Fast Algorithms for Zero-Dimensional Polynomial Systems using Duality

Alin Bostan[1], Bruno Salvy[2], Éric Schost[3]

[1] Laboratoire STIX, École polytechnique, France and IMAR, Romania
Alin.Bostan@stix.polytechnique.fr
[2] Projet Algorithmes, Inria Rocquencourt, France
Bruno.Salvy@inria.fr
[3] Laboratoire STIX, École polytechnique, France
Eric.Schost@stix.polytechnique.fr

Abstract. Many questions concerning a zero-dimensional polynomial system can be reduced to linear algebra operations in the quotient algebra $A = k[X_1, \ldots, X_n]/\mathcal{I}$, where $\mathcal{I}$ is the ideal generated by the input system. Assuming that the multiplicative structure of the algebra A is (partly) known, we address the question of speeding up the linear algebra phase for the computation of minimal polynomials and rational parametrizations in A.
We present new formulæ for the rational parametrizations, extending those of Rouillier, and algorithms extending ideas introduced by Shoup in the univariate case. Our approach is based on the A-module structure of the dual space $\widehat{A}$. An important feature of our algorithms is that we do not require $\widehat{A}$ to be free and of rank 1.
The complexity of our algorithms for computing the minimal polynomial and the rational parametrizations are $O(2^n D^{5/2})$ and $O(n2^n D^{5/2})$ respectively, where D is the dimension of A. For fixed n, this is better than algorithms based on linear algebra except when the complexity of the available matrix product has exponent less than $5/2$.

Key words: Duality, polynomial system solving, linear recurrent sequences.

1 Introduction

Many questions concerning zero-dimensional polynomial systems can be reduced to linear algebra operations in some quotient algebra. Assuming that the multiplicative structure of this algebra is (partly) known, we address the question of speeding up the linear algebra phase for two questions.

Specifically, let k be a field, $\overline{k}$ its algebraic closure and $\mathcal{I}$ a zero-dimensional ideal of $k[X_1, \ldots, X_n]$. Let $\mathcal{V}(\mathcal{I}) \subset \overline{k}^n$ be the zero-set of the polynomial system defined by $\mathcal{I}$. Given an element u of $A = k[X_1, \ldots, X_n]/\mathcal{I}$, we consider the following problems:

1. compute its *minimal polynomial* m_u, that is, the (unique) monic univariate polynomial of minimal degree such that $m_u(u) = 0$ in A;

2. if u *separates* the points of $\mathcal{V}(\mathcal{I})$ (see definition below), compute *parametrizations* expressing the coordinates of these points in terms of u.

We suppose that k is a *perfect* field. This discards many pathologies such as algebraic field extensions of k without a primitive element. In most applications we have in mind, k is finite or of characteristic zero, so this assumption is satisfied.

The computation of minimal polynomials of elements in such quotient algebras is of particular interest when A is a field or a product of fields. This question appears as a basic subroutine for the computation of triangular sets [40], for the study of the intermediate fields between k and A [41], in Galois theory [3], ... For instance, starting from a description of a quotient algebra by means of a Gröbner basis, Lazard's algorithm `Triangular` [40] produces a "triangular description" of the input ideal through repeated minimal polynomial computations.

In the noncommutative setting of the effective theory of $\mathcal{D}$-modules, an important role is played by the *b-function* of a holonomic system of linear partial differential equations. Algorithm 5.1.5 in [61] reduces the computation of the b-function to that of the minimal polynomial of an element in a quotient algebra of the type we consider here.

Another of our initial motivations is the study of algebraic curves and cryptosystems built upon them. Factorization patterns of the minimal polynomials of well-chosen elements help determine the cardinality of the Jacobian of hyperelliptic curves over finite fields, see [15, 23, 64, 24]. In such situations, the element u will typically not be primitive for $k \to A$. The polynomial m_u has degree less than the dimension of A, and of course we want to make use of this fact.

Our second interest is the determination of a parametrization of the coordinates of the solutions of $\mathcal{I}$. To this effect, we say that $u \in A$ *separates* the points of $\mathcal{V}(\mathcal{I})$, or is a *separating element* for $\mathcal{I}$, if for all points $P \neq P'$ in $\mathcal{V}(\mathcal{I})$, u takes distinct values on P and P' (see [1, 60]). Since k is a perfect field, this is the case if and only if u is a primitive element of the reduced algebra $A_{\mathrm{red}} = k[X_1, \dots, X_n]/\sqrt{\mathcal{I}}$, where $\sqrt{\mathcal{I}}$ is the radical of $\mathcal{I}$, see [5]. In this situation, the coordinates of the points in $\mathcal{V}(\mathcal{I})$ can be expressed as *rational* functions of u. We call *rational parametrization* of the coordinates of the points in the zero-set $\mathcal{V}(\mathcal{I})$ the data of a separating element u, its minimal polynomial m_u, and rational functions $f_1, \dots, f_n$ such that $X_i = f_i(u)$ holds in A_{red}.

Such representations, which go back to Kronecker [35], are well suited to many purposes such as effective computation in the reduced algebra A_{red} or counting and isolation of real or complex roots. This representation bears the name *Geometric Resolution* in [26, 25, 27, 42]. Using the characteristic polynomial of u instead of its minimal polynomial, this representation is called a *Rational Univariate Representation* of the roots of $\mathcal{I}$, using the denomination introduced in [60].

In this article, we present some structure theorems related to the two questions mentioned above, then show how algorithmic ideas introduced in the univariate case by Shoup [66, 67] fit into this context. Our algorithms require precomputations, either of some multiplication matrices in A, or of the whole multiplication table. These objects may be obtained from the computation of a Gröbner basis [13, 20, 19]. We do not address the difficult question of the complexity of these precomputations.

Computing a minimal polynomial. Let u be an element in A and δ a bound on the degree of its minimal polynomial m_u. A natural algorithm for the computation of m_u consists in expressing the first δ powers of u on a basis of the k vector space A and then looking for a linear dependency between them. This last step has complexity $O(D^\omega)$, where ω is the exponent of the complexity of matrix multiplication, and D is the dimension of A over k [14, Chapter 16]. Thus $\omega = 3$ for the naive product, and the best result known to this date is $\omega < 2.376$ [16]. However, the fastest widely available implementation we are aware of is based on Strassen's algorithm [68] of exponent $\log_2(7) \simeq 2.808$, in the computer algebra system Magma [10].

A first improvement consists in considering the values taken by a linear form ℓ on the powers of u. The sequence $\left(\ell(u^i)\right)_{i\geq 0}$ admits a minimal linear recurrence relation, which coincides, for a random choice of ℓ, with the minimal polynomial of u, and which can be computed efficiently. This suggests the following algorithm: compute the powers of u, evaluate ℓ on them, and recover the minimal polynomial. This requires the ability to multiply by u. The input of this first algorithm will thus be the multiplication matrix of u in A.

In the context of polynomial factorization over finite fields, Shoup showed in [66, 67] how to speed up these computations in the univariate case when $A = k[X]/(f)$. His idea is to adapt Paterson and Stockmeyer's fast evaluation algorithm [58] using an A-module structure on the dual space $\widehat{A}$. The clever use of this structure avoids the computation of all the powers of the element u.

We demonstrate here that this idea extends to multivariate situations, and yields another method for computing a minimal polynomial. The main difficulty lies in obtaining an efficient implementation of the operations in $\widehat{A}$. For the moment, our solution requires a stronger input than above: the whole multiplication table of A. This input is also used for instance in the algorithms of [1, 60].

These results are presented in a precise fashion in the following theorem. The algorithms require an *a priori* bound δ on the degree of the minimal polynomial we want to compute. A trivial bound is the dimension D of A. Problem-specific bounds are often available, as for instance in [15, 23, 24, 64].

Theorem 1 *Let D be the dimension of A as a k-vector space, and let u be in A, with minimal polynomial m_u. Suppose that δ is an* a priori *bound on the degree of m_u.*

1. *If the matrix of multiplication by u is known, then m_u can be computed in $O(\delta D^2)$ operations in k.*
2. *If the multiplication table of A is known, then m_u can be computed in $O(2^n \delta^{1/2} D^2)$ operations in k.*

In both cases, the algorithm chooses D values in k. If these values are chosen in a finite subset Γ of k, all choices except at most $\delta|\Gamma|^{D-1}$ assure success.

For $\delta \approx D$, the complexity is $O(D^3)$ in the first case and $O(2^n D^{5/2})$ in the second case. If the number of variables n is fixed, the gain in complexity is of order $\sqrt{D}$, typical of the baby step/giant step techniques which underlie the second approach.

The probabilistic aspect comes from the choice of a linear form over A. For unlucky choices, the output of our algorithms is a strict divisor of the actual minimal polynomial. If the degree of the output coincides with the upper bound δ, then this output is necessarily correct. Otherwise, we can either estimate the probability of an unlucky choice, or evaluate the candidate minimal polynomial on u.

Computing parametrizations. In the discussion leading to the proof of Theorem 1, we introduce some generating series, depending on both the element u and a linear form over A. If u is separating, we show that such series allow to compute rational parametrizations of the points of $\mathcal{V}(\mathcal{I})$. This yields our formulæ in Proposition 3, that extend those of Rouillier [60].

Our formulæ are satisfied if $\mathcal{I}$ is a radical ideal. In the general case, they remain valid under an additional hypothesis, given in Theorem 2 below, and explained in more detail in §3.2. In short, the minimal polynomial of u must have the maximal possible degree, and the characteristic of the base field must be zero or large enough.

To use these formulæ in practice, the computational task is quite similar to that required to compute a minimal polynomial: evaluating some linear forms on the powers of u. So in a similar fashion, we propose two methods: the direct approach, which requires only multiplication matrices, or its refinement based on Shoup's idea, using the whole multiplication table.

The first approach has the same complexity as the algorithm of [60], at most $O(D^3)$, but our input is weaker. The second approach takes the same input as [60]. Its complexity is at most $O(n2^n D^{5/2})$. This becomes better when the number n of variables is kept constant, whereas the dimension of the quotient algebra becomes large. As above, the gain is then of order $\sqrt{D}$.

Theorem 2 *Let D be the dimension of $A = k[X_1, \ldots, X_n]/\mathcal{I}$ as a k-vector space, and let u be a separating element in A, with minimal polynomial m_u. Assume that*

- *the characteristic of k is zero or greater than $\min\{s \mid \sqrt{\mathcal{I}}^{\,s} \subset \mathcal{I}\}$;*
- *the degree of the minimal polynomial of u is the degree of the minimal polynomial of a generic element in A.*

If δ is an a priori *bound on the degree of m_u, then the following holds:*

1. *If the matrices of multiplication by u and $x_1, \ldots, x_n$ are known, then a rational parametrization of the zero-set $\mathcal{V}(\mathcal{I})$ can be computed in $O(\delta D^2 + nD^2)$ operations in k.*

2. If the multiplication table of A is known, then a parametrization can be computed in $O(n2^n\delta^{1/2}D^2)$ operations in k.

The algorithms are probabilistic. In both cases, the algorithm chooses D values in k. If these values are chosen in a finite subset Γ of k, all choices except at most $\delta|\Gamma|^{D-1}$ assure success.

The probabilistic aspect lies, as in Theorem 1, in the choice of a linear form over A. If $\mathcal{I}$ is a radical ideal, it is straightforward to check the correctness of the output, see Section 3.1. Otherwise, the last assertion in the theorem makes it possible to estimate the probability of choosing an unlucky linear form.

The algorithms mentioned in Theorems 1 and 2 are easily implemented in a computer algebra system such as Magma [10]. Our experiments show their good practical behavior (see Section 5).

Related results. The A-module $\widehat{A}$ is called the *canonical module* [63, 36, 18], and has been used in a variety of applications. In particular, the case when the dual $\widehat{A}$ is a free A-module of rank 1 has led to new geometric and arithmetic forms of the Nullstellensatz [26, 25], a new proof of the Eisenbud-Levine formula [4], or fast algorithms for isolating roots of complete intersection multivariate systems [51–54].

One of our main contributions is to propose algorithms using this module structure whenever the operations in A and $\widehat{A}$ are effective, even if the dual is not free and of rank 1.

We have focused on the case when the structure of the algebra A is explicitly given. Our ideas also apply if $\mathcal{I}$ is given by n generators without zeros at infinity. Indeed, in this context, the basis of the results in [52–54] are fast multiplication algorithms in A. It might be possible to extend these results so as to obtain similar complexity estimates for the operations in $\widehat{A}$, which would lead to improved complexity algorithms in this case. More generally, any efficient algorithm for the operations in A and $\widehat{A}$ can be used in conjunction with the ideas presented here.

In a different context, the *geometric resolution* algorithm of [27] solves polynomial systems of dimension zero without multiplicities. Its complexity is quadratic in a geometric quantity attached to the input system, and linear in its *complexity of evaluation*, that is, the number of arithmetic operations necessary to evaluate the system. Recently, this algorithm has been extended so as to handle arbitrary systems, see [42–44]. An important issue is to extend our algorithmic ideas to this context.

Finally, let us mention that F. Rouillier informed us of an improvement of the second result given in Theorem 2, where a factor of order n is saved.

Outline of the paper. In Section 2, we define the module structure on the dual of A, and some useful generating series. In Section 3, we show how both a minimal polynomial and some parametrizations can be read out from such series.

A direct approach to compute these series yields at once the first assertions in Theorems 1 and 2. In Section 4, we show how to improve the crucial step: the evaluation of a linear form on the successive powers of an element in A. This will prove the second parts of Theorems 1 and 2. In Section 5 we present the experimental behavior of our algorithms. The last section gives the proof of a key proposition in Section 3.

Notation. We use the following notation:

- The radical of an ideal $\mathcal{I}$ of $k[X_1, \ldots, X_n]$ is denoted by $\sqrt{\mathcal{I}}$.
- The algebra A is the quotient $k[X_1, \ldots, X_n]/\mathcal{I}$; the images of the variables $X_1, \ldots, X_n$ in A are denoted by $x_1, \ldots, x_n$. We denote by D the dimension of the k-vector space A, by $\Omega = \{\omega_i\}_{i=1,\ldots,D}$ a monomial basis of A and by $E \subset \mathbb{N}^n$ the set of exponents of the elements in Ω.
- Given $\alpha = (\alpha_1, \ldots, \alpha_n)$ in $\mathbb{N}^n$, we write X^α for the monomial $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, and x^α for the product $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$.
- The minimal polynomial of any element t in a finite-dimensional algebra is denoted by m_t.
- For two subsets $E \subset \mathbb{N}^n$ and $F \subset \mathbb{N}^n$, we let $E + F$ be their Minkowski sum, that is, the set $\{e + f,\ e \in E, f \in F\}$. We use the abbreviation $2E$ for $E + E \subset \mathbb{N}^n$.
- $\widehat{A}$ designates the dual space $\mathrm{Hom}_k(A, k)$ of the k-linear forms on A. The set $\widehat{\Omega} = \{\widehat{\omega}_i\}_{i=1,\ldots,D}$ represents the dual basis of Ω.
- For a polynomial $P \in k[U]$, we write $\mathrm{rec}(P)$ for its reciprocal $U^{\deg(P)} P(\frac{1}{U})$.

2 On the Dual of the Quotient Algebra

Most results in this article involve linear forms defined over the algebra A. We frequently use the following operation, which makes the dual $\widehat{A}$ a A-module:

$$\begin{aligned} \circ : A \times \widehat{A} &\to \widehat{A} \\ (u, \ell) &\mapsto u \circ \ell : v \mapsto \ell(vu). \end{aligned}$$

This section is devoted to basic results related to this operation. As mentioned in the introduction, the case when $\widehat{A}$ is a free A-module of rank 1 is of particular interest, but this assumption is not required here.

The following lemma (see also [67, 53]) justifies the terminology *transposed product* for the A-module operation on $\widehat{A}$.

Lemma 1 *Let u be in A. The matrix of the linear operator*

$$\begin{aligned} \widehat{A} &\to \widehat{A} \\ \ell &\mapsto u \circ \ell \end{aligned}$$

in the dual basis $\widehat{\Omega}$ is the transposed of the matrix of multiplication by u in the basis Ω.

Proof. Let ω be in Ω. The value $(u \circ \ell)(\omega)$ is $\ell(\omega u)$. It is given by the product between the row-vector of the coefficients of ωu on the basis Ω and the vector representing ℓ on the dual basis. This implies that the vector representing $u \circ \ell$ is the product $\mathbf{M}_u^t \ell$, where $\mathbf{M}_u^t$ is the transposed of the matrix $\mathbf{M}_u$ representing the multiplication by u in the basis Ω. $\square$

This result has a strong consequence in terms of complexity, based on the *transposition principle*, or *Tellegen's principle*. This principle is actually a theorem about arithmetic circuits, which originates from linear circuit design and analysis [69, 9, 59, 2] and was introduced in computer algebra in [21, 22, 30, 33]. The proof can be found in [14, Theorem 13.20], see also [32, Problem 6] for more comments.

Transposition principle. Let $\mathbf{M}$ be a $n \times n$ matrix, with no zero row nor column, and suppose that the product $\mathbf{v} \mapsto \mathbf{M}\mathbf{v}$ can be computed by an arithmetic circuit of size $\mathcal{C}$. Then there exists an arithmetic circuit of size $\mathcal{C}$ that computes the transposed product $\mathbf{w} \mapsto \mathbf{M}^t\mathbf{w}$.

In most applications, the multiplication matrix $\mathbf{M}_u$ is not known, and its determination might be quite costly. Nevertheless, the transposition principle implies that, whatever the algorithm used for multiplication, there exists an algorithm for transposed multiplication with the same cost, as long as arithmetic circuits are used.

Yet, the algorithms used for (fast) multiplication may not be given by arithmetic circuits. Moreover, even if the proof of the transposition principle is constructive, it is far from obvious how to put it to practice in a computer algebra environment. Therefore, particular attention must be given to design explicit versions of transposed algorithms. In [11], the transposes of some basic algorithms for univariate polynomials are described. In what follows, we will give algorithms for the transposed product in the algebra A.

Generating series. We associate to every element ℓ of $\widehat{A}$ a multivariate formal power series, denoted $S(\ell)$. For a subset $F \subset \mathbb{N}^n$ we also define a truncated series $S(\ell, F)$. These series are given by:

$$S(\ell) := \sum_{\alpha \in \mathbb{N}^n} \ell(x^\alpha) X^\alpha, \quad S(\ell, F) := \sum_{\alpha \in F} \ell(x^\alpha) X^\alpha.$$

Since E is the set of exponents of the monomial basis Ω, a linear form ℓ in $\widehat{A}$ is uniquely determined by $S(\ell, E)$. Given u in A and ℓ in $\widehat{A}$, we also introduce the univariate Laurent series

$$R(u, \ell) := \sum_{i \geq 0} \frac{\ell(u^i)}{U^{i+1}}.$$

The series $S(\ell)$ and particularly $R(u, \ell)$ are used repeatedly in this article. Similar representations appear in [67, 52, 53], and in [60] for specific linear forms. The following proposition gathers the results we will need when using these generating series. The first point is folklore, similar arguments can be found in [52, 53] and [67]. Let us also mention that results very similar to the second point below can be found in [45], which describes the use of duality-based techniques in coding theory.

Proposition 1 *Let ℓ be in $\widehat{A}$.*

- *Let $u = \sum_{\alpha \in E} u_\alpha x^\alpha$ be in A, let F be a subset of $\mathbb{N}^n$ and let T be the Laurent series*
$$T = \sum_{\alpha \in \mathbb{Z}^n} t_\alpha X^\alpha := \left(\sum_{\alpha \in E} \frac{u_\alpha}{X^\alpha} \right) \cdot S(\ell, E+F).$$
Then the series $S(u \circ \ell, F)$ is $\sum_{\alpha \in F} t_\alpha X^\alpha$.
- *For i in $1, \ldots, n$, let $m_i \in k[X_i]$ be the minimal polynomial of x_i, and let δ_i be its degree. Then there exists a polynomial $H_\ell \in k[X_1, \ldots, X_n]$ of partial degree in each variable X_i less than δ_i, such that the following holds:*
$$S(\ell) = \frac{H_\ell}{\mathrm{rec}(m_1) \cdots \mathrm{rec}(m_n)}.$$
- *Let u be in A, with minimal polynomial $m_u \in k[U]$ of degree δ_u. Then there exists a polynomial $G_{u,\ell} \in k[U]$ of degree less than δ_u such that the following holds:*
$$R(u, \ell) = \frac{G_{u,\ell}}{m_u}.$$
Moreover, $G_{u,\ell}$ is the quotient of $\displaystyle m_u \sum_{i=0}^{\delta_u - 1} \ell(u^i) U^{\delta_u - i - 1}$ by U^{δ_u}.
- *There exists a nonzero polynomial $r_u \in k[L_1, \ldots, L_D]$ of total degree at most δ_u, such that $G_{u,\ell}$ is coprime to m_u if and only if $r_u(\ell_1, \ldots, \ell_D) \neq 0$, where $(\ell_1, \ldots, \ell_D)$ are the coordinates of ℓ on the dual basis $\widehat{\Omega}$.*

Proof. For α' in F, the value $(u \circ \ell)(x^{\alpha'})$ is $\ell(ux^{\alpha'}) = \sum_{\alpha \in E} u_\alpha \ell(x^{\alpha+\alpha'})$. The series T can be written

$$T = \left(\sum_{\alpha \in E} u_\alpha X^{-\alpha} \right) \left(\sum_{\beta \in E+F} \ell(x^\beta) X^\beta \right) = \sum_{\alpha' \in E+F-E} \left(\sum_{\alpha \in E} u_\alpha \ell(x^{\alpha+\alpha'}) \right) X^{\alpha'}.$$

The coefficient of $X^{\alpha'}$ in T coincides with $\ell(ux^{\alpha'})$, which proves the first point.

We turn to the second point. Taking $F = \mathbb{N}^n$ shows that for any u in A, the series $S(u \circ \ell)$ is the restriction of $u(1/X_1, \ldots, 1/X_n) S(\ell)$ to the set of monomials with exponent in $\mathbb{N}^n$.

Let i be in $1, \ldots, n$. Since $m_i(X_i)$ is zero in A, the series $S(m_i(x_i) \circ \ell)$ is zero. Consequently, all the monomials in $m_i(1/X_i) S(\ell)$ have degree in X_i between $-\delta_i$ and -1. This means that all monomials in $\mathrm{rec}(m_i)(X_i) S(\ell) = X_i^{\delta_i} m_i(1/X_i) S(\ell)$

have degree in X_i between 0 and $\delta_i - 1$. Taking all i into account shows that the series $\mathrm{rec}(m_1)(X_1)\cdots\mathrm{rec}(m_n)(X_n)S(\ell)$ is a polynomial, whose partial degree in each variable X_i is less than δ_i.

Next, we prove the third part. The linear form ℓ induces a linear form on the algebra $k[U]/m_u$. The previous point shows that $\mathrm{rec}(m_u)\sum_{i\geq 0}\ell(u^i)U^i$ is a polynomial of degree less than δ_u. Evaluating it at $1/U$ and multiplying the result by $U^{\delta_u - 1}$ shows that $m_u R(u,\ell) = m_u \sum_{i\geq 0}\ell(u^i)/U^{i+1}$ is also a polynomial of degree less than δ_u, denoted by $G_{u,\ell}$. For degree reasons, only a finite number of terms in $R(u,\ell)$ contribute at the product $m_u R(u,\ell)$ defining $G_{u,\ell}$. More exactly, the polynomial $G_{u,\ell}$ equals the polynomial part of the series $m_u \sum_{i=0}^{\delta_u - 1}\ell(u^i)/U^{i+1}$ containing only nonnegative powers of U; on the other hand, this polynomial part is obviously the quotient of the division of $m_u \sum_{i=0}^{\delta_u-1}\ell(u^i)U^{\delta_u - i - 1}$ by U^{δ_u}.

Let us finally prove the last point. For ω_i in Ω, we let $G_{u,i} \in k[U]$ be $m_u R(u, \widehat{\omega}_i)$. If $\ell_1, \ldots, \ell_D$ are the coordinates of ℓ on the dual basis, then $G_{u,\ell}$ is $\sum_{1\leq i\leq D}\ell_i G_{u,i}$. Let now $r_u \in k[L_1,\ldots,L_D]$ be the resultant of $\sum_{1\leq i\leq D} L_i G_{u,i}$ and m_u with respect to U. Then, using [71, Lemma 6.25], we see that $G_{u,\ell}$ and m_u are coprime if and only if $r_u(\ell_1,\ldots,\ell_D)\neq 0$.

For any polynomial G of degree less than δ_u, we now prove that there exists $\ell \in \widehat{A}$ such that $G = G_{u,\ell}$. This suffices to show that r_u is a nonzero polynomial. Since r_u has total degree at most δ_u, this will prove the proposition.

The system $m_u R(u,\ell) = G$ is linear in $(\ell(1),\ldots,\ell(u^{\delta_u - 1}))$, of triangular form with diagonal entries equal to 1 as m_u is monic. Since $(1,\ldots,u^{\delta_u-1})$ are linearly independent, it is always possible to find ℓ which takes prescribed values on these powers of u. □

This proposition shows that for a generic choice of ℓ, the irreducible form of the rational series $R(u,\ell)$ has the minimal polynomial m_u for denominator. This will be used repeatedly in the rest of this article.

An algorithm for the transposed product. The first point in the previous proposition suggests the following algorithm for the transposed product: given ℓ and u, first compute $S(\ell, 2E)$, taking $F = E$; then perform a power series multiplication, and read off the coefficients of $S(u\circ\ell, E)$.

The main difficulty lies in determining the truncated series $S(\ell,2E)$ from its first terms $S(\ell,E)$. The second point of Proposition 1 shows that the series $S(\ell)$ is rational. When there is only one variable, the quotient A is given as $k[X]/(f)$, so the denominator of $S(\ell)$ is known *a priori*, as it is the reciprocal polynomial of f. It is then straightforward to recover the numerator from the first terms $S(\ell,E)$, which in turns gives the next terms of $S(\ell,2E)$ by Taylor expansion. This is the basis of Shoup's algorithm for the univariate transposed product [67].

In the general case, the denominator is not known in advance. At the moment, we are unable to make an algorithmic use with good complexity of the rationality of the series $S(\ell)$, or even of the stronger form given in the second part of Proposition 1.

3 Computing Minimal Polynomials and Rational Parametrizations

We now describe our first algorithms solving the questions mentioned in the introduction: computing the minimal polynomial of an element u in A, and the corresponding parametrization, if u is separating. These algorithms are derived from the study of the generating series introduced in the previous section, and yield the first parts of Theorems 1 and 2.

Similar considerations to those presented in Subsection 3.1 can be found in the literature, for instance in [72, 66, 67, 31]. The main new result is Proposition 3 in Subsection 3.2: it provides a generalization of Rouillier's formulæ [60], which does not require the use of a specific linear form to compute parametrizations. In [60], this specific form, the *trace*, is computed from the multiplication table of A. Here, we avoid this precomputation, as we show that almost any form can be used. Consequently, the algorithms presented in Subsection 3.3 only require multiplication matrices as input.

All these algorithms are based on the same basic subroutine, the evaluation of a linear form on the successive powers of an element in A. Thus their complexity is fundamentally dependent on the cost of this particular task; reducing this cost will be the object of Section 4.

3.1 Computing a minimal polynomial

Our method to compute a minimal polynomial in A is based on the following property: if ℓ is an arbitrary linear form on A, then the scalar sequence $\left(\ell(u^i)\right)_{i\geq 0}$ is linearly recurrent, that is, it can be defined by a linear recurrence relation with constant coefficients. The relation of minimal degree is called its *minimal polynomial*; if ℓ is a "generic" linear form, then this polynomial equals the the minimal polynomial of u.

This principle has been used in a variety of settings. It underlies Wiedemann's algorithm [72] for solving sparse — or rather, easy-to-evaluate — linear systems, and is the basis of Thiong Ly's and Shoup's algorithms [70, 66, 67] to compute minimal polynomials in the univariate case $A = k[X]/(f)$.

Given an upper bound δ on its degree, the minimal polynomial of a sequence of scalars $\mathcal{L}$ satisfying a linear recurrence can be computed by Berlekamp-Massey's algorithm, see [6, 49] and [71, chapter 12.3]. This algorithm requires the first 2δ values of $\mathcal{L}$, and amounts to the computation of a (δ, δ) Padé approximant for the generating series $\sum_{i\geq 0} \mathcal{L}_i U^i$. This is denoted by `MinimalPolynomial`$(\mathcal{L})$ in the algorithm below.

Computing the minimal polynomial

Input: u in A, ℓ in $\widehat{A}$, a bound δ on the degree of m_u.
Output: a polynomial $m_{u,\ell}$ in $k[U]$.

$\mathcal{L} \leftarrow [\ell(1), \ell(u), \dots, \ell(u^{2\delta-1})]$;
$m_{u,\ell} \leftarrow \mathtt{MinimalPolynomial}(\mathcal{L})$;
$\mathtt{return}(m_{u,\ell})$;

The next proposition encapsulates the cost and correctness analysis of this algorithm. Similar considerations for Wiedemann's algorithm can be found in [31].

Proposition 2 *Let u be in A and let m_u be its minimal polynomial. If δ is a bound on the degree of m_u, then besides the evaluation of the sequence $[\ell(1), \ell(u), \dots, \ell(u^{2\delta-1})]$, the previous algorithm requires $O(\delta^2)$ operations in k. Its output is the polynomial m_u if and only if the polynomial $G_{u,\ell}$ from Proposition 1 and m_u are coprime. Otherwise, the output $m_{u,\ell}$ is a strict divisor of m_u.*

Proof. Using a naive version of the extended Euclidean algorithm, the running time of Berlekamp-Massey's algorithm is quadratic in δ [71, Theorem 12. 10]. This proves the complexity estimate.

Let $m_{u,\ell}$ be the (monic) minimal polynomial of the sequence $\big(\ell(u^i)\big)_{i\geq 0}$. The polynomial m_u cancels this sequence, since $\sum_i a_i u^i = 0$ implies that the equality $\sum_i a_i \ell(u^{i+j}) = 0$ holds for all j. Consequently, $m_{u,\ell}$ divides m_u. Let us show that they coincide if and only if the polynomials $G_{u,\ell}$ and m_u are coprime, where $G_{u,\ell}$ is defined in Proposition 1:

$$R(u,\ell) := \sum_{i\geq 0} \frac{\ell(u^i)}{U^{i+1}} = \frac{G_{u,\ell}}{m_u}. \tag{1}$$

To this effect, we recall the following result from [28, Lemma 1]: the generating series $R(u,\ell)$ has the rational form

$$R(u,\ell) = \frac{H_{u,\ell}}{m_{u,\ell}}, \tag{2}$$

the polynomials $H_{u,\ell}$ and $m_{u,\ell}$ *being coprime.*

The two rational expressions of $R(u,\ell)$ in equations (1) and (2) show that if $m_{u,\ell}$ and m_u coincide, then $G_{u,\ell}$ and $H_{u,\ell}$ coincide, so $G_{u,\ell}$ and m_u are coprime. For the converse direction, we first notice that, by equations (1) and (2), m_u divides $m_{u,\ell}G_{u,\ell}$. Therefore, if $G_{u,\ell}$ and m_u are coprime, then m_u divides $m_{u,\ell}$. Since $m_{u,\ell}$ always divides m_u, it follows that $m_{u,\ell}$ and m_u coincide. This finishes the proof. □

Using a fast extended Euclidean algorithm [71, chapter 11.1], the complexity of Berlekamp-Massey's algorithm drops to $O(\delta \log^2 \delta \log\log \delta)$. The polynomial

$G_{u,\ell}$ can be computed as a byproduct without affecting the complexity. In any case, the limiting factor in this algorithm is the computation of the sequence $[\ell(1), \ell(u), \ldots, \ell(u^{2\delta-1})]$.

If the degree of the output coincides with the known upper bound for $\deg m_u$, the output is necessarily correct. A trivial upper bound is the dimension of A: if the degree of the output reaches this upper bound, then u is primitive for $k \to A$, and the result of the algorithm is correct. Otherwise, Proposition 2 states that the output $m_{u,\ell}$ is correct if and only if $m_{u,\ell}(u)$ is zero.

3.2 Computing parametrizations

If u is a separating element for $\mathcal{I}$, we want to compute parametrizations giving the values of the variables X_j on $\mathcal{V}(\mathcal{I})$ as functions of u, that is, rational functions $f_j(u)$ such that the relations $x_j = f_j(u)$ hold in the reduced algebra $A_{\mathrm{red}} = k[X_1, \ldots, X_n]/\sqrt{\mathcal{I}}$. Following the ideas of Kronecker [35] and Macaulay [46], we propose a method to compute *rational* parametrizations of the form

$$x_j = \frac{g_j(u)}{g(u)}.$$

Our method requires the following assumptions:

1. the characteristic of k is zero or larger than $\min\{s, \sqrt{\mathcal{I}}^{\,s} \subset \mathcal{I}\}$;
2. the degree of the minimal polynomial m_u of u is the degree of the minimal polynomial of a generic element in A.

A *generic element* in A is defined as $\sum_{i=1}^{D} T_i \omega_i$ in $A \otimes_k k(T_1, \ldots, T_D)$. This element depends on the choice of the basis Ω, but the degree of its minimal polynomial over $k(T_1, \ldots, T_D)$ depends only on A, as a standard linear algebra fact [37, Section 62] ensures that two similar matrices have the same minimal polynomial. As an illustration, consider the case $A = \mathbb{Q}[X_1, X_2]/(X_1^2, X_2^2)$. The minimal polynomial of a generic element has degree 3, but x_1, even though separating, has U^2 for minimal polynomial. The possible defects can be measured using the nil-indices of the local factors of A, see Section 6.

If $\mathcal{I}$ is a radical ideal, assumption 1 is obviously satisfied. Since k is perfect, a separating element is also primitive, so assumption 2 is also satisfied in this case.

Taking the above assumptions for granted, our main result is the following proposition:

Proposition 3 *Let u in A be a separating element of $\mathcal{I}$, such that the above assumptions are satisfied. Let v be in A, ℓ in $\widehat{A}$, and let $G_{u,\ell}$ and $G_{u,v\circ\ell}$ be the polynomials in $k[U]$ of degree less than that of m_u such that*

$$R(u, \ell) = \frac{G_{u,\ell}}{m_u}, \quad R(u, v \circ \ell) = \frac{G_{u,v\circ\ell}}{m_u}.$$

Then if m_u and $G_{u,\ell}$ are coprime, the following equality holds:

$$v = \frac{G_{u,v\circ\ell}(u)}{G_{u,\ell}(u)} \quad in \quad A_{\mathrm{red}}.$$

This proposition requires a few comments:

- If the condition on the degree of m_u is not satisfied, then the conclusion may become false for a generic linear form. Consider again $A = \mathbb{Q}[X_1, X_2]/(X_1^2, X_2^2)$ with basis $(1, x_1, x_2, x_1x_2)$, $u = x_1$, $v = x_2$, and let $\ell_1, \ell_{x_1}, \ell_{x_2}, \ell_{x_1x_2}$ be the coordinates of ℓ on the dual basis. A short calculation shows that
$$m_u = U^2, \quad R(x_1, \ell) = \frac{\ell_1 U + \ell_{x_1}}{U^2}, \quad R(x_1, x_2 \circ \ell) = \frac{\ell_{x_2} U + \ell_{x_1x_2}}{U^2};$$
so our formulæ would wrongly give the value $\ell_{x_1x_2}/\ell_{x_2}$ for x_2 instead of 0.
- In [60, Theorem 3.1], a similar result is proved for a particular linear form, the *trace*, which associates to any element v in A the trace of the multiplication map by v. For this particular form, the hypothesis on the degree of m_u is not required.
- If $\mathcal{I}$ is a radical ideal, a direct proof of Proposition 3 is the following: since k is a perfect field, the trace form generates $\widehat{A}$ as a A-module [4, 62]. The conclusion follows from [60, Theorem 3.1].

We defer the somewhat lengthy proof of Proposition 3 to the last section of the paper and we directly present our algorithm for computing rational parametrizations. It takes as input a linear form ℓ on A, an element u in A, its minimal polynomial m_u of degree δ_u, as well as the polynomial $G_{u,\ell}$ defined in Proposition 1.

Computing the parametrizations

Input: u in A, ℓ in $\widehat{A}$, m_u and $G_{u,\ell}$ in $k[U]$.
Output: a rational parametrization of the coordinates.

`for` j in $1, \dots, n$ `do`
  $c^{(j)} \leftarrow [(x_j \circ \ell)(1), (x_j \circ \ell)(u), \dots, (x_j \circ \ell)(u^{\delta_u - 1})]$;
  $C_j \leftarrow \sum_{i=0}^{\delta_u - 1} c_i^{(j)} U^{\delta_u - i - 1}$;
  $G_{u,x_j\circ\ell} \leftarrow m_u \cdot C_j$ quo U^{δ_u};
`return` $[\frac{G_{u,x_1\circ\ell}}{G_{u,\ell}}, \dots, \frac{G_{u,x_n\circ\ell}}{G_{u,\ell}}]$;

Proposition 4 *Under the hypotheses of Proposition 3, the output of the previous algorithm is a rational parametrization of the points in $\mathcal{V}(\mathcal{I})$. Besides the evaluation of the sequences*

$$[(x_j \circ \ell)(1), (x_j \circ \ell)(u), \dots, (x_j \circ \ell)(u^{\delta_u - 1})], \qquad j \in \{1, \dots, n\},$$

this algorithm requires at most $O(nD^2)$ additional operations in k.

Proof. We begin by recalling that the polynomial $G_{u,x_j \circ \ell}$ can be obtained as the quotient of $m_u \sum_{i=0}^{\delta_u - 1} (x_j \circ \ell)(u^i) U^{\delta_u - i - 1}$ by U^{δ_u}, where δ_u is the degree of m_u. We proved this fact in the third part of Proposition 1. The correctness of the above algorithm then follows from the formulæ in Proposition 3, applied to $v = x_j$, for $j = 1, \ldots, n$. The cost analysis is straightforward, since each polynomial multiplication has complexity at most quadratic in the degree $\delta_u \leq D$. $\square$

We point out that fast algorithms for polynomial multiplication would yield a linear complexity in D, up to logarithmic factors, but the bottleneck of this algorithm is the computation of the sequences $[(x_j \circ \ell)(1), (x_j \circ \ell)(u), \ldots, (x_j \circ \ell)(u^{\delta_u - 1})]$. We stress the fact that the probabilistic aspect of the output relies only on the correct computation of the minimal polynomial of u; see the previous subsection for more comments on this point.

3.3 Complexity estimates for the first approach

To put the algorithms of the previous subsections to practice, we must specify the operations in A. In this subsection, we assume that the *matrices of multiplication* by u and $x_1, \ldots, x_n$ are known and prove the first parts of Theorems 1 and 2.

The algorithm for a minimal polynomial is given in Subsection 3.1. The main task lies in computing the values

$$[\ell(1), \ell(u), \ldots, \ell(u^{2\delta - 1})],$$

δ being an *a priori* bound on the degree of m_u and ℓ a linear form on A. To compute the parametrizations corresponding to a separating element u, we first compute its minimal polynomial as above, then evaluate

$$[(x_j \circ \ell)(1), (x_j \circ \ell)(u), \ldots, (x_j \circ \ell)(u^{\delta_u - 1})], \quad j = 1, \ldots, n,$$

where $\delta_u \leq \delta$ is the degree of the minimal polynomial of u.

The other necessary operations and their complexity are given in Propositions 2 and 4, so we just need to detail the cost of the successive evaluations of respectively ℓ and $x_1 \circ \ell, \ldots, x_n \circ \ell$. For the moment, we follow a direct approach. All powers of u are computed, then the linear forms are evaluated on all of them. A more refined method is introduced in the next section.

- Using its multiplication matrix, one multiplication by u has cost $O(D^2)$ operations in k. Consequently, all the requested powers of u can be computed within $O(\delta D^2)$ operations in k.
- Given the linear form ℓ, each linear form $x_j \circ \ell$ can be computed using Lemma 1 since the matrix of multiplication by x_j is known. The total cost is thus within $O(nD^2)$ operations in k.
- The evaluation of a single linear form takes $O(D)$ operations in k. Evaluating all the linear forms on the powers of u requires respectively $O(\delta D)$ or $O(n\delta_u D)$ operations in k.

This gives respectively $O(\delta D^2)$ operations in k for the minimal polynomial, and $O(\delta D^2 + nD^2)$ for the parametrizations. The additional costs are given in Propositions 2 and 4. They fit into the complexity bounds $O(\delta D^2)$ and $O(\delta D^2 + nD^2)$. This concludes the complexity analysis.

Propositions 2 and 4 show that the output is correct whenever the polynomials $G_{u,\ell}$ and m_u are coprime. The last point in Proposition 1 shows that this is the case if and only if the coefficients of ℓ on the dual basis cancel a nonzero polynomial r_u of degree at most δ_u. Zippel-Schwartz's lemma (see [73, 65] and [71, Lemma 6.44]) concludes the probability analysis.

4 Speeding up the Power Projection

The algorithms presented in the previous section share the same basic subroutine: the evaluation of a linear form on the successive powers of an element in A. Their complexity fundamentally relies on the cost of this particular operation, called *power projection*.

Power Projection Problem. Let u be in A, ℓ in $\widehat{A}$ and $N > 0$. Compute the sequence $[\ell(1), \ell(u), \ldots, \ell(u^{N-1})]$.

The naive solution to this question used in the previous section requires to evaluate all the powers of u. In this section, we present a result given by Shoup in the univariate case [66, 67], which shows how to avoid the computations of all those powers, by a "transposition" of Paterson and Stockmeyer's fast evaluation algorithm [58]. This brings a speed-up of order $\sqrt{N}$ over the naive version.

This approach requires other operations than mere multiplications by u or x_i. Thus, we first state the complexity results in terms of the cost of product and transposed product in A, denoted respectively by $\mathcal{M}(A)$ and $\mathcal{M}^t(A)$. Next, we put these ideas to practice. For the time being, our effective version of the transposed product requires the whole multiplication table of the algebra A.

4.1 Baby step / giant step techniques

It is noted in [66, 67, 32] that the power projection problem itself is a transposition of the question of polynomial evaluation in A:

Polynomial Evaluation Problem. Let p be a polynomial in $k[T]$ of degree $N - 1$, and u in A. Compute $p(u)$.

For both questions, the point is to avoid the computation of *all* powers u^i, which would lead to a complexity of $O(N\mathcal{M}(A))$ operations in k. In [58], Paterson and Stockmeyer propose an algorithm for the polynomial evaluation problem (see also [12]) which saves a factor $\sqrt{N}$ using a baby step / giant step technique.

The idea underlying this process also applies to the power projection problem and yields the following algorithm, initially presented in [66] for the case $A = k[X]/(f)$. As in Paterson and Stockmeyer's, this algorithm takes as input two parameters k and k', which must satisfy $kk' \geq N$.

Power projection

Input: u in A, ℓ in $\widehat{A}$, N, k, k'.
Output: the sequence $[\ell(1), \ell(u), \ldots, \ell(u^{N-1})]$.

$u_i \leftarrow u^i, \ \ i = 0, \ldots, k$
`for` $i \leftarrow 0, \ldots, k'-1$ `do`
  $c_{ik+j} \leftarrow \ell(u_j), \ \ j = 0, \ldots, k-1$
  $\ell \leftarrow u_k \circ \ell$
`return` $[c_0, \ldots, c_{N-1}]$;

We encapsulate the complexity of this algorithm in the following proposition. A similar result is presented in [67].

Proposition 5 *Let u be in A, let ℓ be in $\widehat{A}$ and let $N > 0$. Then, the sequence*

$$[\ell(1), \ell(u), \ldots, \ell(u^{N-1})]$$

can be computed within $O\left(N^{1/2}(\mathcal{M}(A) + \mathcal{M}^t(A)) + ND\right)$ operations in k.

Proof. We take k and k' of the same magnitude, that is

$$k = \lfloor \sqrt{N} \rfloor, \quad k' = \lceil N/k \rceil,$$

where $\lfloor x \rfloor$ and $\lceil x \rceil$ respectively denote the largest integer less than or equal to x, and the smallest integer larger than or equal to x.

The precomputation of the first k powers of u requires $O(N^{1/2})$ multiplications in A. Each of the k' passes through the `for` loop requires the evaluation of k linear forms, plus a transposed multiplication. Since $kk' = O(N)$, the overall cost is thus $O(ND)$ operations for the evaluation of the linear forms and $O(N^{1/2})$ transposed multiplications. This proves the proposition. $\square$

Corollary 1 *Let D be the dimension of A as a k-vector space, and let u be in A. Let δ be a bound on the degree of the minimal polynomial of u. Then:*

- *The minimal polynomial of u can be computed by a probabilistic algorithm in $O\left(\delta^{1/2}(\mathcal{M}(A) + \mathcal{M}^t(A)) + \delta D\right)$ operations in k.*
- *If u is a separating element of $\mathcal{V}(\mathcal{I})$ such that the assumptions of Subsection 3.2 are satisfied, a parametrization of the algebraic variables can be computed in*

$$O\left(n\delta^{1/2}(\mathcal{M}(A) + \mathcal{M}^t(A)) + nD^2\right)$$

operations in k.

In both cases, the algorithm chooses D values in k. If these values are chosen in a finite subset Γ of k, all choices except at most $\delta|\Gamma|^{D-1}$ assure success.

Proof. The proof is similar to that of Subsection 3.3, the difference lies in the complexity analysis of the power projection. Proposition 5 brings the result, taking respectively $N = 2\delta$ for the minimal polynomial computation, and $N = \delta_u \leq \delta$ for the parametrizations. $\square$

Using the transposition principle, these complexity results could be rewritten in terms of $\mathcal{M}(A)$ only, but our explicit version reflects the underlying algorithm more closely.

4.2 Complexity estimates for the second approach

To put such algorithms to practice, we need an effective version of the transposed product. To this effect we suppose that the structure of the algebra A is given by a monomial basis *and* the corresponding multiplication tensor. This makes it possible to estimate the cost of the product and transposed product, which will conclude the proofs of Theorems 1 and 2.

More precisely, in the following paragraphs, we show that the costs of multiplication and transposed multiplication, denoted by $\mathcal{M}(A)$ and $\mathcal{M}^t(A)$ up to now, are in $O(2^n D^2)$ operations in k. With these results, the complexity estimates of Corollary 1 become respectively $O(2^n \delta^{1/2} D^2)$ and $O(n 2^n \delta^{1/2} D^2)$ operations in k, which concludes the proof of Theorems 1 and 2.

A note on Rouillier's algorithm. The input is now the same as that of [60]. Yet, Rouillier's algorithm uses a particular linear form, the trace. In the present context, computing the trace is straightforward, since we have precomputed the whole multiplication table. Thus, we can apply our baby step/giant step techniques to speed up the deterministic algorithm of [60]. Still, using random linear forms has its benefits; for instance, we may choose forms with many coefficients equal to zero.

To prove the estimates on the complexity of the operations in A and $\widehat{A}$, we recall and introduce some notation.

- We recall that $\Omega = \{\omega_i\}_{i=1,\dots,D}$ is a monomial basis of A, and that $E \subset \mathbb{N}^n$ is the corresponding set of exponents, so that $\Omega = x^E$.
- We denote by $\Omega \cdot \Omega$ the set of products $\{\omega_i \omega_j \mid \omega_i \in \Omega, \omega_j \in \Omega\}$. The corresponding set of exponents is denoted by $2E$, and is the Minkowski sum $E + E \subset \mathbb{N}^n$. Its cardinality is bounded by $2^n |E| = 2^n D$.
- We assume that the sets Ω and $\Omega \cdot \Omega$ are ordered; the elements of A will be given by their coefficients on the basis Ω. The multiplication tensor in A is given by a $|E| \times |2E|$ matrix $\mathbf{M}$, with rows indexed by the elements in Ω and columns indexed by the elements of $\Omega \cdot \Omega$. The columns of $\mathbf{M}$ give the coordinates of the element in $\Omega \cdot \Omega$ on the basis Ω.

Introducing the matrix $\mathbf{M}$ is a convenient way to describe the operations in A and $\widehat{A}$ and bound their complexity.

Multiplication in the quotient. We first give the cost of the multiplication in A. This operation is done in a straightforward manner. Two elements u and v in A are multiplied as polynomials in $k[X_1, \ldots, X_n]$, then reduced using the matrix $\mathbf{M}$.

In the algorithm below, u and v are given by the vectors $\mathbf{u}$ and $\mathbf{v}$ of their coefficients on the basis Ω. Given a vector $\mathbf{u}$ of size D and a monomial ω in Ω, $\mathbf{u}[\omega]$ denotes the entry of $\mathbf{u}$ corresponding to ω. The function $\texttt{Coefficients}(W, \Omega \cdot \Omega)$ returns the vector of the coefficients of W on the monomial family $\Omega \cdot \Omega$.

Multiplication in the quotient

Input: the coefficients of u, v in A, the matrix $\mathbf{M}$.
Output: the coefficients of the product uv in A.

$U \leftarrow \sum_{\omega \in \Omega} \mathbf{u}[\omega]\omega;$
$V \leftarrow \sum_{\omega \in \Omega} \mathbf{v}[\omega]\omega;$
$R \leftarrow UV;$ # the multiplication is done in $k[X_1, \ldots, X_n]$
$\mathbf{c}_W \leftarrow \texttt{Coefficients}(W, \Omega \cdot \Omega);$
$\texttt{return } \mathbf{M}\mathbf{c}_W;$

Given u and v in A, the previous algorithm computes the product uv in A within $O(2^n D^2)$ operations in k. Indeed, the naive multiplication of two polynomials with support in E requires $O(D^2)$ operations. The reduction of the product is done by the matrix-vector product, which requires $|E||2E| \leq 2^n |E|^2 = 2^n D^2$ operations in k.

Transposed multiplication. Our effective version of the transposed product was described at the end of Section 2. There, we reduced the transposed multiplication $u \circ \ell$ to two steps. First computing $S(\ell, 2E)$, that is, the values of ℓ on the elements of $\Omega \cdot \Omega$, then performing a multivariate series multiplication and extracting the required coefficients.

For any η in $\Omega \cdot \Omega$, the value $\ell(\eta)$ is the product between the row $\mathbf{c}_\ell$ of the coefficients of ℓ on the dual basis and the column of the coefficients of η on the basis Ω. In other words, the coefficients of $S(\ell, 2E)$ are the entries of the product $\mathbf{c}_\ell \mathbf{M}$.

This property yields the following algorithm for the transposed product. The linear form ℓ is given as the row-vector $\mathbf{c}_\ell$ of its coefficients on the dual basis. The other notation was introduced above.

Transposed multiplication in the quotient

Input: u in A, ℓ in $\widehat{A}$, the matrix $\mathbf{M}$.
Output: $u \circ \ell$ in $\widehat{A}$.

$\mathbf{d}_\ell \leftarrow \mathbf{c}_\ell \mathbf{M}$;
$S \leftarrow \sum_{\eta \in \Omega \cdot \Omega} \mathbf{d}_\ell[\eta] X^\eta$;
$T \leftarrow u(1/X_1, \ldots, 1/X_n) \cdot S$;
`return Coefficients`(T, Ω);

Given u in A and ℓ in $\widehat{A}$, the previous algorithm computes the transposed product $u \circ \ell$ within $O(2^n D^2)$ operations in k. Indeed, the matrix-vector product requires $|E||2E| \leq 2^n D^2$ operations in k. Using a naive series multiplication routine, the Laurent series product also requires $2^n D^2$ operations in k.

5 Experimental Results

System	1	2	3	4	5	6	7	8
Variables	3	4	6	7	3	4	3	4
Max. Degree	12	12	6	7	12	6	12	6
Solutions	30	192	156	962	1728	1296	1728	1296
Gröbner basis	1	4	4.5	309	0.2	0.2	6.2	170
Reconstruction	0.2	0.1	0.1	0.5	4	6	7	8

Algorithms of Section 3.3:

Mult. Matrices	0.1	2	1	6	3	4	5	30
Power Projection	0.4	3.6	3	57	695	763	700	1220
Total	0.5	5.6	4	63	698	767	705	1250

Algorithms of Section 4.2:

Mult. Table	0.2	2.5	1.5	80	24	54	403	1330
Power Projection	0.3	2.1	2.2	20	164	250	290	370
Total	0.5	4.6	3.7	100	188	304	693	1700

Fig. 1. Experimental Data; times are given in seconds

The algorithms underlying Theorems 1 and 2 have been implemented in the Magma computer algebra system [10]. In this section, we compare the methods presented respectively in Subsections 3.3 and 4.2, for the computation of a parametrization of the solutions of a polynomial system. Recall that the two methods differ by their input, respectively some multiplication matrices or the whole multiplication table, and by the computation of the power projection.

Since our complexity estimates are stated in terms of operations in the base field, we insist on computations on a finite field, where such operations have almost constant cost. Our base field is thus the finite field with 9001 elements.

The systems we have chosen are presented in Figure 1. All of them are complete intersection zero-dimensional systems. Systems 1 and 2 were proposed by S. Mallat for the design of foveal wavelets [47]. Systems 3 and 4 are the Cyclic systems [7] for $n = 6$ and $n = 7$. Systems 5 and 6 are sparse systems, with about 10 monomials of degree at most 4 per equation, and a single higher-degree monomial. Systems 7 and 8 are obtained by applying a linear change of variables on the previous systems.

- The first lines indicate the number of variables and the maximum degree of the input equations, then the dimension of the quotient algebra, that is the number of solutions counted with multiplicities.
- For all systems, the separating element is a randomly chosen linear combination of the variables, and the linear form has only 5 nonzero coefficients on the dual basis. In all cases, we find a minimal polynomial of degree the dimension of the quotient, so the output is correct.
- A basis for the quotient algebra is computed using Magma's `GroebnerBasis` function for a Graded Reverse Lexicographical order. Its computation time is given in the line labelled "Gröbner Basis". The line labelled "Reconstruction" gives the time necessary to perform all reconstruction operations, that is, Berlekamp Massey's algorithm and univariate polynomial multiplications. Their cost is detailed in Propositions 2 and 4, and is the same for both approaches.
- The computation times are next given for both approaches. For the algorithm of Section 3.3, this includes the computation of some multiplication matrices (using Magma's `RepresentationMatrix` function), then the naive version of the power projection. For the algorithm of Section 4.2, this includes the computation of the whole multiplication table, which enables a faster version of the power projection.

As was to be expected, the baby steps/giant steps techniques bring a consequent speed up over the naive version of the power projection. On the other hand, the precomputation of the whole multiplication table obviously affects this speed-up.

Systems 5 and 6 were chosen such that the Gröbner basis and the multiplication table were fast to compute. The advantage of using baby step/giant step techniques appears clearly for such examples.

Remark that the algorithm in [60] first requires to compute the whole multiplication table, then computes a power projection using the slower technique, i.e. without using the baby steps / giant steps techniques. The solutions we present here are certainly competitive with this approach.

6 Proof of Proposition 3

In this section, we prove Proposition 3. The data is a finite dimensional quotient algebra $A = k[X_1, \dots, X_n]/\mathcal{I}$ over a perfect field k, a separating element u in A and a linear form ℓ in $\widehat{A}$. Our assumptions are as follows:

Assumption 1 *The following conditions hold:*

- *the characteristic of k is zero or greater than $\min\{s, \sqrt{\mathcal{I}}^s \subset \mathcal{I}\}$;*
- *the degree of the minimal polynomial m_u of u equals the degree of the minimal polynomial of a generic element in A (see definition below);*
- *ℓ and u are such that*

$$R(u, \ell) := \sum_{i \geq 0} \frac{\ell(u^i)}{U^{i+1}} = \frac{G_{u,\ell}}{m_u},$$

with $G_{u,\ell}$ and m_u coprime (the definitions of the series R and the polynomial $G_{u,\ell}$ are given in Section 2).

Note that if $\mathcal{I}$ is a radical ideal, then the first two assumptions are satisfied as soon as u is a separating element, since in this case the degree of the minimal polynomial of u equals the dimension D of A. The number $\min\{s, \sqrt{\mathcal{I}}^s \subset \mathcal{I}\}$ is called the *exponent* of $\mathcal{I}$; it equals 1 if $\mathcal{I}$ is radical.

Our goal is to show that for every v in A and for every $\alpha \in \mathcal{V}(\mathcal{I})$,

$$\left(\frac{G_{u,v\circ\ell}}{G_{u,\ell}}\right)(u(\alpha)) = v(\alpha).$$

Recall the in the particular case when $\mathcal{I}$ is radical, we indicated, in the comments following Proposition 3, a quick proof of these formulæ. The rest of the paper is devoted to the proof in the general case. Since the arguments are a little involved, we divide their exposition in three parts. In Subsection 6.1 we relate the factorization of m_u and the exponents of the primary components of $\mathcal{I}$; the main result is Proposition 6, which is an analogue for minimal polynomials of a classical result on characteristic polynomials, sometimes referred to as Stickelberger's theorem [17, Proposition 2.7].

In Subsection 6.2 we rewrite the series $R(u, v \circ \ell)$ using a description of $\widehat{A}$ by differential conditions on the local factors of A. Finally, our knowledge of the factorization of m_u will make it possible to read out the required result on the new expression of $R(u, v \circ \ell)$ and to conclude in Subsection 6.3 the proof of Proposition 3.

6.1 Minimal polynomials of generic elements and local factors

Given the k-algebra $A = k[X_1, \dots, X_n]/\mathcal{I}$ and its basis $\Omega = (\omega_1, \dots, \omega_D)$, we recall that we call the *generic element* in A the element $T := \sum_{i=1}^{D} T_i \omega_i$ in

$A \otimes_k k(T_1, \ldots, T_D)$. We denote by m_T the minimal polynomial of T and by $\delta(A)$ the degree of m_T. The polynomial m_T depends on the choice of the basis Ω, but its degree depends only on A. The numbers $\delta(A_\alpha)$ will be used in the next paragraph, for some algebras A_α to be introduced. They are defined in the same manner.

Reduction to the case k algebraically closed. This first section encloses a result on transfer properties of ideals in polynomial algebras under extension from k to its algebraic closure $\overline{k}$. This result will serve to reduce the proof of Proposition 3 to the case when k algebraically closed.

In the lemma below, if $\mathcal{J}$ is an ideal in $k[X_1, \ldots, X_n]$, we denote by $\overline{\mathcal{J}}$ the ideal it generates in $\overline{k}[X_1, \ldots, X_n]$, that is, the set of all finite sums $\sum a_i f_i$, where $a_i \in \overline{k}[X_1, \ldots, X_n]$ and $f_i \in \mathcal{J}$. We will particularly focus on the ideal $\overline{\mathcal{I}}$, and we will denote $\overline{A} = \overline{k}[X_1, \ldots, X_n]/\overline{\mathcal{I}}$.

Lemma 2 *The following results hold:*

- *The ideal $\overline{\mathcal{I}}$ is zero-dimensional in $\overline{k}[X_1, \ldots, X_n]$ and $\dim_k A$ equals $\dim_{\overline{k}} \overline{A}$.*
- *The minimal polynomial over k of an element u in A coincides with the minimal polynomial of u as an element of $\overline{A}$ over $\overline{k}$.*
- *The degree of the minimal polynomial of a generic element in A equals the degree of the minimal polynomial of a generic element in $\overline{A}$.*
- *The exponent of $\overline{\mathcal{I}}$ equals the exponent of $\mathcal{I}$.*

Before starting the proof, we stress the fact that the first three points do not require that k is a perfect field, while for the last point, this hypothesis is crucial, as showed by the following example. Let k be the field $\mathbb{F}_p(Y)$ of rational functions over the finite field with p elements; then the polynomial $X^p - Y$ is square-free over k but not over $\overline{k}$, therefore the ideal it generates in $k[X]$ is radical, while its extension to $\overline{k}[X]$ is not.

Proof. The first assertion is a classical one, we refer to [34, Corollary 3.7.3] for a proof. The second and the third assertions are direct consequences of the fact that minimal polynomials are invariant under change of base ring, see for instance [39, Chapter XIV, Corollary 2.2].

It remains to prove the last assertion. We begin by showing that the operations of extending an ideal and taking the radical of an ideal commute, that is the ideals $\overline{\sqrt{\mathcal{I}}}$ and $\sqrt{\overline{\mathcal{I}}}$ are equal. Since $\sqrt{\mathcal{I}}$ contains $\mathcal{I}$ and extending ideals preserves inclusion, we have that $\overline{\mathcal{I}} \subset \overline{\sqrt{\mathcal{I}}}$. Since k is a perfect field, and $\sqrt{\mathcal{I}}$ is radical, [34, Proposition 3.7.18] shows that its extension $\overline{\sqrt{\mathcal{I}}}$ is also radical, so taking again radicals in $\overline{\mathcal{I}} \subset \overline{\sqrt{\mathcal{I}}}$, we obtain the first inclusion $\sqrt{\overline{\mathcal{I}}} \subset \overline{\sqrt{\mathcal{I}}}$. Let us now justify the converse inclusion $\overline{\sqrt{\mathcal{I}}} \subset \sqrt{\overline{\mathcal{I}}}$. Since $\overline{\mathcal{I}}$ contains $\mathcal{I}$ and taking radicals preserves inclusion, we have that $\sqrt{\mathcal{I}} \subset \sqrt{\overline{\mathcal{I}}}$. Thus any element y in $\overline{\sqrt{\mathcal{I}}}$ may be written as a finite sum $\sum_i a_i f_i$, for some polynomials a_i with coefficients in $\overline{k}$ and some f_i belonging to $\sqrt{\overline{\mathcal{I}}}$, so $y \in \sqrt{\overline{\mathcal{I}}}$. Thus, the equality of $\overline{\sqrt{\mathcal{I}}}$ and $\sqrt{\overline{\mathcal{I}}}$ is proved.

We finally prove the last assertion concerning the exponent preservation under extension to $\overline{k}$. By definition of the exponent, it is enough to show that $\sqrt{\mathcal{I}}^{\,s} \subset \mathcal{I}$ if and only if $\sqrt{\overline{\mathcal{I}}}^{\,s} \subset \overline{\mathcal{I}}$. For the direct assertion, suppose that $\sqrt{\mathcal{I}}^{\,s} \subset \mathcal{I}$. Taking extensions and using the property proved in the previous paragraph, we deduce $\sqrt{\overline{\mathcal{I}}}^{\,s} \subset \overline{\mathcal{I}}$. Conversely, suppose that $\sqrt{\overline{\mathcal{I}}}^{\,s} \subset \overline{\mathcal{I}}$. Intersecting both sides with $k[X_1, \ldots, X_n]$ (this operation is called *contraction*), we assert that we recover $\sqrt{\mathcal{I}}^{\,s} \subset \mathcal{I}$. In order to justify this, we use the fact that in polynomial algebras, extension followed by contraction of an ideal returns the initial ideal, see for instance [38, Chapter III, Proposition 7]. Indeed, this fact, in conjunction with the previous arguments implies the equalities $\mathcal{I} = k[X_1, \ldots, X_n] \cap \overline{\mathcal{I}}$ and $\sqrt{\mathcal{I}}^{\,s} = \sqrt{\overline{\mathcal{I}}}^{\,s} \cap k[X_1, \ldots, X_n]$, and this concludes the proof of our lemma. $\square$

In view of the previous lemma, we legitimately suppose, from now on, that k **is algebraically closed**.

Minimal polynomials of generic elements. The following lemma shows that over an algebraically closed field, the degree of the minimal polynomial of a generic element in A equals the maximal degree of all minimal polynomials of elements in A. We point out that this result applies to any algebra of finite dimension, and will be used for the algebras A_α introduced in the next paragraph.

Lemma 3 *For every t in A, $\deg m_t \leq \delta(A)$, and there exists t in A such that $\deg m_t = \delta(A)$. In other words, $\delta(A) = \max_{t \in A}(\deg m_t)$.*

Proof. Let B be $A \otimes_k k(T_1, \ldots, T_D)$ and let $T \in B$ be $\sum_{i=1}^{D} T_i \omega_i$. The k-basis Ω of A is also a $k(T_1, \ldots, T_D)$-basis of B. We define $\mathbf{M}_T$ as the matrix of multiplication by T in this basis; then $m_T(\mathbf{M}_T) = 0$.

Let t be in A; t can be written $\sum_{i=1}^{D} t_i \omega_i$. Both $\mathbf{M}_T$ and m_T have their coefficients in $k[T_1, \ldots, T_D]$, so the equality $m_T(\mathbf{M}_T) = 0$ can be specialized at $(t_1, \ldots, t_D)$. The matrix $\mathbf{M}_T$ specializes into the multiplication matrix of t in A, which shows that $\deg m_t \leq \deg m_T = \delta(A)$.

Consider now the $D \times \delta(A)$ matrix whose columns contain the coefficients of $T^0, \ldots, T^{\delta(A)-1}$ on the basis Ω. This matrix has entries that are polynomial in $(T_1, \ldots, T_D)$, and has maximal rank, so admits a $\delta(A) \times \delta(A)$ submatrix with nonzero determinant $\mathcal{D} \in k[T_1, \ldots, T_D]$.

Since k is algebraically closed, there exists a D-tuple $(t_1, \ldots, t_D)$ which does not cancel $\mathcal{D}$. Then the first $\delta(A) - 1$ powers of $t = \sum_{i=1}^{D} t_i \omega_i$ are independent over k, so the minimal polynomial of t has degree $\delta(A)$. $\square$

Minimal polynomials and local factors. Let $u \in A$ be an element of A, whose minimal polynomial m_u has degree $\delta(A)$, the degree of the minimal polynomial of a generic element in A. The aim of the rest of this section is to describe the factorization properties of the polynomial m_u.

Since k is algebraically closed, each zero α of $\mathcal{I}$ is in k^n. Moreover, if we let $\mathfrak{m}_\alpha \subset k[X_1, \ldots, X_n]$ be the maximal ideal at α, then the primary decomposition of the zero-dimensional ideal $\mathcal{I}$ has the form:

$$\mathcal{I} = \bigcap_{\alpha \in \mathcal{V}(\mathcal{I})} \mathcal{I}_\alpha,$$

where $\mathcal{I}_\alpha$ is a $\mathfrak{m}_\alpha$-primary ideal.

We write A_α for the local algebra $k[X_1, \ldots, X_n]/\mathcal{I}_\alpha$ and denote by N_α the exponent of $\mathcal{I}_\alpha$, that is the minimal s such that $\mathfrak{m}_\alpha^s \subset \mathcal{I}_\alpha$. This is also the nil-index of the local algebra A_α.

The main result of this section shows that under Assumption 1, the minimal polynomial of u equals

$$m_u = \prod_{\alpha \in \mathcal{V}(\mathcal{I})} \big(U - u(\alpha)\big)^{N_\alpha}.$$

This fact is crucial in proving Proposition 3; we divide its proof into several lemmas.

Lemma 4 *Suppose $u \in A$ has minimal polynomial m_u of degree $\delta(A)$. Then the minimal polynomial of u is given by*

$$m_u = \prod_{\alpha \in \mathcal{V}(\mathcal{I})} \big(U - u(\alpha)\big)^{\delta(A_\alpha)}.$$

Proof. By the Chinese Remainder Theorem, A is isomorphic to the product $\prod_\alpha A_\alpha$. We denote by u_α the images of u in A_α under this isomorphism. Let us show that the minimal polynomial of u equals the least common multiple of the minimal polynomials m_{u_α}.

For any polynomial P, the image in A_α of the element $P(u)$ under the Chinese isomorphism is $P(u_\alpha)$. Since $m_u(u) = 0$, this implies that $m_u(u_\alpha) = 0$ for all α, therefore all m_{u_α} divide m_u. Conversely, let m be a polynomial divisible by all m_{u_α}. It follows that $m(u_\alpha) = 0$ for all α, so $m(u) = 0$. Thus, m_u divides m and this proves that m_u is the lcm of m_{u_α}. As a consequence, we have the inequality

$$\delta(A) \leq \sum_\alpha \deg m_{u_\alpha} \leq \sum_\alpha \delta(A_\alpha). \tag{3}$$

We next show that for all α, the polynomial m_{u_α} has the form $\big(T - u(\alpha)\big)^{s_\alpha}$, for some integer $1 \leq s_\alpha \leq N_\alpha$. Since it vanishes on α, the element $u_\alpha - u(\alpha)$ belongs to the radical $\mathfrak{m}_\alpha$ of $\mathcal{I}_\alpha$. It follows that the element $\big(u_\alpha - u(\alpha)\big)^{N_\alpha}$ belongs to $\mathcal{I}_\alpha$, thus is zero in the quotient A_α. Therefore, m_{u_α} divides $\big(T - u(\alpha)\big)^{N_\alpha}$, hence it has the form $\big(U - u(\alpha)\big)^{s_\alpha}$. Since m_u equals their lcm, it has the form $m_u = \prod_\alpha \big(U - u(\alpha)\big)^{r_\alpha}$.

We show now that $r_\alpha = \delta(A_\alpha)$, for all α. Using Lemma 3 for each α in $\mathcal{V}(\mathcal{I})$, we choose elements t_α in A_α such that the degree of the minimal polynomial of t_α is $\delta(A_\alpha)$. The previous paragraph shows that, up to adding well-chosen constants to the t_α, we can assure that their minimal polynomials are pairwise coprime. Let $t \in A$ be such that its images in the local algebras A_α are the elements t_α. Then the minimal polynomial of t is the product $\prod_\alpha m_{t_\alpha}$, so its degree is $\sum_\alpha \delta(A_\alpha)$. Thus:

$$\sum_\alpha \delta(A_\alpha) \leq \delta(A). \tag{4}$$

Combining the inequalities (3) and (4) with the fact that $\delta(A) = \deg m_u$ equals $\sum_\alpha r_\alpha$, we conclude that $r_\alpha = \delta(A_\alpha)$, for all α, so m_u has the desired form. $\square$

The next lemma relates the degree $\delta(A_\alpha)$ to the local exponents N_α. We point out that this result depends on the characteristic of the base field k.

Lemma 5 *Let $a = (a_1, \ldots, a_n) \in k^n$, let $\mathcal{J}$ be a $(X_1 - a_1, \ldots, X_n - a_n)$-primary ideal of $k[X_1, \ldots, X_n]$, let $N_\mathcal{J}$ be the exponent of $\mathcal{J}$ and let $A_\mathcal{J}$ be $k[X_1, \ldots, X_n]/\mathcal{J}$. If the characteristic of k is zero or greater than $N_\mathcal{J} - 1$ then $\delta(A_\mathcal{J}) = N_\mathcal{J}$.*

Proof. Up to a translation, we may assume that the point a is the origin of k^n and that the ideal $\mathcal{J}$ is $(X_1, \ldots, X_n)$-primary.

Let $D_\mathcal{J}$ be the dimension of $A_\mathcal{J}$ and $\beta_1, \ldots, \beta_{D_\mathcal{J}}$ be a monomial basis of $A_\mathcal{J}$. We suppose that $\beta_1 = 1$. By Lemma 3, we can choose $t := \sum_{i=1}^{D_\mathcal{J}} t_i \beta_i$ such that $\deg m_t = \delta(A_\mathcal{J})$. Then $t - t_1$ is in $(X_1, \ldots, X_n)$, so $(t - t_1)^{N_\mathcal{J}} = 0$. This shows that the degree of the minimal polynomial of t is at most $N_\mathcal{J}$, i.e. $\delta(A_\mathcal{J}) \leq N_\mathcal{J}$.

By assumption, there exists a monomial M of total degree $N_\mathcal{J} - 1$ which is not in $\mathcal{J}$. Without loss of generality, M can be written $\prod_{i=1}^d X_i^{\alpha_i}$ for some integer $1 \leq d \leq D_\mathcal{J}$ and some positive integers α_i, of sum $N_\mathcal{J} - 1$. We let t be $\sum_{i=1}^d X_i$. The coefficient of M in $t^{N_\mathcal{J}-1}$ is

$$\frac{(N_\mathcal{J} - 1)!}{\alpha_1! \cdots \alpha_d!},$$

which is well-defined and nonzero since the characteristic of k is either zero or greater than $N_\mathcal{J} - 1$. Consequently, $t^{N_\mathcal{J}-1}$ is not zero, so the minimal polynomial of t is $T^{N_\mathcal{J}}$. This shows that $N_\mathcal{J} \leq \delta(A_\mathcal{J})$. The converse inequality follows from the first part of Lemma 4. This concludes the proof. $\square$

To apply this result to each local factor, we need to ensure that the characteristic of k is indeed greater than the exponents of the local factors. This is the objective of the next lemma.

Lemma 6 *The exponent of $\mathcal{I}$ equals* $\max_{\alpha \in \mathcal{V}(\mathcal{I})} N_\alpha$.

Proof. Let S be the exponent of $\mathcal{I}$ and N be $\max_{\alpha\in\mathcal{V}(\mathcal{I})} N_\alpha$. Then $\sqrt{\mathcal{I}}^N$ is $\prod_\alpha \mathfrak{m}_\alpha^N$, which is contained in $\prod_\alpha \mathcal{I}_\alpha = \mathcal{I}$, so $S \le N$. Conversely, for any α in $\mathcal{V}(\mathcal{I})$, we have

$$\mathcal{I}_\alpha + \prod_{\alpha'\neq\alpha} \mathfrak{m}_{\alpha'}^S = (1).$$

Multiplying both sides by $\mathfrak{m}_\alpha^S$ yields

$$\mathfrak{m}_\alpha^S \mathcal{I}_\alpha + \prod_{\alpha'\in\mathcal{V}(\mathcal{I})} \mathfrak{m}_{\alpha'}^S = \mathfrak{m}_\alpha^S.$$

Now S is such that $\sqrt{\mathcal{I}}^S \subset \mathcal{I}$, so $\prod_{\alpha'\in\mathcal{V}(\mathcal{I})} \mathfrak{m}_{\alpha'}^S \subset \mathcal{I} \subset \mathcal{I}_\alpha$. The previous equality then shows that $\mathfrak{m}_\alpha^S \subset \mathcal{I}_\alpha$, for each α, hence $S \ge N$. $\square$

The following proposition summarizes the results of this section.

Proposition 6 *Let u be in A, such that the degree of its minimal polynomial m_u equals the degree of the minimal polynomial of a generic element in A. If furthermore the characteristic of k is zero or greater than the exponent of $\mathcal{I}$, then the polynomial m_u factorizes as*

$$m_u = \prod_{\alpha\in\mathcal{V}(\mathcal{I})} \big(U - u(\alpha)\big)^{N_\alpha}.$$

Proof. By assumption and using Lemma 6, we are in position to apply Lemma 5 on each local factor A_α. Together with Lemma 4, this gives the result. $\square$

6.2 High order derivations, dual spaces and generating series

In this section, we recall the notion of *high order derivations* and exhibit their connection with the dual spaces of quotient algebras. We also give a description of some generating series of the type $R(u, \ell)$ which are built upon such derivations.

Basic facts. We start by recalling the notion of high order derivation over an algebra, introduced in [57, 55]. Let k be an arbitrary field and R be a k-algebra. A k-linear map $d : R \to R$ is called a *k-derivation of order 1* if $d(xy) = xd(y) + yd(x)$, for all x and y in R. High order derivations are defined recursively. A k-linear map $d : R \to R$ is called a *k-derivation of order $N > 1$* if the map $[d, x] : y \mapsto d(xy) - xd(y) - yd(x)$ is a k-derivation of order $N - 1$ for all $x \in R$. For $N \ge 1$, we write $\mathrm{Der}_k^N(R)$ for the k-vector space of all k-derivations of order N, and we take $\mathrm{Der}_k^0(R) = k \cdot 1_R$. One can easily show that $d(1) = 0$ for any derivation d of order at least 1 and that $\mathrm{Der}_k^N(R) \subset \mathrm{Der}_k^{N+1}(R)$ for all $N \ge 1$, see [8, Section 1]. These two basic properties will be implicitly used in the proofs below.

In the particular case $R = k[X_1, \ldots, X_n]$, the k-linear map $\delta^v : R \to R$ defined on the monomial basis by:

$$\delta^v : X_1^{\mu_1} \cdots X_n^{\mu_n} \mapsto \binom{\mu_1}{v_1} \cdots \binom{\mu_n}{v_n} X_1^{\mu_1 - v_1} \cdots X_n^{\mu_n - v_n}$$

is a k-derivation in $\mathrm{Der}^{|v|}(R)$, with $|v| = v_1 + \cdots + v_n$. Remark that the binomial coefficient $\binom{\beta}{\alpha}$ is defined over any field, for instance as the coefficient of Y^α in $(1+Y)^\beta$. If k has characteristic zero, then we recover the well-known definition of differential operators:

$$\delta^v(P) = \frac{1}{v_1! \cdots v_n!} \frac{\partial^{v_1 + \cdots + v_n}(P)}{\partial_{X_1}^{v_1} \cdots \partial_{X_n}^{v_n}}.$$

Dual spaces and high order derivations. We next exhibit the connection between high order derivations and dual spaces of quotient algebras. The idea to characterize primary ideals by differential conditions in characteristic zero is due to Gröbner [29]. Similar or more general treatment can be found in [48, 50, 8, 56]. For the sake of completeness, we gather in the following lemma the needed facts, in *arbitrary* characteristic. Our proof is inspired by that of [8, Proposition 3.2].

Lemma 7 *Let $a = (a_1, \ldots, a_n) \in k^n$, let $\mathcal{J}$ be a $(X_1 - a_1, \ldots, X_n - a_n)$-primary ideal of $R = k[X_1, \ldots, X_n]$ and let $N_{\mathcal{J}}$ be the exponent of $\mathcal{J}$. Then there exists a k-basis of the dual $\widehat{R/\mathcal{J}}$ consisting of elements*

$$L_i : P + \mathcal{J} \longmapsto (D_i P)(a),$$

where D_1 is the identity map and with D_i in $\mathrm{Der}_k^{N_{\mathcal{J}}-1}(R)$ for $i > 1$.

Proof. Up to a translation, we assume, without loss of generality, that the point a is the origin of k^n and that the ideal $\mathcal{J}$ is $(X_1, \ldots, X_n)$-primary. If v is a multi-index with $|v| < N_{\mathcal{J}}$, the k-linear map $R \to k$ given by $P \mapsto (\delta^v P)(0)$ factors to a k-linear map $\delta_*^v : R/(X_1, \ldots, X_n)^{N_{\mathcal{J}}} \to k$ and the induced maps $\{\delta_*^v\}_{|v| < N_{\mathcal{J}}}$ form the dual k-basis of the monomial basis $\{x^\mu\}_{|\mu| < N_{\mathcal{J}}}$ of $R/(X_1, \ldots, X_n)^{N_{\mathcal{J}}}$.

The dual of $R/\mathcal{J}$ is a k-linear subspace of the dual of $R/(X_1, \ldots, X_n)^{N_{\mathcal{J}}}$, which contains δ_*^0. Thus, it admits a k-basis whose elements are of the form $L_1 = \delta_*^0$ and $L_i = \sum_{0 < |v| < N_{\mathcal{J}}} b_v^{(i)} \delta_*^v$ for $i > 1$. We take D_1 as the identity map and, for $i > 1$, $D_i = \sum_{0 < |v| < N_{\mathcal{J}}} b_v^{(i)} \delta^v$, so that $D_i \in \mathrm{Der}_k^{N_{\mathcal{J}}-1}(R)$. This proves the lemma. $\square$

High order derivations and generating series. The following result makes a link between the poles of the rational series $R(u, \ell)$ introduced in Proposition 1 and the order of a derivation.

Lemma 8 *Let $N \geq 0$, R be a k-algebra, $u \in R$ and D in $\mathrm{Der}^N(R)$. Then there exists c in R such that, for every $v \in R$, there exist N elements c_j in R such that the following equality holds in $R[[U^{-1}]]$:*

$$\sum_{i\geq 0} \frac{D(vu^i)}{U^{i+1}} = \frac{cv}{(U-u)^{N+1}} + \sum_{j=1}^{N} \frac{c_j}{(U-u)^j}.$$

Proof. We proceed by induction on N. We begin by considering the case $N=0$, that is, D is the multiplication map by a certain element r in R. We have that

$$\sum_{i\geq 0} \frac{D(vu^i)}{U^{i+1}} = rv \sum_{i\geq 0} \frac{u^i}{U^{i+1}} = \frac{rv}{U-u},$$

so this series has the desired form.

We treat now the inductive step. Let $N \geq 1$; we suppose the lemma is true for index $N-1$ and we prove it for index N. Let thus D be an arbitrary derivation in $\mathrm{Der}^N(R)$. By definition, we have the formula $D(vu^i) = [D,v](u^i) + vD(u^i) + u^i D(v)$, so

$$\sum_{i\geq 0} \frac{D(vu^i)}{U^{i+1}} = \sum_{i\geq 0} \frac{[D,v](u^i)}{U^{i+1}} + v \sum_{i\geq 0} \frac{D(u^i)}{U^{i+1}} + D(v) \sum_{i\geq 0} \frac{u^i}{U^{i+1}}. \tag{5}$$

We analyze each term in this sum separately. Since $[D,v]$ belongs to $\mathrm{Der}^{N-1}(R)$, the induction hypothesis shows that

$$\sum_{i\geq 0} \frac{[D,v](u^i)}{U^{i+1}} = \frac{c'}{(U-u)^N} + \sum_{j=1}^{N-1} \frac{c'_j}{(U-u)^j}$$

for some elements c' and c'_j in R. Using the fact that $D(u^i) = [D,u](u^{i-1}) + uD(u^{i-1}) + u^{i-1}D(u)$, it is easy to derive the formula

$$\sum_{i\geq 0} \frac{D(u^i)}{U^{i+1}} = \frac{1}{U-u} \sum_{i\geq 0} \frac{[D,u](u^i)}{U^{i+1}} + \frac{D(u)}{(U-u)^2}.$$

By the inductive hypothesis, the second term in the sum (5) is thus equal to

$$\frac{v}{U-u} \left(\frac{c''}{(U-u)^N} + \sum_{j=1}^{N-1} \frac{c''_j}{(U-u)^j} + \frac{D(u)}{(U-u)} \right),$$

for some elements c'' and c''_j in R depending *only* on D and u. Finally, the third term in the sum (5) obviously equals

$$D(v) \sum_{i\geq 0} \frac{u^i}{U^{i+1}} = \frac{D(v)}{U-u}.$$

Putting these pieces all together in sum (5) completes the proof. $\square$

6.3 Conclusion

The final step of the proof consists in rewriting the series $R(u, v \circ \ell)$ so as to exhibit its dependence with respect to v. Lemma 7 shows that for each $\alpha \in \mathcal{V}(\mathcal{I})$ there exists a family of derivations $\Delta^\alpha = \{D_j^\alpha\}_{j=1,\ldots,\dim_k(A_\alpha)}$, such that the functionals

$$L_j^\alpha : P + \mathcal{I}_\alpha \mapsto D_j^\alpha(P)(\alpha)$$

form a k-basis of $\widehat{A_\alpha}$. Furthermore, $D_1^\alpha = 1$ and for $j > 1$, D_j^α belongs in $\mathrm{Der}^{N_\alpha - 1}(k[X_1, \ldots, X_n])$. Using Lemma 8 and evaluating at α, we see that there exist c_j^α in k, and, for every $v \in k[X_1, \ldots, X_n]$, some elements $(c_{j,i}^\alpha)_{1 \le i < N}$ in k such that

$$R(u, v \circ L_1^\alpha) = \sum_{i \ge 0} \frac{(vu^i)(\alpha)}{U^{i+1}} = \frac{v(\alpha)}{U - u(\alpha)} \tag{6}$$

and, for $j > 1$,

$$R(u, v \circ L_j^\alpha) = \sum_{i \ge 0} \frac{D_j^\alpha(vu^i)(\alpha)}{U^{i+1}} = \frac{v(\alpha) c_j^\alpha}{(U - u(\alpha))^{N_\alpha}} + \sum_{i=1}^{N_\alpha - 1} \frac{c_{j,i}^\alpha}{(U - u(\alpha))^j} \tag{7}$$

hold in $k[[U^{-1}]]$.

Let now ℓ be in $\widehat{A}$. Since the union $\cup_\alpha \Delta^\alpha$ forms a k-basis of $\widehat{A}$, and using the linearity of $R(u, v \circ \ell)$ with respect to ℓ, equations (6) and (7) show that for every v the equality

$$R(u, v \circ \ell) = \sum_{\alpha \in \mathcal{V}(\mathcal{I})} \frac{v(\alpha) c_\alpha}{(U - u(\alpha))^{N_\alpha}} + \sum_{\alpha \in \mathcal{V}(\mathcal{I})} \sum_{j=1}^{N_\alpha - 1} \frac{c_j^\alpha}{(U - u(\alpha))^j} \tag{8}$$

holds, where c_α and c_j^α belong to k, and c_α does not depend on v. If one of the coefficients c_α were zero, then for any v, $R(u, v \circ \ell)$ could be written with a denominator of degree less than $\sum_\alpha N_\alpha$, that is, of degree less than $\deg m_u$, by Proposition 6. In particular, for $v = 1$, $R(u, \ell)$ would admit a denominator of degree less than $\deg m_u$. Since, by Assumption 1, ℓ is such that

$$R(u, \ell) = \frac{G_{u,\ell}}{m_u},$$

with $G_{u,\ell}$ and m_u coprime, none of the coefficients c_α can be zero.

Recall that by Proposition 6, the polynomial m_u writes as

$$m_u = \prod_{\alpha \in \mathcal{V}(\mathcal{I})} \left(U - u(\alpha)\right)^{N_\alpha}.$$

Let Q_α be the quotient of m_u by $(U - u(\alpha))^{N_\alpha}$, so that Q_α takes a nonzero value on $u(\alpha)$. Using equation (8), we deduce that for any v, there exists a polynomial

$V_v \in k[U]$ such that

$$G_{u,v\circ\ell} = m_u R(u, v\circ\ell) = \sum_{\alpha\in\mathcal{V}(\mathcal{I})} v(\alpha)c_\alpha Q_\alpha(U) + V_v(U) \prod_{\alpha\in\mathcal{V}(\mathcal{I})} (U - u(\alpha)).$$

This implies that $G_{u,v\circ\ell}(u(\alpha))$ equals $v(\alpha)c_\alpha Q_\alpha(u(\alpha))$. Since $c_\alpha Q_\alpha(u(\alpha))$ is not zero and is independent from v, this shows that $\frac{G_{u,v\circ\ell}}{G_{u,\ell}}$ takes the value $v(\alpha)$ at $u(\alpha)$. This proves the proposition.

References

1. M.-E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeros, multiplicities, and idempotents for zero-dimensional systems. In *Algorithms in algebraic geometry and applications (Santander, 1994)*, pages 1–15. Birkhäuser, Basel, 1996.
2. A. Antoniou. *Digital Filters: Analysis and Design.* McGraw-Hill Book Co., 1979.
3. J.-M. Arnaudiès and A. Valibouze. Lagrange resolvents. *Journal of Pure and Applied Algebra*, 117/118:23–40, 1997. Algorithms for algebra (Eindhoven, 1996).
4. E. Becker, J. P. Cardinal, M.-F. Roy, and Z. Szafraniec. Multivariate Bezoutians, Kronecker symbol and Eisenbud-Levine formula. In *Algorithms in algebraic geometry and applications (Santander, 1994)*, pages 79–104. Birkhäuser, Basel, 1996.
5. E. Becker and T. Wörmann. Radical computations of zero-dimensional ideals and real root counting. *Mathematics and Computers in Simulation*, 42(4-6):561–569, 1996. Symbolic computation, new trends and developments (Lille, 1993).
6. E. R. Berlekamp. *Algebraic coding theory.* McGraw-Hill Book Co., New York, 1968.
7. G. Björck. Functions of modulus 1 on Z_n whose Fourier transforms have constant modulus, and "cyclic n-roots". In *Recent advances in Fourier analysis and its applications (Il Ciocco, 1989)*, volume 315 of *NATO Advance Science Institutes Series C: Mathematical and Physical Sciences*, pages 131–140. Kluwer Academic Publishers, Dordrecht, 1990.
8. R. Bommer. High order derivations and primary ideals to regular prime ideals. *Archiv der Mathematik*, 46(6):511–521, 1986.
9. J. L. Bordewijk. Inter-reciprocity applied to electrical networks. *Appl. Sci. Res. B*, 1:1–74, 1956.
10. W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *Journal of Symbolic Computation*, 24(3-4):235–265, 1997. See also `http://www.maths.usyd.edu.au:8000/u/magma/`.
11. A. Bostan, G. Lecerf, and É. Schost. Tellegen's principle into practice. In *Symbolic and Algebraic Computation*, 2003. Proceedings ISSAC'03, Philadelphia, August 2003. To appear.
12. R. P. Brent and H. T. Kung. Fast algorithms for manipulating formal power series. *Journal of the ACM*, 25(4):581–595, October 1978.
13. B. Buchberger. Gröbner bases: An algorithmic method in polynomial ideal theory. In *Multidimensional System Theory*, pages 374–383. Reidel, Dordrecht, 1985.
14. P. Bürgisser, M. Clausen, and A. Shokrollahi. *Algebraic Complexity Theory.* Springer, 1997.
15. L. S. Charlap, R. Coley, and D. Robbins. Enumeration of rational points on elliptic curves over finite fields. Preprint, 1991.

16. D. Coppersmith and S. Winograd. Matrix multiplication via arithmetic progressions. *Journal of Symbolic Computation*, 9(3):251–280, March 1990.
17. D. Cox, J. Little, and D. O'Shea. *Using algebraic geometry.* Springer-Verlag, New York, 1998.
18. D. Eisenbud. *Commutative algebra, with a view toward algebraic geometry.* Graduate Texts in Mathematics. Springer-Verlag, New York, 1995.
19. J.-C. Faugère. A new efficient algorithm for computing Gröbner bases (F_4). *Journal of Pure and Applied Algebra*, 139(1-3):61–88, 1999. Proceedinds of MEGA'98.
20. J.-C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.
21. C. M. Fiduccia. On obtaining upper bounds on the complexity of matrix multiplication. In *Complexity of computer computations (Proc. Sympos., IBM Thomas J. Watson Res. Center, Yorktown Heights, N.Y., 1972)*, pages 31–40, 187–212. Plenum, New York, 1972.
22. C. M. Fiduccia. *On the algebraic complexity of matrix multiplication*. PhD thesis, Brown Univ., Providence, RI, Center Comput. Inform. Sci., Div. Engin., 1973.
23. P. Gaudry. *Algorithmique des courbes hyperelliptiques et applications à la cryptologie.* PhD thesis, École polytechnique, 2000.
24. P. Gaudry and É. Schost. Modular equations for hyperelliptic curves. Technical report, École polytechnique, 2002.
25. M. Giusti, J. Heintz, K. Hägele, J. E. Morais, L. M. Pardo, and J. L. Montaña. Lower bounds for Diophantine approximations. *Journal of Pure and Applied Algebra*, 117/118:277–317, 1997. Algorithms for algebra (Eindhoven, 1996).
26. M. Giusti, J. Heintz, J. E. Morais, J. Morgenstern, and L. M. Pardo. Straight-line programs in geometric elimination theory. *Journal of Pure and Applied Algebra*, 124:101–146, 1998.
27. M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *Journal of Complexity*, 17(1):154–211, 2001.
28. R. Göttfert and H. Niederreiter. On the minimal polynomial of the product of linear recurring sequences. *Finite Fields and their Applications*, 1(2):204–218, 1995. Special issue dedicated to Leonard Carlitz.
29. W. Gröbner. La théorie des idéaux et la géométrie algébrique. In *Deuxième Colloque de Géométrie Algébrique, Liège, 1952*, pages 129–144. Georges Thone, Liège, 1952.
30. J. Hopcroft and J. Musinski. Duality applied to the complexity of matrix multiplication and other bilinear forms. *SIAM Journal on Computing*, 2, 1973.
31. E. Kaltofen. Analysis of Coppersmith's block Wiedemann algorithm for the parallel solution of sparse linear systems. *Mathematics of Computation*, 64(210):777–806, 1995.
32. E. Kaltofen, R. M. Corless, and D. J. Jeffrey. Challenges of symbolic computation: my favorite open problems. *Journal of Symbolic Computation*, 29(6):891–919, 2000.
33. M. Kaminski, D.G. Kirkpatrick, and N.H. Bshouty. Addition requirements for matrix and transposed matrix products. *J. Algorithms*, 9(3):354–364, 1988.
34. M. Kreuzer and L. Robbiano. *Computational commutative algebra. 1.* Springer-Verlag, Berlin, 2000.
35. L. Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *Journal für die reine und angewandte Mathematik*, 92:1–122, 1882.
36. E. Kunz. *Kähler differentials.* Vieweg advanced lectures in Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 1986.

37. A. Kurosh. *Cours d'algèbre supérieure.* Éditions Mir, Moscou, 1973.
38. S. Lang. *Introduction to algebraic geometry.* Interscience Publishers, New York, 1958.
39. Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, third edition, 2002.
40. D. Lazard. Solving zero-dimensional algebraic systems. *Journal of Symbolic Computation*, 13:117–133, 1992.
41. D. Lazard and A. Valibouze. Computing subfields: reverse of the primitive element problem. In *Computational algebraic geometry (Nice, 1992)*, pages 163–176. Birkhäuser Boston, Boston, MA, 1993.
42. G. Lecerf. *Une alternative aux méthodes de réécriture pour la résolution des systèmes algébriques.* PhD thesis, École polytechnique, 2001.
43. G. Lecerf. Quadratic Newton iteration for systems with multiplicity. *Journal of FoCM*, 2(3):247–293, 2002.
44. G. Lecerf. Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. *Journal of Complexity*, 2003. To appear.
45. J. Little. A key equation and the computation of error values for codes from order domains. Available at http://arXiv.org/math.AC/0303299, 2003.
46. F. S. Macaulay. *The Algebraic Theory of Modular Systems.* Cambridge University Press, 1916.
47. S. Mallat. Foveal detection and approximation for singularities. *Applied and Computational Harmonic Analysis*, 2003. To appear.
48. M. G. Marinari, T. Mora, and H. M. Möller. Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *Applicable Algebra in Engineering, Communication and Computing*, 4(103–145), 1993.
49. J. L. Massey. Shift-register synthesis and BCH decoding. *IEEE Transactions on Information Theory*, IT-15:122–127, 1969.
50. B. Mourrain. Isolated points, duality and residues. *Journal of Pure and Applied Algebra*, 117/118:469–493, 1997. Algorithms for algebra (Eindhoven, 1996).
51. B. Mourrain and V. Y. Pan. Solving special polynomial systems by using structured matrices and algebraic residues. In *Foundations of computational mathematics (Rio de Janeiro, 1997)*, pages 287–304. Springer, Berlin, 1997.
52. B. Mourrain and V. Y. Pan. Asymptotic acceleration of solving multivariate polynomial systems of equations. In *Proceedings STOC*, pages 488–496. ACM Press, 1998.
53. B. Mourrain and V. Y. Pan. Multivariate polynomials, duality, and structured matrices. *Journal of Complexity*, 16(1):110–180, 2000.
54. B. Mourrain, V. Y. Pan, and O. Ruatta. Accelerated solution of multivariate polynomial systems of equations. *SIAM Journal on Computing*, 32(2):435–454, 2003.
55. Y. Nakai. High order derivations. I. *Osaka Journal of Mathematics*, 7:1–27, 1970.
56. U. Oberst. The construction of Noetherian operators. *Journal of Algebra*, 222(2):595–620, 1999.
57. H. Osborn. Modules of differentials. II. *Mathematische Annalen*, 175:146–158, 1968.
58. M. S. Paterson and L. J. Stockmeyer. On the number of nonscalar multiplications necessary to evaluate polynomials. *SIAM Journal on Computing*, 2(1):60–66, March 1973.
59. P. Penfield, Jr., R. Spencer, and S. Duinker. *Tellegen's theorem and electrical networks.* The M.I.T. Press, Cambridge, Mass.-London, 1970.

60. F. Rouillier. Solving zero-dimensional systems through the Rational Univariate Representation. *Applicable Algebra in Engineering, Communication and Computing*, 9(5):433–461, 1999.
61. M. Saito, B. Sturmfels, and N. Takayama. *Gröbner deformations of hypergeometric differential equations*. Springer-Verlag, Berlin, 2000.
62. P. Samuel. *Théorie algébrique des nombres*. Hermann, 1971.
63. G. Scheja and U. Storch. Über Spurfunktionen bei vollständigen Durchschnitten. *Journal für die reine und angewandte Mathematik*, 278-279:174–190, 1975.
64. É. Schost. *Sur la résolution des systèmes polynomiaux à paramètres*. PhD thesis, École polytechnique, 2000.
65. J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27(4):701–717, October 1980.
66. V. Shoup. Fast construction of irreducible polynomials over finite fields. *Journal of Symbolic Computation*, 17(5):371–391, 1994.
67. V. Shoup. Efficient computation of minimal polynomials in algebraic extensions of finite fields. In *Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC)*, pages 53–58, New York, 1999. ACM.
68. V. Strassen. Gaussian elimination is not optimal. *Numerische Mathematik*, 13:354–356, 1969.
69. B. Tellegen. A general network theorem, with applications. *Philips Research Reports*, (7):259–269, 1952.
70. J.-A. Thiong Ly. Note for computing the minimum polynomial of elements in large finite fields. In *Coding theory and applications (Toulon, 1988)*, volume 388 of *Lecture Notes in Comput. Sci.*, pages 185–192. Springer, New York, 1989.
71. J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, New York, 1999.
72. D. Wiedemann. Solving sparse linear equations over finite fields. *IEEE Transactions on informations theory*, IT-32:54–62, 1986.
73. R. Zippel. Probabilistic algorithms for sparse polynomials. In *Symbolic and algebraic computation*, number 72 in Lecture Notes in Computer Science, pages 216–226, Berlin, 1979. Springer. Proceedings EUROSAM '79, Marseille, 1979.