

**EVALUATION TECHNIQUES FOR ZERO-DIMENSIONAL
PRIMARY DECOMPOSITION**
EXTENDED ABSTRACT

CLÉMENTINE DURVYÉ

ABSTRACT. In this talk, we will present an algorithm that computes the local algebra of the roots of a zero-dimensional polynomial equations system, whose cost is polynomial in the number of variables, in the evaluation cost of the equations and in the Bézout number of the input system.

Let K be a field of characteristic zero, and let f_1, \dots, f_s, g be polynomials in $K[x_1, \dots, x_n]$ such that the system $f_1 = \dots = f_s = 0$ with $g \neq 0$ has a finite set of solutions over the algebraic closure \bar{K} of K . We give an algorithm that computes the roots of the system together with the structure of their multiplicities. More precisely, our purpose is to compute the primary decomposition of the zero-dimensional ideal $(f_1, \dots, f_s) : g^\infty$, where for any ideal \mathcal{J} in $K[x_1, \dots, x_n]$, $\mathcal{J} : g^\infty$ denotes the saturation of \mathcal{J} with respect to g , that is, the ideal $\{f \mid \exists m \geq 0, g^m f \in \mathcal{J}\}$.

Main Result. For any root $p = (p_1, \dots, p_n) \in \bar{K}^n$ of $(f_1, \dots, f_s) : g^\infty$, let $\bar{K}[[x_1 - p_1, \dots, x_n - p_n]]$ denote the ring of formal series in $x_1 - p_1, \dots, x_n - p_n$ over the algebraic closure \bar{K} of K . The *local algebra of p as a root of $(f_1, \dots, f_s) : g^\infty$* is the \bar{K} -algebra

$$\mathbb{D}_p = \bar{K}[[x_1 - p_1, \dots, x_n - p_n]] / ((f_1, \dots, f_s) : g^\infty)_p,$$

where for any ideal \mathcal{J} in $K[x_1, \dots, x_n]$, the notation \mathcal{J}_p stands for the ideal \mathcal{J} extended to $\bar{K}[[x_1 - p_1, \dots, x_n - p_n]]$. The *multiplicity* μ_p of the root p is the dimension of the \bar{K} -algebra \mathbb{D}_p . The matrices of the morphism of multiplication by the variables in some basis of \mathbb{D}_p allow all computations in \mathbb{D}_p . Here we propose a new algorithm for computing such matrices. The improvement of the exponents involved in the complexity is still in progress.

Theorem 1 ([2]). *Let K be a field of characteristic zero and let f_1, \dots, f_s, g be polynomials in $K[x_1, \dots, x_n]$ of degree at most d , given by straight-line programs of size at most L . Let us assume that the system $f_1 = \dots = f_s$ with $g \neq 0$ has only a finite set of solutions over the algebraic closure \bar{K} of K . The roots of the system together with the matrices of multiplication by the variables with respect to a basis of their local algebra can be computed with a number of arithmetic operations in K which is polynomial in n , L and d^n . We give a probabilistic algorithm performing these computations. Its probability of returning the correct result relies on choices of elements in K . Choices for which the result is not correct are enclosed in strict algebraic subsets.*

Related Works. By now, there are several known algorithms for computing the primary decomposition of an ideal; a detailed bibliography will be available in the full text [2]. Most of these algorithms use Gröbner or standard bases (see [7, Chapter 4]), reducing the general problem to primary decomposition of zero-dimensional ideals. In all these algorithms, polynomials are represented by vectors of their

coefficients in the canonical monomial basis, and a primary decomposition $\mathcal{I} = \mathcal{Q}_1 \cap \dots \cap \mathcal{Q}_s$ of an ideal \mathcal{I} is given by a set of generators of \mathcal{Q}_j for each $j \in \{1, \dots, s\}$.

Instead of expanding a polynomial in the monomial basis, alternative suitable data structures can be used in order to represent it as the function that computes its values at any given points. We often refer to these methods as *evaluation techniques*. We recall the algorithm of [12], and the similar ideas of [1], that already take advantage of the evaluation property of the input system. Given a system $f_1 = \dots = f_s = 0$ together with an isolated root p , the algorithm of [12] computes the matrices of multiplication by the variables in the local algebra \mathbb{D}_p by the use of duality between polynomials and formal series in differential operators. But these algorithms remains related to the latter approach since their cost still depends on the number of monomials obtained by derivation of the monomials of f_1, \dots, f_s .

We propose here an algorithm for the primary decomposition of a zero-dimensional ideal by evaluation techniques, that does not involve the monomials appearing in the equations anymore. This algorithm relies on the computation of Hermite and Smith forms of matrices with entries in the formal series ring $K[[x_1]]$.

In a first section, we explain quickly how we reduce our problem to the computation of the local algebra at the origin of the intersection of a reduced curve and an hypersurface. Then, we introduce a localized module of the previous curve, and we give an algorithm for computing a basis of this module. Finally, we explain how the end of the algorithm boils down to a Smith form computation.

1. REDUCING THE PROBLEM: THE KRONECKER SOLVER

Even if it means replacing f_1, \dots, f_s with linear combinations of f_1, \dots, f_s , we can assume that for $i \in \{1, \dots, n-1\}$, the ideal $(f_1, \dots, f_i) : g^\infty$ is radical and f_{i+1} is a non zero divisor in $K[x_1, \dots, x_n]/(f_1, \dots, f_i) : g^\infty$ (see [9, Section 6], [8, Section 3.5] or [11, Lemmas 1 and 2]). In particular, these assumptions imply that $\mathcal{I} = (f_1, \dots, f_{n-1}) : g^\infty$ is an unmixed radical one dimensional ideal. From now on, we let f denote the polynomial f_n . Since f is a non zero divisor in $K[x_1, \dots, x_n]/\mathcal{I}$, the ideal $\mathcal{I} + (f)$ is zero dimensional. Let p be a root of $(\mathcal{I} + (f)) : g^\infty$. The local algebra of p as a root of $(\mathcal{I} + (f)) : g^\infty$ is exactly the one of p as a root of $\mathcal{I} + (f)$. Now, if $s > n$, we can also assume that $s = n + 1$ without loss of generality; if the matrices of multiplication by x_1, \dots, x_n in the latter algebra are known, we easily deduce those in \mathbb{D}_p by linear algebra computations in the algebraic extension $K(p) = K(p_1, \dots, p_n)$ of K . Afterwards, we assume that $s = n$.

After an affine change of variables, the following statements hold with a high probability (see for instance [8] or [3][Proposition 4.3]):

- the ideal \mathcal{I} is in *general Noether position*, that is, $\mathcal{I} \cap K[x_1] = (0)$ and x_2, \dots, x_n are generally integral over $K[x_1]$ modulo \mathcal{I} , that is for $i \in \{2, \dots, n\}$, there exists $q_i \in K[x_1, x_i] \cap \mathcal{I}$ such that the degree of q_i is equal to its degree in x_i ;
- x_2 is *primitive for \mathcal{I}* , that is, the powers of x_2 generate the $K(x_1)$ -vector space $K(x_1)[x_2, \dots, x_n]/\mathcal{I}'$, where \mathcal{I}' stands for the ideal \mathcal{I} extended to $K(x_1)[x_2, \dots, x_n]$;
- x_1 *separates the roots of $\mathcal{I} + (f)$* , that is, if $p = (p_1, \dots, p_n)$ and $p' = (p'_1, \dots, p'_n)$ are two distinct roots of $\mathcal{I} + (f)$ in \bar{K}^n , then $p_1 \neq p'_1$.

Under these assumptions, it can be proved that there exists a unique sequence of polynomials $q, w_3, \dots, w_n \in K[x_1, x_2]$ such that q is monic in x_2 , that for all $j \in \{3, \dots, n\}$, $\deg_{x_2}(w_j) < \deg_{x_2}(q)$ and that $\mathcal{I}' = (q, (\partial q / \partial x_2)x_3 - w_3, \dots, (\partial q / \partial x_2)x_n - w_n)$. The sequence q, w_3, \dots, w_n is called a *Kronecker representation of \mathcal{I}* (see [6]

or [3, Section 3] for further details). Let us recall from [3, Corollary 3.4] the only properties of the Kronecker representation that will be used afterwards:

$$\mathcal{I} \cap K[x_1, x_2] = (q) \text{ and } \forall j \in \{3, \dots, n\}, \frac{\partial q}{\partial x_2} x_j - w_j \in \mathcal{I}.$$

Moreover, we can assume that the total degree of q is equal to its degree in x_2 (see [3, Corollary 3.4 and Proposition 4.3]).

The Kronecker solver of [6] computes the Kronecker representation of \mathcal{I} and the set of roots of $(\mathcal{I} + (f)) : g^\infty$ with a polynomial cost in the aforementioned quantities. We proved in [3] that it even computes the multiplicities of the roots of $(\mathcal{I} + (f)) : g^\infty$ with the same cost. From now on, we focus on the computation of one local algebra \mathbb{D}_p . Even if it means replacing K with an algebraic extension of K , we can assume that the root p is the origin $0 = (0, \dots, 0)$; we focus on the computation of \mathbb{D}_0 .

As a conclusion, our problem is now to compute the local algebra of the origin as an isolated root of $\mathcal{I} + (f)$, where \mathcal{I} is a one dimensional radical ideal in Noether position given by its Kronecker representation, and where x_1 separates the roots of $\mathcal{I} + (f)$.

2. A LOCALIZED MODULE OF THE CURVE

We use the latter assumptions to define a localized module of the curve. Let $K[[x_1]]$ be the ring of formal power series in x_1 over K , and let \mathcal{I}_0 denote the ideal \mathcal{I} extended to $K[[x_1]][x_2, \dots, x_n]$. We set

$$\mathbb{B}_0 = K[[x_1]][x_2, \dots, x_n]/\mathcal{I}_0.$$

It is well known that the algebra $\bar{K}[x_1, \dots, x_n]/(\mathcal{I} + (f))$ is isomorphic to the direct product of all the \mathbb{D}_p when p covers the set of roots of $\mathcal{I} + (f)$ in \bar{K}^n (see [4, Theorem 2.13] for instance). Since the only root of $\mathcal{I} + (f)$ in \bar{K}^n whose first coordinate is 0 is the origin, the \bar{K} -algebra $\bar{K} \otimes \mathbb{B}_0/(f)$ is isomorphic to \mathbb{D}_0 , as we illustrate with the following example: let \mathbb{Q} be the rational number field, let \mathcal{I} be the ideal of $\mathbb{Q}[x_1, x_2]$ generated by $q = (x_1^2 + (x_2 - 1)^2 - 1)$ and let $f = x_2 - x_1^2$; then $\mathcal{I} + (f) = (x_1^2(x_1 - 1)(x_1 + 1), x_2 - x_1^2)$, and the \mathbb{C} -algebra $\mathbb{C}[x_1, x_2]/\mathcal{I} + (f)$ is isomorphic to $\mathbb{D}_{(0,0)} \times \mathbb{D}_{(1,1)} \times \mathbb{D}_{(-1,1)}$; localizing in $x_1 = 0$ allows us to remove the two points $(1, 1), (-1, 1)$ since $(x_1 - 1)$ and $(x_1 + 1)$ are invertible in $\mathbb{Q}[[x_1]]$.

Now, since \mathcal{I} is radical unmixed in general Noether position, \mathbb{B}_0 is a $K[[x_1]]$ -module of finite type. We express \mathbb{B}_0 as a submodule of an easily computable free module \mathbb{L}_0 ; this will allow us to do all the forthcoming computations in a given basis of \mathbb{L}_0 . Let $\text{Disc}(q) \in K[[x_1]]$ denote the discriminant of q with respect to x_2 , that is, the resultant of q and $\partial q/\partial x_2$ with respect to x_2 . Since the ideal \mathcal{I} is radical, the polynomial q is square free, so that $\text{Disc}(q) \neq 0$. Let m_0 denote the valuation of $\text{Disc}(q)$ in x_1 , that is, the largest integer such that $x_1^{m_0}$ divides $\text{Disc}(q)$. Let δ be the degree of q when seen as a polynomial in x_2 in $K[[x_1]][x_2]$. Let us remark that since the total degree of q is equal to δ , m_0 is at most $\delta(\delta - 1)$. We set

$$\mathbb{L}_0 = K[[x_1]] \frac{1}{x_1^{m_0}} \oplus K[[x_1]] \frac{x_2}{x_1^{m_0}} \oplus \dots \oplus K[[x_1]] \frac{x_2^{\delta-1}}{x_1^{m_0}}.$$

Since \mathcal{I} is in Noether position, x_3, \dots, x_n belong to the integral closure of $K[[x_1]]$ in $K(x_1)[x_2]/(q)$. Then \mathbb{B}_0 is a submodule of \mathbb{L}_0 by a classical result about integral closures (see [4, Proposition 13.14] for instance).

All computations will now be done in the canonical basis $1/x_1^{m_0}, \dots, x_2^{\delta-1}/x_1^{m_0}$ of \mathbb{L}_0 . In short, we will say that we compute *coordinates in \mathbb{L}_0* when we compute

coordinates in the latter basis. The polynomials w_3, \dots, w_n of the Kronecker representation of \mathcal{I} and the algebra structure of \mathbb{B}_0 allow us to compute the coordinates of all monomials in the variables x_2, \dots, x_n in \mathbb{L}_0 .

Since q is the monic generator of $\mathcal{I}_0 \cap K[[x_1]][x_2]$, the $K[[x_1]]$ -module

$$\mathbb{M}_0 = K[[x_1]] \oplus K[[x_1]]x_2 \oplus \dots \oplus K[[x_1]]x_2^{\delta-1}$$

is a $K[[x_1]]$ -submodule of \mathbb{B}_0 . We will compute \mathbb{B}_0 by adding to \mathbb{M}_0 all the monomials in x_3, \dots, x_n seen as elements of \mathbb{L}_0 .

A first idea is to take advantage of the algebra structure of \mathbb{B}_0 as the following algorithm does:

- initialize \mathbb{M} with \mathbb{M}_0 ,
- compute a basis e_1, \dots, e_δ of $\mathbb{M}' = \mathbb{M} + K[[x_1]]x_3 + \dots + K[[x_1]]x_n$;
- while $\mathbb{M} \neq \mathbb{M}'$, replace \mathbb{M} with \mathbb{M}' , and replace e_1, \dots, e_δ with a basis of $\mathbb{M}' = \mathbb{M} + \sum_{1 \leq k, \ell \leq \delta} K[[x_1]]e_k e_\ell$.

It is quite easy to see that if $\mathbb{M}_0 \subset \mathbb{M}_1 \subset \dots \subset \mathbb{M}_\gamma \subset \mathbb{L}_0$ is a chain of submodules of \mathbb{L}_0 beginning with \mathbb{M}_0 , where the inclusions are strict, then its length γ is at most $m_0\delta$. Therefore the number of crossings through the while loop is at most $m_0\delta$, and this algorithm computes at most $(n-2) + m_0\delta^3$ sums of type $\mathbb{M} + K[[x_1]]v$, where \mathbb{M} is a submodule of \mathbb{L}_0 and v belongs to \mathbb{L}_0 .

This algorithm can be improved by adding variables one by one: by computing the algebras $\mathbb{B}_0^{(2)} = \mathbb{B}_0 \cap K[[x_1]][x_2]$, $\mathbb{B}_0^{(3)} = \mathbb{B}_0 \cap K[[x_1]][x_2, x_3], \dots, \mathbb{B}_0^{(n)} = \mathbb{B}_0 \cap K[[x_1]][x_2, \dots, x_n]$ successively, we can reduce the number of vectors to add to \mathbb{M}_0 so that it belongs to $\mathcal{O}(nm_0\delta)$. This alternative algorithm relies on the good properties of the lexicographic ordering and on methods inspired by [5].

Now, coordinates in \mathbb{L}_0 belong to $K[[x_1]]$, so that we have to work with truncated series. If \mathbb{M} is a submodule of \mathbb{L}_0 of rank δ , Hermite normal forms permit to define a basis of \mathbb{M} whose coordinates belong to $K[x_1]$, that we call *normal lower triangular basis*. This basis is uniquely determined by \mathbb{M} . Moreover, if \mathbb{M}_0 is a submodule of \mathbb{M} , the degrees of the coordinates of the elements of this basis of \mathbb{M} in \mathbb{L}_0 are bounded by m_0 . For any element v of \mathbb{L}_0 , the computation of the normal lower triangular basis of $\mathbb{M} + K[[x_1]]v$ is just a Hermite form computation. If \mathbb{M} contains \mathbb{M}_0 , we can prove that this computation can be done with $\mathcal{O}(\delta^3)$ arithmetic operations in the ring $K[[x_1]]/(x_1^{m_0\delta+1})$. The cost of this step is polynomial in the quantities announced in Theorem 1 since δ is bounded by d^n .

3. INTERSECTION

At this stage, we have computed the normal lower triangular basis $\varepsilon_1, \dots, \varepsilon_\delta$ of the $K[[x_1]]$ -module \mathbb{B}_0 . We have to calculate the matrices M_{x_1}, \dots, M_{x_n} of the morphisms of multiplication by x_1, \dots, x_n in $\mathbb{B}_0/(f)$, where f is a non zero divisor in \mathbb{B}_0 . As a straightforward consequence of existence and uniqueness of the Smith form of matrices whose entries are in the principal ideal domain $K[[x_1]]$ (see [10][Chapter 3, 7] for instance), there exist two bases e_1, \dots, e_δ and e'_1, \dots, e'_δ of the $K[[x_1]]$ -module \mathbb{B}_0 and some unique integers $\nu_1 \leq \dots \leq \nu_\delta$ such that for all $k \in \{1, \dots, \delta\}$, $f e_k = x_1^{\nu_k} e'_k$. Then $e'_1, x_1 e'_1, \dots, x_1^{\nu_1-1} e'_1, e'_2, \dots, x_1^{\nu_2-1} e'_2, \dots, e'_\delta, \dots, x_1^{\nu_\delta-1} e'_\delta$ is a basis of $\mathbb{B}_0/(f)$.

If we discard the truncation of series, it is now easy to compute the matrices of multiplication by x_1, \dots, x_n in this basis of $\mathbb{B}_0/(f)$. First, we compute the Smith form of the matrix of multiplication by f in the basis $\varepsilon_1, \dots, \varepsilon_\delta$ of the $K[[x_1]]$ -module \mathbb{B}_0 , together with the basis e'_1, \dots, e'_δ . Then for $i \in \{2, \dots, n\}$, we calculate the matrix of multiplication by x_i in the basis e'_1, \dots, e'_δ of \mathbb{B}_0 , that is some elements $m_{k,\ell}(x_i) \in K[[x_1]]$, $1 \leq k, \ell \leq \delta$ such that $x_i e'_\ell = \sum_{k=1}^{\delta} m_{k,\ell}(x_i) e'_k$. For $\ell \in \{1, \dots, \delta\}$ and $s \in \{0, \dots, \nu_\ell\}$, we obtain the coordinates of $x_i(x_1^s e'_\ell)$ in the previous

basis of $\mathbb{B}_0/(f)$ as the coefficients in K of $\sum_{k=1}^{\delta} (x_1^s m_{k,\ell}(x_1) \bmod x_1^{\nu_k}) e'_k$. The matrix M_{x_1} follows directly from the shape of the latter basis of $\mathbb{B}_0/(f)$.

Let us now recall that μ_0 denotes the multiplicity of 0 as a root of $\mathcal{I} + (f)$, and that we know it since it can be computed by the Kronecker solver. By definition, the dimension of $\mathbb{B}_0/(f)$ is μ_0 , and so $\sum_{k=1}^{\delta} \nu_k = \mu_0$. Assume that we know the coordinates of $x_i, e'_1, \dots, e'_\delta$ in \mathbb{L}_0 to precision $\mu_0 + m_0 + 1$. Then we can compute the entries of the matrices M_{x_i} to precision $\mu_0 + 1$, which is enough for the matrices of x_i in the latter basis of $\mathbb{B}_0/(f)$. The question is now to give an algorithm for the computation of the Smith form of a square matrix with entries in $K[[x_1]]$, together with the post-multiplier, that is, the matrix whose k -th column is the vector of coordinates of e'_k in \mathbb{L}_0 to a given precision. As for the Hermite forms, this is not immediate. The algorithm presented in [13] can be adapted to answer this question, as detailed in [2]. In particular, we prove that in our case, the computation of the needed Smith form with the wanted precision can be done with $\mathcal{O}(\delta^3)$ arithmetic operations in $K[[x_1]]/(x_1^{\mu_0+m_0+1})$. Here again, all the computations can be done with a polynomial cost in the quantities of Theorem 1.

4. FINAL COMMENTS

The efficiency of the algorithm presented in this paper can be improved. In the first section, the computation of the roots in \bar{K}^n as a vector of coordinates from the output of the Kronecker algorithm requires a factorization of a polynomial in $K[x_1]$. This can be avoided by dynamic evaluation techniques. In the second section, we can replace the module \mathbb{B}_0 with a module which only takes in account the irreducible analytic components of the curve that pass through the origin. These improvements can be found in [2].

REFERENCES

1. B. Dayton and Z. Zeng, *Computing the multiplicity structure in solving polynomial systems*, Proceedings of the 2005 International Symposium on Symbolic and Algebraic Computation, ACM, 2005, pp. 116–123.
2. C. Durvy, *Evaluation techniques for zero-dimensional primary decomposition*, preprint 2007, www.math.uvsq.fr/~durvy.
3. C. Durvy and G. Lecerf, *A concise proof of the Kronecker polynomial system solver from scratch*, to appear in *Expositiones Mathematicae*, 2006.
4. D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry*, Graduate Texts in Mathematics, Springer-Verlag, 1995.
5. J. C. Faugère, P. Gianni, D. Lazard, and T. Mora., *Efficient computation of zero-dimensional gröbner basis by change of ordering*, J. Symbolic Comput. **16** (1993), no. 4, 329–344.
6. M. Giusti, G. Lecerf, and B. Salvy, *A Gröbner free alternative for polynomial system solving*, Journal of Complexity **17** (2001), no. 1, 154–211.
7. G.-M. Greuel and G. Pfister, *A Singular introduction to commutative algebra*, Springer-Verlag, 2002.
8. G. Jeronimo, T. Krick, J. Sabia, and M. Sombra, *The computational complexity of the Chow form*, Found. Comput. Math. **4** (2004), no. 1, 41–117.
9. T. Krick and L. Pardo, *A computational method for Diophantine approximation*, Algorithms in algebraic geometry and applications (Santander, 1994), Progr. Math., vol. 143, Birkhäuser, 1996, pp. 193–253.
10. S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, 2002.
11. G. Lecerf, *Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions*, Proceedings of the 2000 International Symposium on Symbolic and Algebraic Computation, ACM, 2000, pp. 209–216.
12. B. Mourrain, *Isolated points, duality and residues*, J. of Pure Appl. Algebra **117/118** (1997), 469–493.
13. G. Villard, *Computation of the Smith normal form of polynomial matrices*, Proceedings of the 1993 International Symposium on Symbolic and Algebraic Computation, ACM, 1993, pp. 209–217.

CLÉMENCE DURVYE, LABORATOIRE DE MATHÉMATIQUES (UMR 8100 CNRS), UNIVERSITÉ
DE VERSAILLES SAINT-QUENTIN-EN-YVELINES, 45 AVENUE DES ÉTATS-UNIS, 78035 VERSAILLES,
FRANCE

E-mail address: `Clemence.Durvye@math.uvsq.fr`