Mathématiques, Genève (1982) 237-254.

[35] J. HEINTZ, M. SIEVEKING, *Absolute primality of polynomials is decidable in random polynomial time in the number of the variables,* 8th International Colloquium on Automata, Languages and Programming ICALP 81, Springer LN Comput. Sci. **115** (1981) 16-28.

[36] G. HERMANN, *Der Frage der endlich vielen Schritte in der Theorie der Polynomideale,* Math. Ann. **95** (1926) 736-788.

[37] G. JERONIMO, T. KRICK, J. SABIA, M. SOMBRA, *The computational complexity of the Chow form,* Preprint University of Buenos Aires, University of La Plata and University of Paris 7 (2002).

[38] G. JERONIMO, J. SABIA, *Probabilistic equidimensional decomposition,* C. R. Acad. Sci. Paris **331** (2000) 485-490.

[39] G. JERONIMO, J. SABIA, *Effective equidimensional decomposition of affine varieties,* J. Pure Appl. Algebra **169** (2002) 229-248.

[40] E. Kaltofen, *Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization,* SIAM J. Comput., 14(2) (1985) 469-489.

[41] E. Kaltofen, *Greatest common divisors of polynomials given by straight-line programs,* J. ACM **35**, N° 1 (1988) 234-264.

[42] E. Kaltofen, *Factorization of polynomials given by straight-line programs,* Randomness in Computation, Advances in Computing Research **5**, S. Micali, ed., JAI Press Inc., CT. (1989) 375-412.

[43] J. Kollár, *Sharp effective Nullstellensatz,* J. Amer. Math. Soc. **1** (1988) 963-975.

[44] T. Krick, L. M. Pardo, *Une approche informatique pour l'approximation diophantienne,* C. R. Acad. Sci. Paris **318** (1994) 407-412.

[45] T. Krick, L.M. Pardo, *A computational method for Diophantine approximation,* Progress in Math. **143**, Birkhäuser (1996) 193-253.

[46] T. Krick, L.M. Pardo, M. Sombra, *Sharp estimates for the arithmetic Nullstellensatz,* Duke Math. J. **109**, No. 3 (2001) 521-598.

[47] T. Krick, J. Sabia, P. Solernó, *On intrinsic bounds in the Nullstellensatz,* AAECC J. **8** (1997) 125-134.

[48] E. Kunz, *Kähler differentials,* Adv. Lect. in Math., Vieweg–Verlag (1986).

[49] G. Lecerf, *Kronecker 0.16beta-2, April 2000,* `http://kronecker.medicis.polytechnique.fr/`.

[50] G. Lecerf, *Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions,* Proc. ISSAC'2000 (ACM) (2000).

[51] G. Lecerf, *Une alternative aux méthodes de réécriture pour la résolution des systèmes algébriques,* PhD Thesis, Ecole Polytechnique (2001).

[52] G. Lecerf, *Quadratic Newton iteration for systems with multiplicity,* Journal of FoCM, 2(3) (2002) 247-293.

[53] G. Lecerf, *Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers,* Preprint Universit de Versailles St-Quentin-en-Yvelines, (2002).

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

[55] P. Philippon, *Dénominateurs dans le théorème des zeros de Hilbert,* Acta Arith. **58** (1990) 1-25.

[56] P. Philippon, *Sur des hauteurs alternatives, I,* Math. Ann. **289** (1991), 255-283; *II,* Ann. Inst. Fourier **44** (1994) 1043-1065; *III,* J. Math. Pures Appl. **74** (1995) 345-365.

[57] M. Rojas, *Toric laminations, sparse generalizd characteristic polynomials, and a refinement of Hilbert's tenth problem,* Proc. FoCM'97, Springer-Verlag (1997) 369-381.

[58] J. Sabia, P. Solernó, *Bounds for traces in complete intersections and degrees in the Nullstellensatz,* AAECC J. **6** (1995) 353-376.

[59] J.T. Schwartz, *Fast probabilistic algorithms for verification of polynomial identities,* J. ACM, **27** (1980) 701-717.

[60] I. Shafarevich, *Basic algebraic geometry,* Springer-Verlag (1972).

[61] M. Sombra, *Bounds for the Hilbert function of polynomial ideals and for the degrees in the Nullstellensatz,* J. Pure Appl. Algebra **117 & 118** (1997) 565-599.

[62] M. Sombra, *A sparse effective Nullstellensatz,* Adv. Appl. Math. **22** (1999) 271-295.

[63] M. Sombra, *Minima successifs de variétés toriques projectives,* Preprint Univ. Paris 7 (2002).

[64] V. STRASSEN, *Vermeidung von Divisionen,* J. Reine Angew. Math. **264** (1973) 182-202.

[65] B. STURMFELS, *Sparse elimination theory,* in D. Eisenbud and L. Robbiano, eds., Computational algebraic geometry and commutative algebra, Cambridge Univ. Press (1993) 377-396.

[66] W. TRINKS, *On improving approximate results of Buchberger's algorithm by Newton's method,* L. N. Comput. Sci. **204**, Springer-Verlag (1985) 608-611.

[67] F. WINKLER, *A p-adic approach to the computation of Gröbner bases,* J. Symb. Comput. **6** (1988) 287-304.

[68] R. ZIPPEL, *Probabilistic algorithms for sparse polynomials,* Proceedings EUROSAM'79, Lecture Notes in Comput. Sci. **72**, Springer (1979) 216-226.