Gröbner Duality and Multiplicities in Polynomial System Solving *

Maria Grazia Marinari
Dipartimento di Matematica
Università di Genova
marinari@dima.unige.it

Teo Mora †
Dipartimento di Informatica
Università di Genova
theomora@dima.unige.it

Hans Michael Möller
Fachbereich Mathematik
FernUniversität Hagen
michael.moeller@fernuni-hagen.de

Abstract

This paper deals with the description of the solutions of zero dimensional systems of polynomial equations. Based on different models for describing solutions, we consider suitable representations of a multiple root, or more precisely suitable descriptions of the primary component of the system at a root. We analyse the complexity of finding the representations. We also discuss the current approach to the representation of real roots.

1 Introduction

When solving a 0 - dimensional system of polynomial equations it is often satisfactory to know the zeroes of the system in such a way, that one can perform arithmetical operations on the coordinates of each root. One could however be interested also in the multiplicity of each root, not just in the weak "arithmetical" sense of simple, double, triple, etc. root, but in the stronger "algebraic" sense of giving a suitable description of the primary component at a root of the ideal defining the solution set of the system. The aim of this paper is to discuss a representation of the "algebraic" multiplicity and ways of computing it.

There is of course a stream of research about methods for solving systems of equations (for a survey we refer to [L93]) and also a "reflection" about the "meaning" of solving a system. The philosophy essentially goes back to Kronecker: a system is solved, if each root is represented in a way which allows to perform any arithmetical operations over the arithmetical expressions of its coordinates (the operations include, in the real case, numerical interpolation). For instance, in the classical Kronecker method, concerning the univariate case, one is given a tower of algebraic field extensions over the field of rational numbers, each field being a polynomial ring over the previous one modulo the ideal generated by a single polynomial and each root is represented by an element in such fields. The main effort of the actual research is devoted to effective techniques for representing roots of a systems and allowing efficient arithmetical operations over their expressions.

In this setting of research, we are interested in how to describe a primary at a root of a system and how to be able to compute representation of such primary ideal, i.e. try to answer the question how to "compute multiplicity".

The "arithmetical" multiplicity of a primary ideal for the maximal at the origin can be easily computed and read from the Hilbert polynomial but this doesn't give a sufficient description of the "algebraic" multiplicity. In fact it is known that up to invertible transformations in $K[[X,Y]]$ there are exactly two classes of primaries at the origin having multiplicity 3, they are represented by (X^3, Y) and $(X,Y)^2$.

One could hope that more accurate invariants allow to distinguish primary ideals which are locally isomorphic, e.g. the Hilbert function (remark that of course it allows to discriminate the two classes above). However an example by Galligo [G] casts some doubts on this hope: it implies the existence of two primaries of the same multiplicity, which are not locally isomorphic and are not distinguishable by the Hilbert funcion and the Betti numbers.

Therefore, in order to describe multiplicities of roots, we begin as a preliminary with the obvious "algebraic" approach which describes a root by studying the primary component of the ideal of the system corresponding to the given zero.

While obviously Gröbner bases and (mainly due to the "local" setting) standard bases are natural representations of primaries, a different approach was proposed by Gröbner in order to reinterpret Macaulay notion of inverse systems. Gröbner's suggestion is a generalization of the obvious univariate case, where α is a root of $f(X)$ of multiplicity d iff $\frac{\partial^n}{\partial X^n}(f)(\alpha) = 0 \ \forall n, 0 \leq n < d$.

Gröbner proved that if $\mathbf{a} \in \mathbf{k}^n$ is a common root of multivariate polynomials $f_1, \ldots, f_r, \in k[X_1, \ldots, X_n]$ (k any field of characteristic 0 and $\mathbf{k}$ its algebraic closure), then there are finitely many linear combinations D_i of partial derivatives $\frac{\partial^{i_1+\ldots+i_n}}{\partial x_1^{i_1} \ldots \partial x_n^{i_n}}$, such that every polynomial f in the ideal $(f_1, \ldots, f_r)$ satisfies $D_i(f)(\mathbf{a}) = 0$ for all i. Moreover the set of polynomials f satisfying $D_i(f)(\mathbf{a}) = 0$ for all i is exactly the primary component at $\mathbf{a}$ of the ideal $(f_1, \ldots, f_r)$. The D_i are therefore a basis of a so called *closed subspace of differential conditions at the point.* By the way, its dimension is the "arithmetical" multiplicity of the root. Because

* This research was performed with the contribution of CEC Basic Research ESPRIT contract n. 6846 POSSO

† The coauthor thanks the GAGE, École Polytechnique, Palaiseau in Paris for hospitality and financial support during the preparation of this paper

of this (Gröbner theory is presented in §3 and detailed in [MMM2]), it is natural to describe a primary by a closed subset of differential conditions.

In our paper [MMM2] we studied how to transform any such representation into another one and how to compute them to represent a primary of a root of a system. We give here a survey of our results related to the Gröbner proposal, which we call *Gröbner Duality* [1]

In this paper we give a brief survey of the Gröbner Duality and of the relevant results contained in [MMM2] and related results.

In §3 we reintroduce the duality concept by Gröbner which proved the duality between primary ideals at the origin with "closed" subspaces of differential conditions. We propose a specific representation of dual bases (§4) in order to have the same complexity for the representation of a primary ideal given by differential conditions and by a Gröbner-standard basis. Then we show how it can be used to test whether a polynomial belongs to a primary (§5).

In order to compute the dual basis representing a primary we introduce the notion of *continuation*, which allows to find all primaries containing the given one and with multiplicity 1 higher (§6) and then we introduce algorithms to compute continuations (§7).

They allow to compute a dual basis of a primary given by any basis (Gröbner, standard or whatever) (§8).

We also discuss the current approaches in representing the roots of a system following Kronecker's philosophy and the important generalizations by Duval [D] (§9).

On the basis of that, we show that applying the algorithm discussed in §8 to a 0-dimensional multivariate ideal and computing arithmetics "à la Duval" we get a sort of primary factorization, exactly as the Duval algorithm provided distinct-power-factorization for univariate polynomials (§10).

2 Preliminary and Notation

2.1 Notation

Let k be an effective field of characteristic zero, $\mathbf{k}$ its algebraic closure, $\mathcal{P} := k[X_1, \ldots, X_n]$, $\mathbf{T}$ the semigroup generated by $\{X_1, \ldots, X_n\}$, $\forall i \geq 1$ $\mathbf{T}_i$ the semigroup generated by $\{X_1, \ldots, X_i\}$, $\mathbf{m} = (X_1, \ldots, X_n)$ the maximal ideal at the origin.

Let $K \subset \mathbf{k}$ be a finite algebraic extension of k and let $\mathcal{P}_K := K[X_1, \ldots, X_n]$; for an ideal $\mathcal{I} \subset \mathcal{P}$, we will denote $\mathcal{I}_K := \mathcal{I}\mathcal{P}_K$.

For a sparse polynomial $f = \sum_{i=1}^{\mu} c_i \tau_i$, $c_i \neq 0 \; \forall i$, $\tau_j \neq \tau_j$ for $i \neq j$, we will call *staircase generated by* f, the set $\Sigma(f) := \{\tau \in \mathbf{T} : \tau \text{ divides } \tau_i \text{ for some } i\}$ ([MT]).

2.2 Primary decomposition

A zero-dimensional ideal $\mathcal{I} \subset \mathcal{P}$ has a primary decomposition $\mathcal{I} = \mathbf{q}_1 \cap \ldots \cap \mathbf{q}_t$, where each $\mathbf{q}_i$ is $\mathbf{m}_i$-primary for a maximal ideal $\mathbf{m}_i$, and $\mathbf{m}_i \neq \mathbf{m}_j$ for $i \neq j$.

Each maximal ideal corresponds to a set of k-conjugate zeroes of $\mathcal{I}$, whose coordinates live in the finite algebraic extension $K_i := \mathcal{P}/\mathbf{m}_i$ of the field k.

[1] In site of the conjuring name, Gröbner Duality is not directly related with the duality notions connected with polynomial systems introduced in [FGS], [C],(*cf* also [BK]) while however it would be interesting to understand if such a relation exists. Gröbner theory can be found in many papers by him and in his book [Gr]

If $\mathbf{m}_i$ is linear, $\mathbf{m}_i = (X_1 - a_1, \ldots, X_n - a_n)$, then it defines a *rational* root of $\mathcal{I}$, $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{k}^n$.

If $\mathbf{m} := \mathbf{m}_i$ is not linear, and $K := \mathcal{P}/\mathbf{m}$, then $\mathbf{m}\mathcal{P}_K$ has a decomposition into maximal ideals in P_K, $\mathbf{m}\mathcal{P}_K = \mathbf{n}_1 \cap \ldots \cap \mathbf{n}_r$, the $\mathbf{n}_j$'s are k-conjugate, linear, defining roots $\mathbf{b}_j \in K^n$, which are conjugate over k; moreover $\mathbf{m} = \mathbf{n}_j \cap \mathcal{P} \; \forall j$. As for the $\mathbf{m}$-primary $\mathbf{q} = \mathbf{q}_i$ in the decomposition of $\mathcal{I}$, $\mathbf{q}\mathcal{P}_K$ has a primary decomposition, $\mathbf{q}\mathcal{P}_K = \mathbf{p}_1 \cap \ldots \cap \mathbf{p}_r$, where $\mathbf{p}_j$ is $\mathbf{n}_j$-primary, the $\mathbf{p}_j$'s are k-conjugate and $\mathbf{q} = \mathbf{p}_j \cap \mathcal{P} \; \forall j$.

If $\mathbf{m} \subset \mathcal{P}$ is a maximal ideal, $K := \mathcal{P}/\mathbf{m}$ and $\mathbf{q}$ is an $\mathbf{m}$-primary ideal, then the (arithmetical) multiplicity of $\mathbf{q}$ is $\text{mult}(\mathbf{q}) := \dim_k(\mathcal{P}/\mathbf{q})$. If $\mathbf{q}$ is an $\mathbf{m}$-primary component of a 0-dimensional ideal $\mathcal{I}$, where the roots of $\mathbf{m}$ are $\mathbf{b}_1, \ldots, \mathbf{b}_r \in K^n$, corresponding to primaries $\mathbf{p}_i \in \mathcal{P}_K$, the multiplicity of $\mathcal{I}$ in $\mathbf{b}_i$ is $\text{mult}(\mathbf{p}_i) = \dim_K(\mathcal{P}_K/\mathbf{p}_i) = \dim_k(\mathcal{P}/\mathbf{q})/\dim_k(K)$. See for instance [Gr], pp. 168 – 178.

2.3 Set up

Let us fix a 0-dimensional ideal $\mathcal{I} \subset \mathcal{P}$ and a root $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{k}^n$ of $\mathcal{I}$. We will denote:

- $K = k(a_1, \ldots, a_n)$ the minimal algebraic extension of k containing $\mathbf{a}$,
- $\mathbf{m} = (X_1 - a_1, \ldots, X_n - a_n) \subset \mathcal{P}_K$ the linear maximal ideal whose root is $\mathbf{a}$,
- $\mathbf{q} \subset \mathcal{P}_K$, the $\mathbf{m}$-primary component of $\mathcal{I}\mathcal{P}_K$.

Up to a translation $(X_i \mapsto X_i + a_i)$ we can assume $a_i = 0$, i.e. $\mathbf{m}$ to be the maximal and $\mathbf{q}$ a primary at the origin, and we will do so in order to simplify notation.

2.4 Complexity

In our complexity considerations, we are strictly working in an arithmetical setting and we just count the number of rational operations in k required by our algorithms. Even worse, we will simply count the number operations required over an algebraic extension $K = k(a_1, \ldots, a_n)$. In terms of algorithms for root representations (§9), this complexity can be reduced to the previous one, by multiplying it by a constant, which will be evaluated in §10. It is clear, that under this very weak complexity model, the important question of coefficient growth cannot be considered at all.

We will measure complexity in terms of the following parameters:

- n, the number of variables in $\mathcal{P}$
- $t = \dim_k(K)$
- $s := \text{mult}(\mathcal{I})$
- $r := \text{mult}(\mathbf{q})$
- m the cardinality of the input basis of the ideal $\mathcal{I}$
- Σ the sum of the cardinalities of $\Sigma(f_i)$ for f_i in the input basis of $\mathcal{I}$.

Remark that if $\mathcal{I}$ is given through a reduced Gröbner basis, $m \leq ns$ and $\Sigma = \mathcal{O}(ns^2)$.

Since we may need to perform a translation, for the following complexity discussions, it is preliminary to know, what is the effect of a translation on a polynomial $f = \sum_{i=1}^{\mu} c_i \tau_i$. It is easy to see from Taylor formula (see (**) below) that the only terms with non-zero coefficients are necessarily contained in $\Sigma(f)$ and that computing $f(X + a)$

requires $\mathcal{O}(\mu\sigma)$ arithmetical operations in K and so $\mathcal{O}(t^2\mu\sigma)$ operations in k, where μ is the number of terms in f, σ the cardinality of $\Sigma(f)$. Moreover, if f is an element in the reduced Gröbner basis of a 0-dimensional ideal $\mathcal{I}$, then $\mu \leq s+1$, $\Sigma(f) \leq s$, so, in case of translation, the space complexity of a basis of $\mathcal{I}$ is still bounded by $\Sigma = \mathcal{O}(ns^2)$ and the time complexity of computing it $\mathcal{O}(t^2ns^3)$.

3 Gröbner Duality

We denote by $D(i_1,\ldots,i_n) : \mathcal{P} \to \mathcal{P}$ the differential operator:

$$D(i_1,\ldots,i_n) = \frac{1}{i_1!\ldots i_n!}\frac{\partial^{i_1+\cdots+i_n}}{\partial X_1^{i_1}\cdots\partial X_n^{i_n}}.$$

This notation will be however simplified by denoting $D(t) := D(i_1,\ldots,i_n)$ where $t = X_1^{i_1}\ldots X_n^{i_n}$. Also, $i_1+\cdots+i_n = \deg(t)$ will be called the *order* of $D(t)$, $ord(D(t))$.

We moreover denote $\mathbf{D} := \{D(t) : t \in \mathbf{T}\}$ and $\mathrm{Span}_K(\mathbf{D})$ the K-vector space generated by $\mathbf{D}$; the order of an element $\sum c_i D(t_i) \in \mathrm{Span}_K(\mathbf{D})$, with $c_i \neq 0\ \forall i$, is $\max(ord(D(t_i)))$. In addition $\mathbf{D}_j := \{D(0,\ldots,0,i_j,\ldots,i_n) : i_j \neq 0\}$.

For $t = X_1^{d_1}\cdots X_n^{d_n}$ and $\tau = X_1^{e_1}\cdots X_n^{e_n}$ we get by straightforward calculations

$$D(t)(\tau) = \begin{cases} \binom{\tau}{t}\tau_1 & \text{if } \tau = t\tau_1 \\ 0 & \text{if } t \text{ does not divide } \tau \end{cases}$$

where $\binom{\tau}{t} := \binom{e_1}{d_1}\cdots\binom{e_n}{d_n}$.

Hence if $f = \sum_{\tau\in\mathbf{T}} c_\tau\tau \in \mathcal{P}_K$ and $L = \sum_{\tau\in\mathbf{T}} b_\tau D(\tau) \in \mathrm{Span}_K(\mathbf{D})$, one has $L(f)(\mathbf{0}) = \sum_{\tau\in\mathbf{T}} c_\tau b_\tau$. Remark that for $f = \sum_{i=1}^{\mu} c_i t_i$, the Taylor formula asserts that for $\mathbf{a} = (a_1,\ldots,a_n)$

$$\begin{aligned} f(X_1+a_1,\ldots,X_n+a_n) &= \sum_{\tau\in\mathbf{T}} D(\tau)(f)(\mathbf{a})\tau \\ &= \sum_{\tau\in\mathbf{T}} \tau \sum_{\substack{i=1 \\ \tau|t_i}}^{\mu} c_i\tbinom{t_i}{\tau}\tfrac{t_i}{\tau}(\mathbf{a}). \quad (**) \end{aligned}$$

For each $j = 1,\ldots,n$, $\sigma_{X_j} : \mathrm{Span}_K(\mathbf{D}) \to \mathrm{Span}_K(\mathbf{D})$ is the antiderivative with respect to X_j, i.e. the linear map s.t.:

$$\sigma_{X_j}(D(i_1,\ldots,i_n)) = \begin{cases} D(i_1,\ldots,i_j-1,\ldots,i_n) & \text{if } i_j > 0, \\ 0 & \text{otherwise.} \end{cases}$$

Since $\sigma_{X_j}\sigma_{X_i} = \sigma_{X_i}\sigma_{X_j}\forall i,j$, the linear map σ_t is defined in the obvious way for each $t \in \mathbf{T}$.

Let us consider now, for each $j = 1,\ldots,n$, the linear map $\rho_{X_j} : \mathrm{Span}_K(\mathbf{D}) \to \mathrm{Span}_K(\mathbf{D})$ s.t.:

$$\rho_{X_j}(D(i_1,\ldots,i_n)) = D(i_1,\ldots,i_j+1,\ldots,i_n)$$

Again ρ_t is defined in the obvious way for each $t \in \mathbf{T}$. and the relation $\sigma_t\rho_t = \mathrm{Id}$ holds for each $t \in \mathbf{T}$.

To simplify notations, let us denote $\sigma_j := \sigma_{X_j}$, $\rho_j := \rho_{X_j}$, and $\lambda_j := \rho_j\sigma_j$. Then the following relations hold:

* $\lambda_j(D(i_1,\ldots,i_n)) = \begin{cases} D(i_1,\ldots,i_n) & \text{if } i_j > 0, \\ 0 & \text{otherwise.} \end{cases}$

* $\sigma_j\rho_l(D(i_1,\ldots,i_n)) = \rho_l\sigma_j(D(i_1,\ldots,i_n))$
$= \begin{cases} D(i_1,\ldots,i_j-1,\ldots,i_l+1,\ldots,i_n) & \text{if } i_j > 0, \\ 0 & \text{otherwise.} \end{cases}$

If $<$ is a semigroup ordering on $\mathbf{T}$, the induced ordering on $\mathbf{D}$ satisfies

$$L_1 < L_2 \Rightarrow \rho_t(L_1) < \rho_t(L_2)\ \forall t \in \mathbf{T}, \forall L_1, L_2 \in \mathbf{D}.$$

With respect to this ordering we can speak of the leading term $T(L)$ of $L \in \mathrm{Span}_K(\mathbf{D})$ in a completely analogous way as for a polynomial: if $L = \sum c_i D_i$ with $c_i \neq 0$, $D_i \in \mathbf{D}$, $D_1 > D_2 > \cdots$, then $T(L) = D_1$.

A K-vector subspace $V \subset \mathrm{Span}_K(\mathbf{D})$ is *closed* if $\forall t \in \mathbf{T}$, $\forall L \in V$, $\sigma_t(L) \in V$ and if $\dim_k(V)$ is finite. Let

$$\Im(V) := \{f \in \mathcal{P}_K : L(f)(\mathbf{0}) = 0\ \forall L \in V\}.$$

If $\mathcal{I} \subset \mathbf{m}$ define

$$\Delta(\mathcal{I}) := \{L \in \mathrm{Span}_K(\mathbf{D}) : L(f)(\mathbf{0}) = 0\ \forall f \in \mathcal{I}\}.$$

Theorem 3.1 *$\mathbf{m}$-primary ideals of P_K and closed subspaces of $\mathrm{Span}_K(\mathbf{D})$ are under a biunivocal correspondence. More exactly every closed subspace $V \subset \mathrm{Span}_K(\mathbf{D})$ corresponds to the $\mathbf{m}$-primary ideal $\Im(V)$ and every $\mathbf{m}$-primary ideal $\mathbf{q}$ corresponds to the closed subspace $\Delta(\mathbf{q})$, so that $\mathbf{q} = \Im(\Delta(\mathbf{q}))$ and $V = \Delta(\Im(V))$.* [2] *Moreover*

$$\dim_K(\Delta(\mathbf{q})) = \mathrm{mult}(\mathbf{q}), \mathrm{mult}(\Im(V)) = \dim_K(V).$$

Proof [Gr] 174–178 ∎

4 Representation of differential condition

Theorem 3.1 provides a way of representing any $\mathbf{m}$-primary ideals $\mathbf{q}$, by giving a basis of the closed subspace $\Delta(\mathbf{q})$. There is however a major problem with this representation, that it can be space-exponential in $\mathrm{mult}(\mathbf{q})$.

Example 4.1 Consider the ideal

$$\mathbf{q} := (X_1^r, X_2 - X_1, \ldots, X_n - X_1).$$

Then $\Delta(\mathbf{q})$ is generated by$\{L_0 \ldots L_{r-1}\}$ where $L_0 = D(1) = \mathrm{Id}$, $L_1 = D(X_1) + \cdots + D(X_n)$, and in general

$$L_i = \sum_{\substack{t\in\mathbf{T} \\ \deg(t)=i}} D(t),$$

so that an ideal of multiplicity r could require storing $\binom{r}{n}$ elements in K.

There is an easy way out for *this* example: perform the change of coordinates $Y_1 := X_1$, $Y_2 := X_2 - X_1$, ..., $Y_n := X_n - X_1$, so $\mathbf{q} = (Y_1^r, Y_2, \ldots, Y_n)$ and $\Delta(\mathbf{q})$ is now generated by $\{D(Y_1^i) : i = 0 \ldots r-1\}$. However this procedure doesn't apply to the next example.

Example 4.2 Consider now the ideal $\mathcal{I}$ of the curve with parameteric equations $X_1 = t, X_2 = t^2, \ldots, X_n = t^n$ and the $\mathbf{m}$-primary ideal $\mathbf{q}_r := \mathcal{I} + \mathbf{m}^r$. Define $w : \mathbf{T} \to \mathbb{N}$ by $w(X_i) := i$, $L_i := \sum_{\substack{t\in\mathbf{T} \\ w(t)=i}} D(t)$. It is possible to prove that $\Delta(\mathbf{q}_r)$ is generated by $\{L_0, \ldots, L_{r-1}\}$, requiring the storage of $\mathcal{O}((r/n)^n)$ K-elements and that this basis is the least space-consuming.

It is therefore important to look for an alternative representation of closed subspaces which has less storage requirements. Here we propose one such representation.

[2] We are generalizing the theorem to prove that the duality above relates ideals closed w.r.t. $\mathbf{m}$-adic topology with vector subspace which are closed for antiderivative (but don't have finite dimension)

We start by discussing projections via dual bases.

So let $X_{i_1}, \ldots, X_{i_d}$ be a subset of variables and let $\mathcal{P}' := k[X_{i_1}, \ldots, X_{i_d}]$, $\mathbf{T}'$ the semigroup of terms of $\mathcal{P}'$, $\mathbf{D}' := \{D(t) : t \in \mathbf{T}'\}$ and let $\pi : \mathrm{Span}_K(\mathbf{D}) \to \mathrm{Span}_K(\mathbf{D}')$ be the canonical projection.

Proposition 4.3 *Let $\mathbf{q} \subset \mathcal{P}$ be a primary ideal, $V := \Delta(\mathbf{q})$, $\mathbf{q}' := \mathbf{q} \cap \mathcal{P}'_K$. Then $\pi(V) = \Delta(\mathbf{q}')$.*

Proof First of all remark that $\pi(V)$ is closed. Also, if $f \in \mathcal{P}'_K$ and $L \in \mathrm{Span}_K(\mathbf{D})$, then $L(f) = \pi(L)(f)$, since $D(t)(f) = 0$ if $t \notin \mathbf{T}'$.

Let $L' \in \pi(V)$ and let $L \in V$ be s.t. $\pi(L) = L'$. $L'(f') = L(f') = 0$ holds for each $f' \in \mathbf{q}'$. This implies $\pi(V) \subset \Delta(\mathbf{q}')$.

Conversely, let $f' \in \mathcal{P}'_K$ be s.t. $L(f) = 0$ for all $L \in \pi(V)$. Then $L'(f') = \pi(L')(f') = 0$ for all $L' \in V$, so $f \in \mathbf{q} \cap \mathcal{P}'_K = \mathbf{q}'$. This proves $\Im(\pi(V)) \subset \mathbf{q}'$. Since $\pi(V)$ is closed, we obtain $\pi(V) = \Delta\Im(\pi(V)) \supset \Delta(\mathbf{q}')$. ∎

Each element $L \in \mathrm{Span}_K(\mathbf{D} \setminus \{Id\})$ can be uniquely written as $L = L_1 + \cdots L_n$ where $L_j \in Span_K(\mathbf{D}_j)$. Denote $L_{\geq j} := \sum_{i=j}^{n} L_i$; analogously, we will use also the notation $L_{\leq j}$, $L_{>j}$, $L_{<j}$. Remark that if V is a closed subspace, the set $V_j := \{L_{\geq j} : L \in V\}$ is a projection of V and so it is closed. Then from the above definitions, we immediately get the following:

Lemma 4.4 *Let $L = L_1 + \cdots L_n \in \mathrm{Span}_K(\mathbf{D} \setminus \{Id\})$. The following hold:*

- $\lambda_i(L) = \lambda_i(L_1) + \cdots + \lambda_i(L_{i-1}) + L_i$
- $(\lambda_i(L))_j = \begin{cases} \lambda_i(L_j) & \text{if } j < i, \\ L_j & \text{if } j = i, \\ 0 & \text{if } j > i \end{cases}$
- $L_i = \lambda_i(L_{\geq i}) = (\lambda_i(L))_{\geq i}$

Proposition 4.5 *Let U be a closed subspace of $\mathrm{Span}_K(\mathbf{D})$, let $\Gamma := \{L^{(1)}, \ldots, L^{(r)}\}$ be a basis of U. Let L be s.t. $U + \langle L \rangle$ is closed (i.e. in the terminology which will be introduced in §6 : a continuation of U). Then $\forall j$, $L_j = \sum_{i=1}^{r} c_{ij} \rho_j(L^{(i)}_{\geq j})$ for some $c_{ij} \in K$.*

Proof One has $\sigma_j(L) \in U$ so $\sigma_j(L) = \sum_{i=1}^{r} c_{ij} L^{(i)}$. Therefore:

$$L_j = \lambda_j(L_{\geq j}) = \rho_j(\sigma_j(L_{\geq j})) = \sum_{i=1}^{r} \rho_j(c_{ij} L^{(i)}_{\geq j}). \qquad \blacksquare$$

Corollary 4.6 *A closed vector space $V \subset \mathrm{Span}_K(\mathbf{D})$ with $\dim(V) = r$ can be represented by $\mathcal{O}(nr^2)$ elements in K.*

Proof Let $\Gamma := \{L^{(1)}, \ldots, L^{(r)}\}$ be a basis of V, where, w.l.o.g. $T(L^{(i)}) < T(L^{(j)})$ for $i < j$. Hence $L^{(1)} = \mathrm{Id}$ and moreover, as it is easy to prove, each $\langle L^{(1)}, \ldots, L^{(\ell)} \rangle$ is closed. To represent $L^{(\ell)}$, one can just represent each $L^{(\ell)}_j$ and to represent it one has just to assign the coefficients of $\sum_{i<\ell} c_{ij} \rho_j(L^{(i)}_{\geq j})$.

Therefore one needs $\sum_{\ell=2}^{r} n(\ell - 1) = \frac{nr(r-1)}{2}$ elements in K to represent V. ∎

Remark that if $\mathbf{q} := \mathcal{I}(V) \subset \mathcal{P}_K$ is a 0-dimensional ideal, then $\mathrm{mult}(\mathbf{q}) = \dim(V) = r$; therefore, following [FGLM] and [MMM1], the ideal $\mathbf{q}$ can be represented by Gröbner bases by means of $\mathcal{O}(nr^2)$ elements in K. So the representation we propose has the expected complexity.

Corollary 4.7 *Let U be a closed subspace of $\mathrm{Span}_K(\mathbf{D})$, let $\Gamma_j := \{L^{(j1)}, \ldots, L^{(jr_j)}\}$ be a Gauss basis [3] of $U_j = \{L_{\geq j} : L \in U\}$ for each $j = 1, \ldots, n$. Let L be s.t. $U + \langle L \rangle$ is closed. Then $\forall j$, $L_j = \sum_{i=1}^{r_j} c_{ij} \rho_j(L^{(ji)})$ for some $c_{ij} \in K$.*

Proof By Proposition 4.5, $L_j = \rho_j(\sum_i c_{ij} L^{(i)}_{\geq j})$. Since $\sum_i c_{ij} L^{(i)}_{\geq j} \in U_j$ the assertion follows. ∎

Lemma 4.8 *Denote $B_U := \{\rho_j(L^{(ji)}) : j = 1, \ldots, n,\ i = 1, \ldots, r_j\}$. Then B_U is a Gauss basis for the vector space it generates.*

Proof We have to prove for arbitrary $b_1, b_2 \in B_U$ that $T(b_1) = T(b_2)$, implies $b_1 = b_2$. Remark that $\rho_j(L^{(ji)}) \in \mathrm{Span}_K(\mathbf{D}_j)$, so $T(\rho_j(L^{(ji)})) \in \mathbf{D}_j$ and for $\mu \neq j$ one has $T(\rho_j(L^{(ji)})) \neq T(\rho_\mu(L^{(\mu l)}))$. So assume $T(\rho_j(L^{(ji)})) = T(\rho_j(L^{(jl)}))$. This of course implies $T(L^{(ji)}) = T(L^{(jl)})$ and so $l = i$ since Γ_j is a Gauss basis. ∎

5 Testing ideal membership with this alternative representation

Gröbner bases allow, via Buchberger Reduction, to test whether a polynomial f belongs to an ideal, and in particular to an $\mathbf{m}$-primary ideal. We need therefore to show that this is also allowed by the representation we propose. We will show in fact that the representation discussed in Prop. 4.5 is suitable for testing membership of a polynomial f to an ideal $\mathcal{I}(V)$ where V is a closed vector space; particularly if f is given by a "recursive Horner representation", i.e.

i) a univariate polynomial f in X_1 of degree d is represented as $f = a_0 + X_1 g$, where g has degree $d-1$ and is recursively represented in the same way.

ii) a polynomial f in $X_1, \ldots, X_i$ of degree d in X_i is represented as $f = p_0 + X_i f_1$ where p_0 is a polynomial in $X_1, \ldots, X_{i-1}$, f_1 is a polynomial in $X_1, \ldots, X_i$ of degree $d-1$ in X_i, and both are recursively represented in the same way.

A polynomial f represented in this way is uniquely written as

$$f = \Big(\cdots \big((f_0 + X_1 f_1) + X_2 f_2 \big) + \cdots + X_n f_n \Big)$$

with $f_i \in K[X_1, \ldots, X_i]$. Denote $\wp_0(f) := f_0$, $\wp_1(f) := f_1$, ..., $\wp_i(f) := f_i$, ..., $\wp_n(f) := f_n$.

Given a pointer to a list representation of f, one can extract $\wp_0(f)$ and the pointers to $\wp_n(f), \ldots, \wp_1(f)$ in $n+1$ operations. Let us call a component of f any polynomial which can be obtained from f by iterating the functions $\wp_i$ on it.

Recall that we did assume to have performed a translation to move the zero $\mathbf{a}$ of $\mathbf{q}$ to the origin. Therefore if f is given in the original frame, the first thing to do is to compute $f(X + \mathbf{a})$; this can be done by Taylor formula and it is easy to see that computations can be arranged "à la FGLM" in order to obtain $f(X + \mathbf{a})$ directly in recursive Horner representation, still at a cost of $\mathcal{O}(t^2 \mu \sigma)$ operations

[3] A basis $\Gamma = (L_1, \ldots, L_r)$ of a vector space $V \subset \mathrm{Span}_K(\mathbf{D})$ will be called a *Gauss basis* if:

G1) $T(L_i) < T(L_j)$ for $i < j$,

G2) $L_i = T(L_i) + \sum c_{i\kappa} D_{i\kappa}$ with $c_{i\kappa} \neq 0$, $D_{i\kappa} \neq T(L_j)\ \forall i, j, \kappa$.

We will call it a *reduced Gauss basis*, if for no $L \in \Gamma$ the term $T(L)$ is a D'_i of an other $L' = \sum c_i D'_i \in \Gamma$, $c_i \neq 0$.

in k. We can therefore assume that f is given in recursive Horner representation in the new setting.

Let us be given a basis $\Gamma = \{L^{(1)}, \ldots, L^{(s)}\}$ of a closed vector space V, where each $L_j^{(\ell)}$ is represented as $L_j^{(\ell)} = \sum_{i<\ell} \sum_{\nu=j}^{n} c_{ij} \rho_j(L_\nu^{(i)})$ and let $\alpha_{j\tau}^{(\ell)} \in K$ be s.t. $L_j^{(\ell)} = \sum_{\tau \in \mathbf{T}} \alpha_{j\tau}^{(\ell)} D(\tau)$ so that one has

$$\alpha_{j\tau}^{(\ell)} = \begin{cases} 0 & \text{if } \tau \text{ is not divisible by } X_j \ , \\ \sum_{i<\ell} \sum_{\nu=j}^{n} c_{ij} \alpha_{\nu\omega}^{(i)} & \text{if } \tau = X_j \cdot \omega \ . \end{cases}$$

If $f = \sum_{\tau \in \mathbf{T}} a_\tau \tau \in \mathcal{P}_K$ then $\left(L_j^{(\ell)}(f)\right)(0) = \sum_{\tau \in \mathbf{T}} \alpha_{j\tau}^{(\ell)} a_\tau$. Define now $f_j^{(\ell)} := \sum\limits_{\omega \in \mathbf{T}_j} \omega \sum\limits_{\tau \in \mathbf{T}} a_{\tau \cdot \omega} \alpha_{j\tau}^{(\ell)}$.

Lemma 5.1 *The following hold for each j, for each ℓ:*

1) $\left(L_j^{(\ell)}(f)\right)(0) = f_j^{(\ell)}(0)$,

2) $f_j^{(\ell)} = \sum_{i<\ell} \sum_{\nu=j}^{n} c_{ij} \wp_j(f_\nu^{(i)})$.

Proof

1): $\left(L_j^{(\ell)}(f)\right)(0) = \sum_{\tau \in \mathbf{T}} \alpha_{j\tau}^{(\ell)} a_\tau = f_j^{(\ell)}(0)$.

2): Let's remark that $\wp_j(f_\nu^{(i)}) = \sum\limits_{\omega \in \mathbf{T}_j} \omega \sum\limits_{\tau \in \mathbf{T}} a_{\tau X_j \omega} \alpha_{\nu\tau}^{(i)}$.

Hence, one has

$$\begin{aligned} f_j^{(\ell)} &= \sum_{\omega \in \mathbf{T}_j} \omega \sum_{\tau \in \mathbf{T}} a_{\tau\omega} \alpha_{j\tau}^{(\ell)} = \\ &= \sum_{\omega \in \mathbf{T}_j} \omega \sum_{\tau \in \mathbf{T}} a_{\tau X_j \omega} \sum_{i<\ell} \sum_{\nu=j}^{n} c_{ij} \alpha_{\nu\tau}^{(i)} = \\ &= \sum_{i<\ell} \sum_{\nu=j}^{n} c_{ij} \sum_{\omega \in \mathbf{T}_j} \omega \sum_{\tau \in \mathbf{T}} a_{\tau X_j \omega} \alpha_{\nu\tau}^{(i)} = \\ &= \sum_{i<\ell} \sum_{\nu=j}^{n} c_{ij} \wp_j(f_\nu^{(i)}) \quad \blacksquare \end{aligned}$$

Because of the recursive definition of $f_j^{(\ell)}$ implied by Lemma 5.1 2), accessing each $f_j^{(\ell)}$ requires keeping σ pointers to components of f and as many elements in K.

To test if $f \in \Im(V)$ one has to test whether, for all ℓ:

$$\begin{aligned} 0 &= \left(L^{(\ell)}(f)\right)(0) = \sum_j \left(L_j^{(\ell)}(f)\right)(0) = \\ &= \sum_j f_j^{(\ell)}(0) = \sum_j \wp_0(f_j^{(\ell)}). \end{aligned}$$

The test $\sum_j \wp_0(f_j^{(\ell)}) = 0 \ \forall \ell$ requires again $\mathcal{O}(ns^2)$ arithmetical operations in K, $\mathcal{O}(nt^2 s^2)$ arithmetical operations in k. This gives us the complexity for testing if $f \in \mathbf{q}$ via differential condition.

6 Continuations of a closed vector space

In order to discuss algorithms to compute a differential conditions representation of an $\mathbf{m}$-primary ideal $\mathbf{q}$, it is preliminary to introduce the notion of "continuations of a closed vector space".

We will first need the following formulation of the Leibniz formula, which holds for all $L \in \mathrm{Span}_K(\mathbf{D})$ and $f, g \in \mathcal{P}_K$

$$L(fg) = \sum_{\tau \in \mathbf{T}} D(\tau)(g) \ \sigma_\tau(L(f))$$

which allows us to work in the following with bases instead of the corresponding vector spaces:

Lemma 6.1 [MS] *Let $\{L^{(1)}, \ldots, L^{(r)}\}$ be a basis of a closed space V and let $\{f_1, \ldots, f_s\}$ be any basis of the ideal $\mathcal{I} \subset \mathcal{P}_K$. If $L^{(i)}(f_j)(0) = 0$, $\forall i, j$, then $L(f)(0) = 0$, $\forall f \in \mathcal{I}$, $\forall L \in V$.* $\blacksquare$

Before introducing the notion of continuation, let us recall the representation of differential conditions discussed in §4, introducing also the notation necessary in this and the next section.

Let $\mathcal{I} = \{f_1, \ldots, f_m\}$ be a zero-dimensional ideal, $\mathbf{q}$ be its $\mathbf{m}$ primary at the origin, $V := \Delta(\mathbf{q}) = \Delta(\mathcal{I})$ and let $\Gamma := \{L^{(1)}, \ldots, L^{(r)}\}$ be a Gauss basis of V, then $\forall \ell$, there are $c_{ij} \in K$ s.t.

$$L^{(\ell)} = \sum_{j=1}^{n} \sum_{i<\ell} c_{ij} \rho_j(L_{\geq j}^{(i)}).$$

Remark that if for some i, j there is an l s.t. $T(L^{(l)}) = \rho_j T(L_{\geq j}^{(i)})$, then any occurrence of $\rho_j(L_{\geq j}^{(i)})$ in the formula above can be replaced by Gaussian reduction with $L^{(l)}$. So in the representation of $L^{(l)}$ only terms $\rho_j(L_{\geq j}^{(i)})$ can appear s.t. $\rho_j T(L_{\geq j}^{(i)}) \notin \{T(L^{(1)}), \ldots, T(L^{(\ell-1)})\}$.

In addition the leading term $D(t)$ of $L^{(\ell)}$ must be s.t. that $\sigma_i(D(t)) \in \{T(L^{(1)}), \ldots, T(L^{(\ell-1)})\}$ for all i.

If we moreover assume that $<$ is the lexicographical ordering with $X_1 > \cdots > X_n$, it holds in particular that:

- $D(t) = \rho_\kappa T(L_{\geq \kappa}^{(\lambda)})$ and $\kappa(\ell) := \min\{j : \exists i \ c_{ij} \neq 0\}$ where $\kappa := \kappa(\ell)$ and $\lambda := \max\{i : c_{i\kappa} \neq 0\}$,
- $D(t) \in \langle X_\kappa, \ldots, X_n \rangle, \quad D(t) \notin \langle X_{\kappa+1}, \ldots, X_n \rangle$
- $L_{\geq \kappa}^{(i)} = L^{(i)}$ for all i with $c_{i\kappa} \neq 0$,
- $L^{(\ell)} \in \mathrm{Span}_K(\mathbf{D}_\kappa)$.

Let now U be the closed vector space generated by

$$\{L^{(1)}, \ldots, L^{(\ell-1)}\};$$

to find the next generator $L^{(\ell)}$ of $\Delta(\mathbf{q})$, one could try to produce an element $L = \sum_{j=1}^{n} \sum_{i<\ell} c_{ij} \rho_j(L_{\geq j}^{(i)})$, whose leading term is the minimal $D(t)$ among the possible candidates, and check whether $L(f_i)(0) = 0$ for all f_i in the given basis of $\mathcal{I}$ and whether $\sigma_i(L) \in U$ for all i. If no such element exists, then the next leading term candidate should be tried.

In our experience, the most probable reason why such an L could not exist is, that for all L with $T(L) = D(t)$, $\sigma_i(L) \notin U$ holds for some i.

The problem to be solved first is:

Given $U \subset \mathrm{Span}_K(\mathbf{D})$, closed vector space , find all $L \in \mathrm{Span}_K(\mathbf{D}) \setminus U$ s.t. $V = U + \langle L \rangle$ is closed.

Let $<$ be a semigroup ordering on $\mathbf{T}$ and let

$$\Gamma = \{L^{(1)}, \dots, L^{(r)}\}$$

be the reduced Gauss basis of U, so that necessarily $L^{(1)} = \mathrm{Id}$. Remark that the space $T(U) = \langle T(L^{(1)}), \dots, T(L^{(r)}) \rangle$ is a closed subspace.

If $L \in \mathrm{Span}_K(\mathbf{D}) \setminus U$ is such that $V = U + \langle L \rangle$ is closed, and $D(t) = T(L)$, then necessarily $D(t) \notin T(U)$, $\sigma_i(D(t)) \in T(U)\ \forall i$. Denote therefore

$$\mathcal{C}(U) := \{D(\tau) \in \mathbf{D} : D(\tau) \notin T(U), \sigma_i(D(\tau)) \in T(U)\ \forall i\}$$

which will be called the *corner set* of U and depends of course on $<$.

Let $D(t) \in \mathcal{C}(U)$; an element $L \in \mathrm{Span}_K(\mathbf{D})$ s.t.

c1) $T(L) = D(t)$

c2) $\forall j, \sigma_j(L) \in U$

c3) $L = D(t) + \sum c_i D(\tau_i), c_i \neq 0 \Rightarrow \forall i D(\tau_i) \notin T(U)$

will be called a *continuation* of U at t (omitting the dependence from $<$ which will be always assumed to be fixed in the context).

Lemma 6.2 *The following conditions are equivalent:*

1) *$V := U + \langle L \rangle$ is closed and $\Gamma \cup L$ is its reduced Gauss basis,*

2) *$D(t) := T(L) \in \mathcal{C}(U)$ and L is a continuation of U at $D(t)$.*

Lemma 6.3 *Let L' and L'' be two different continuations of U at t. Then $L' - L''$ is a continuation of U at some $\tau < t$, $D(\tau) \in \mathcal{C}(U)$.*

Proof Let L' and L'' be two continuations of U at t. Then $L' - L''$ is s.t. $\sigma_j(L' - L'') \in U\ \forall j$. Clearly it satisfies c3). Let $D(\tau) = T(L' - L'') \notin T(U)$ of course here $\tau < t$; then $\forall j\ \sigma_j(D(\tau)) \in T(U)$ so that $D(\tau) \in \mathcal{C}(U)$. Therefore $L' - L''$ is a continuation of U at τ. ∎

Corollary 6.4 *If a continuation of U at t exists, there is exactly one continuation L satisfying*

c4) if $L = D(t) + \sum c_i D(\tau_i)$ with $c_i \neq 0$, then for each $D(\tau_i) \in \mathcal{C}(U)$, there is no continuation of U at τ_i.

Proof Let $L' = D(t) + \sum c_i D(\tau_i)$, $c_i \neq 0$, be a continuation of U at t. Let τ_j be the highest term s.t. $D(\tau_j) \in \mathcal{C}(U)$ and there is a continuation L'' of U at τ_j. Then $L' - L''$ is a continuation of U at t since it obviously satisfies c1), c2), c3). Moreover let $L' - L'' = D(t) + \sum d_i D(\omega_i)$ with $d_i \neq 0$; if there is l s.t. $D(\omega_l) \in \mathcal{C}(U)$, then $\omega_l < \tau_j$. So an inductive argument allows to conclude. ∎

The continuation of U at t s.t. c1), c2), c3), c4) are satisfied will be called the *elementary continuation* of U at t and denoted $C_{U,t}$.

Proposition 6.5 *The following conditions are equivalent:*

1) *$V := U + \langle L \rangle$ is closed and $\Gamma \cup L$ is its reduced Gauss basis.*

2) *There are $t_0 > \cdots > t_s$, $D(t_i) \in \mathcal{C}(U)$ such that $L = C_{U,t_0} + \sum_{i=1}^{s} c_i C_{U,t_i}$.*

Proof 1) is satisfied if and only if L is a continuation of U. The assertion follows then from the easy remark that a continuation of U is a linear combination of elementary continuations. ∎

7 Computing elementary continuations

7.1 Computing elementary continuations under the lexicographical ordering

Let us now restrict to the case in which $<$ is the lexicographical ordering and let us give a criterion to decide if the elementary continuation of U at t exists, which is easily transformed into an algorithm to compute it.

Theorem 7.1 *Let $D(t) \in \mathcal{C}(U) \cap \mathbf{D}_\kappa$ and let $L^{(i_\kappa)} \in \Gamma$ be s.t. $T(L^{(i_\kappa)}) = \sigma_\kappa(D(t))$.*

For $\kappa \leq j \leq n$ let $I(j)$ be the set of the indices i s.t.

- *$T(\rho_j(L^{(i)})) \notin T(U)$,*
- *$T(\rho_j(L^{(i)})) < D(t)$ – so that $L^{(i)} \in \mathrm{Span}_K(\mathbf{D}_\kappa)$*
- *if $T(\rho_j(L^{(i)})) \in \mathcal{C}(U)$ then there is no elementary continuation of U at $T(\rho_j(L^{(i)}))$*

Then the following conditions are equivalent:

1) *The elementary continuation $C := C_{U,t}$ exists*

2) *The following set of $1 + 2(n-k)$ linear equations has solutions $d_{(j,i)} \in K$:*

$$\begin{aligned}
C^{(\kappa)} &= \rho_\kappa(L^{(i_\kappa)}) + \textstyle\sum_{i \in I(\kappa)} d_{(\kappa,i)} \rho_\kappa(L^{(i)}) && (c_\kappa)\\
\sigma_{\kappa+1}(C^{(\kappa)}) &= \textstyle\sum_{i \in I(\kappa+1)} d_{(\kappa+1,i)} L^{(i)}_{\leq \kappa} && (d_{\kappa+1})\\
C^{(\kappa+1)} &= \textstyle\sum_{i \in I(\kappa+1)} d_{(\kappa+1,i)} \rho_{\kappa+1}(L^{(i)}_{\geq \kappa+1}) && (c_{\kappa+1})\\
&\vdots\\
\sigma_j(\sum_{l=\kappa}^{j-1} C^{(l)}) &= \textstyle\sum_{i \in I(j)} d_{(j,i)} L^{(i)}_{\leq j-1} && (d_j)\\
C^{(j)} &= \textstyle\sum_{i \in I(j)} d_{(j,i)} \rho_j(L^{(i)}_{\geq j}) && (c_j)\\
&\vdots\\
C^{(n)} &= \textstyle\sum_{i \in I(n)} d_{(n,i)} \rho_n(L^{(i)}_{\geq n}) && (c_n)
\end{aligned}$$

Moreover, if the above conditions are satisfied, $\forall j \geq \kappa, C_j = C^{(j)}$, while $C_j = 0$ for $j < \kappa$.

Proof Let C exist. Then $\sigma_\kappa(C_\kappa) = \sigma_\kappa(C) \in U$, so $\sigma_\kappa(C_\kappa) = L^{(i_\kappa)} + \sum_i d_{(\kappa,i)} L^{(i)}$ for some $d_{(\kappa,i)}$ and $C_\kappa = \rho_\kappa(L^{(i_\kappa)}) + \sum_i d_{(\kappa,i)} \rho_\kappa(L^{(i)}) =: C^{(\kappa)}$. In the sum moreover, i is restricted to $I(\kappa)$, since otherwise there would appear in C terms $D(\tau) \in \mathcal{C}(U)$, where an elementary continuation exists, a contradiction to the assumption that C is elementary.

Assume now there are $d(j,i)$, $j < \lambda$, $i \in I(j)$ satisfying (c_κ), $(d_{\kappa+1})$, …, $(d_{\lambda-1})$, $(c_{\lambda-1})$ and s.t. moreover $C^{(j)} = C_j$ $\forall j < \lambda$.

One has $\sigma_\lambda(C) = \sigma_\lambda(\sum_{l=\kappa}^{\lambda-1} C^{(l)}) + \sigma_\lambda C_\lambda \in U$. So there are $d_{(\lambda,i)}$ s.t. $\sigma_\lambda(C) = \sum_i d_{(\lambda,i)} L^{(i)}$, which implies

$$\sigma_\lambda(\textstyle\sum_{l=\kappa}^{\lambda-1} C^{(l)}) = \sum_i d_{(\lambda,i)} L^{(i)}_{\leq \lambda-1},$$

$$\sigma_\lambda(C_\lambda) = \textstyle\sum_i d_{(j,i)} L^{(i)}_{\geq \lambda},$$

$$C^{(\lambda)} := C_\lambda = \textstyle\sum_i d_{(\lambda,i)} \rho_\lambda(L^{(i)}_{\geq \lambda}).$$

The same argument as above shows that in the sum i is restricted to $I(\lambda)$.

Conversely assume that the given system of linear equations has solutions $d_{(j,i)}$ and let $C := \sum C^{(j)}$, so that $C^{(j)} = C_j \ \forall j$. For each j one has

$$\begin{aligned}\sigma_j(C) &= \sigma_j(\sum_{l=\kappa}^{j-1} C^{(l)}) + \sigma_j(C^{(j)}) = \\ &= \sum_{i\in I(j)} d_{(j,i)} L^{(i)}_{\leq j-1} + \sum_{i\in I(j)} d_{(j,i)} L^{(i)}_{\geq j} = \\ &= \sum_{i\in I(j)} d_{(j,i)} L^{(i)}\end{aligned}$$

so that $\sigma_j(C) \in U$. Since for each (j,i), $i \in I(j)$, the leading term of C is $\rho_\kappa(T(L^{(i_\kappa)})) = D(t)$ and no term $D(\tau)$ in $\mathcal{C}(U)$ appears in the expansion of C such that a continuation of U at τ exists, nor a term $D(\tau) \in T(U)$ appears in the expansion of C, then C is the elementary continuation of U at t. ∎

In order to solve the above system of equations with good complexity, one must however use the Gauss basis $B_V = \{\rho_j(L^{(ji)})\}$. So, adopting freely the notation of Corollary 4.7, one also needs to know:

- a representation of each $L^{(i)}_{\geq j}$ w.r.t. Γ_j
- $\forall j, \forall \lambda > j, \forall i$, $\sigma_\lambda \rho_j(L^{(ji)})$.

In view of an iterative application of the algorithm, this means also that for a continuation $C = \sum c_{ji}\rho_j(L^{(ji)})$ one must be able to compute:

a) a Gauss basis of $V_j + \langle C_{\geq j}\rangle$

b) a representation of $\sigma_\lambda\rho_j(C_{\geq j})$ w.r.t. $B_V \ \forall j, \lambda > j$.

To solve item a), let us remark that each $L^{(ji)}$ itself has a unique Gauss representation as $L^{(ji)} = \sum d_{\mu\kappa}\rho_\mu(L^{(\mu\kappa)})$. Performing Gaussian elimination on the Gauss representation $C_{\geq j} = \sum c_{\mu\kappa}\rho_\mu(L^{(\mu\kappa)})$ allows both to extend the basis Γ_j and to obtain a Gauss representation of the same kind also for the new basis element (if any).

As for b), it is sufficient to give a solution for the elementary continuation obtained by the algorithm of Theorem 7.1; from the Gaussian representation $C_{\geq j} = \sum c_{\mu\kappa}\rho_\mu(L^{(\mu\kappa)})$ one obtains $\sigma_\lambda\rho_j(C_{\geq j}) = \rho_j\left(\sum c_{\mu\kappa}\sigma_\lambda\rho_\mu(L^{(\mu\kappa)})\right)$.

By assumption one knows a representation of

$$L := \sum c_{\mu\kappa}\sigma_\lambda\rho_\mu(L^{(\mu\kappa)})$$

in terms of B_V, from which (since $L \in V_j$) one obtains a representation in terms of Γ_j, $L = \sum d_i L^{(ji)}$ so that $\sigma_\lambda\rho_j(C_{\geq j}) = \sum d_i\rho_j(L^{(ji)})$.

We can now discuss the complexity of the algorithm outlined in Theorem 7.1, assuming the knowledge above. While the linear system of equations of Theorem 7.1 has a block structure which simplifies its solution, we will not take this into account in computing the complexity of solving it. We have therefore $\mathcal{O}(nr)$ unknowns $d_{(j,i)}$ imposing relations on the coefficients of the representation of $\rho_j(L^{(i)}_\nu)$ in terms of B_V and so $\mathcal{O}(nr)$ equations. The system can therefore be solved with $\mathcal{O}(n^3r^3)$ arithmetical operations in K.

Moreover each of the n auxiliary problems

- a) is a Gaussian elimination of a vector with $(n-j)r$ components over a subspace of dimension r; the total cost is therefore $\mathcal{O}(n^2r^2)$ arithmetical operations in K.
- b) it is again a set of Gaussian eliminations and so the complexity is the same.

7.2 Computing elementary continuations under any term ordering

If $<$ is not the lexicographical ordering, elementary continuations can still be computed by linear algebra, but the block structure of the equations coming from Theorem 7.1 is lost. We have however:

Proposition 7.2 *Let $D(t) \in \mathcal{C}(U)$ and let $L^{(\kappa\lambda)} \in \Gamma_\kappa$ be s.t. $\rho_\kappa T(L^{(\kappa\lambda)}) = D(t)$.*

Denote by $J(j)$, for $1 \leq j \leq n$, the set of the indices i s.t.

a) $T(\rho_j(L^{(ji)})) \notin T(U)$,

b) $T(\rho_j(L^{(ji)})) < D(t)$

c) if $T(\rho_j(L^{(ji)})) \in \mathcal{C}(U)$ then there is no elementary continuation of U at $T(\rho_j(L^{(i)}))$.

The following conditions are equivalent:

1) The elementary continuation $C_{U,t}$ exists

2) The following set of linear equations

$$\sigma_\mu\rho_\kappa(L^{(\kappa\lambda)}) + \sum_{j=1}^{n}\sum_{i\in J(j)} c_{(ji)}\sigma_\mu\rho_j(L^{(ji)}) = \sum_{i=1}^{n} d_{\mu i}L^{(1i)}$$

for $\mu = 2, \ldots, n$ has solutions $c_{(ji)}, d_{\mu i} \in K$:

Moreover, if the above conditions are satisfied,

$$C_{U,t} = \rho_\kappa(L^{(\kappa\lambda)}) + \sum_{j=1}^{n}\sum_{i\in J(j)} c_{(ji)}\rho_j(L^{(ji)}).$$

Proof If $C_{U,t} = \rho_\kappa(L^{(\kappa\lambda)}) + \sum_{j=1}^{n}\sum_{i=1}^{r_j} c_{(ji)}\rho_j(L^{(ji)})$, then $c_{(ji)} = 0$ unless $i \in J(j)$ since in the expansion of $C_{U,t}$ there is no term in $T(U)$, nor terms in $\mathcal{C}(U)$ having elementary continuations and moreover $D(t) = T(C_{U,t}) = \rho_\kappa T(L^{(\kappa\lambda)}) > T(\rho_j L^{(ji)})$ for each pair (j,i) s.t. $c_{(ji)} \neq 0$. Moreover $\sigma_\mu(C_{U,t}) \in U$, so that there are $d_{\mu i}$ s.t. $\sigma_\mu(C_{U,t}) = \sum_{i=1}^{n} d_{\mu i}L^{(1i)}$.

Conversely let

$$C = \rho_\kappa(L^{(\kappa\lambda)}) + \sum_{j=1}^{n}\sum_{i\in J(j)} c_{(ji)}\rho_j(L^{(ji)})$$

be such that $\sigma_\mu(C) = \sum_{i=1}^{n} d_{\mu i}L^{(1i)}$; since

$$\sigma_1(C) = \sum_{i\in J(1)} c_{(1i)}\rho_1(L^{(1i)}) \in U,$$

then $U + \langle C\rangle$ is closed. Since the sum is restricted on $J(j)$, C is the continuation of U at t. ∎

The algorithm needs to solve $\mathcal{O}(n^2r)$ equations in $\mathcal{O}(nr)$ unknowns and so $\mathcal{O}(n^4r^3)$ arithmetical operations in K.

8 An algorithm to compute a primary component at the origin of a 0-dim. ideal

After this discussion on elementary continuation, we now present an algorithm s.t. given a basis $\{f_1, \ldots, f_m\}$ of a 0-dimensional ideal $\mathcal{I} \subset \mathcal{P}$ vanishing at the origin allows to compute the closed vector space $\Delta(\mathcal{I}) = \Delta(\mathbf{q})$ of differential conditions defining $\mathbf{q}$, the primary component at the origin of $\mathcal{I}$.

The algorithm uses the following data:

- $\Gamma_i = \{L^{(i1)}, \ldots, L^{(i\kappa_i)}\}$ a Gauss basis for the projection U_i of a closed space U of differential conditions, $i = 1, \ldots, n$.
- $\Lambda := \{C_{U,\tau} : D(\tau) < T(L^{(\kappa)})\}$, (The algorithms outlined in §7 to compute $C_{U,\tau}$ for each $\tau \in \mathcal{C}(U)$ are used here.)
- $\mathcal{B} := \{\tau \in \mathcal{C}(U) : D(\tau) > T(L^{(\kappa)})\}$.

At initialization: $\Gamma_i := \{L^{(i1)}\}$ where $L^{(i1)} = Id$,
$\Lambda := \emptyset$, $\mathcal{B} := \{D(X_i) : i = 1, \ldots, n\}$.
At termination: Γ_1 is the reduced Gauss basis of $\Delta(\mathcal{I})$,
$\Lambda := \{C_{U,\tau} : \tau \in \mathcal{C}(U)\}$, $\mathcal{B} := \emptyset$.

Repeat
$t := \min_{\mathcal{B}}(\tau)$
$\mathcal{B} := \mathcal{B} \setminus \{t\}$
If $C_{U,t}$ exists **then**
  If $\exists c_\tau \in K \ \forall j = 1 \ldots, m :$
    $C_{U,t}(f_j)(0) = \sum_{C_{U,\tau} \in \Lambda} c_\tau C_{U,\tau}(f_j)(0)$
  then
    $\kappa_1 := \kappa_1 + 1$,
    $L^{(1\kappa_1)} := C_{U,t} - \sum_{C_{U,\tau} \in \Lambda} c_\tau C_{U,\tau}$,
    $\Gamma_1 := \Gamma_1 \cup \{L^{(1\kappa_1)}\}$
    For $j = 2 \ldots n$ **do**
      $L := \text{Gaussreduction}(L^{(1\kappa_1)}_{\geq j}, \Gamma_j)$,
    If $L \not\equiv 0$ **then**
      $\kappa_j := \kappa_j + 1$,
      $L^{(j\kappa_j)} := L$,
      $\Gamma_j := \Gamma_j \cup \{L^{(j\kappa_j)}\}$
      $\mathcal{B} := \mathcal{B} \cup \{\rho_j(D(t)) : j = 1, \ldots, n, X_j t \in \mathcal{C}(U)\}$
    else
      $\Lambda := \Lambda \cup \{C_{U,t}\}$
until $\mathcal{B} = \emptyset$

As an example we compute the differential conditions of degree at most 6 of the *node*, i.e. the primary at the origin $\mathbf{q} = \mathcal{I} + \mathbf{m}^6 \in K[X,Y]$ where $\mathcal{I} = (Y^2 - X^2 - X^3)$, $\mathbf{m} = (X, Y)$, so $\mathbf{q} = (f_1, f_2, f_3)$, with

$$f_1 = Y^2 - X^2 - X^3, f_2 = X^5 Y, f_3 = X^6$$

(see Figure 2). [4]

[4] The ordering is the lex one with $X < Y$. The differential conditions produced are:

$$\begin{aligned}
L^{(1)} &= D(1) \\
L^{(2)} &= D(X) \\
\mathcal{C}_{X^2} &= D(X^2) \\
L^{(3)} &= D(Y) \\
L^{(4)} &= D(XY)
\end{aligned}$$

$$\begin{aligned}
\mathcal{C}_{Y^2} &= D(Y^2) \\
L^{(5)} &= D(Y^2) + D(X^2) \\
\mathcal{C}_{XY^2} &= D(XY^2) + D(X^3) \\
L^{(6)} &= D(XY^2) + D(X^3) + D(X^2) \\
L^{(7)} &= D(Y^3) + D(X^2Y) \\
L^{(8)} &= D(XY^3) + D(X^3Y) + D(X^2Y) \\
L^{(9)} &= D(Y^4) + D(X^2Y^2) + D(X^4) + D(X^3) \\
\mathcal{C}_{XY^4} &= D(XY^4) + D(X^3Y^2) + D(X^2Y^2) + \\
&\quad + D(X^5) + 2D(X^4) + D(X^4) \\
\mathcal{C}_{Y^5} &= D(Y^5) + D(X^2Y^3) + D(X^4Y) + D(X^3Y)
\end{aligned}$$

9 Representation of roots

All over the paper, given a root $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{k}^n$ of an ideal $\mathcal{I}$, we assumed it were the origin by means of the translation $X_i \mapsto X_i + a_i$. Of course making this assumption we need to specify some points:

1) Obviously we must assume to be able to compute over the field $K = k(a_1, \ldots, a_n)$
2) and apparently to precompute the roots of $\mathcal{I}$;
3) in our complexity analisys we computed the number of operations in K and we should at least be able to reduce them to operations in k.

The aim of this section is to discuss these points, reducing them to a presentation of the current reflection about the meaning of solving systems. In particular we will recall briefly different ways of representing the roots of a zero-dimensional ideal, and indicate how to perform arithmetical operations over arithmetical expressions of its roots. As a consequence of that, the points above will be disposed of.

Informally speaking an elementary "arithmetical expression" over a root $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbf{k}^n$ of a zero-dimensional ideal $\mathcal{I}$ is either:

Notes

(1) The computation of $\sigma_Y(L^{(4)})$ (and analogous computations) are obtained by $\sigma_X(L^{(4)}) = \sigma_X\rho_Y(L^{(2)}) = \rho_Y(L^{(1)}) = L^{(3)}$, the last but one equality is in the table itself.

(2) The computation of $L := \sigma_X\rho_Y(L^{(4)})$ (and analogous computations) are obtained by
$L = \rho_Y\sigma_X\rho_Y(L^{(2)}) = \rho_Y\rho_Y(L^{(1)}) = \rho_Y(L^{(3)})$.

(3) The computation of $\mathcal{C}_{XY^2}$ is as follows:
one computes $\sigma_X\rho_Y(L^{(4)}) = \rho_Y(L^{(3)}) = L^{(5)}_{\leq Y}$, from which one deduces $\mathcal{C}_{XY^2} = \rho_Y(L^{(4)}) + \rho_X(L^{(5)}_{\geq X}) = \rho_Y(L^{(4)}) + \rho_X(\mathcal{C}_{X^2})$.
One also has
$\sigma_X\rho_Y(\mathcal{C}_{XY^2}) = \sigma_X\rho_Y\rho_Y(L^{(4)}) + \sigma_X\rho_Y\rho_X(\mathcal{C}_{X^2}) =$
$= \rho_Y(\mathcal{C}_{Y^2}) + \rho_Y(\mathcal{C}_{X^2}) = \rho_Y(L^{(5)})$, since $\sigma_X\rho_Y(L^{(4)}) = \rho_Y(L^{(3)}) = \mathcal{C}_{Y^2}$ and
$\sigma_X\rho_Y\rho_X(\mathcal{C}_{X^2}) = \rho_X(\mathcal{C}_{X^2})$

(4) $\sigma_X(L^{(8)}) = \sigma_X\rho_Y(L^{(6)}) =$
$\rho_Y\sigma_X(L^{(6)}) = \rho_Y(L^{(5)}) + \rho_Y(L^{(2)}) = L^{(7)} + L^{(4)}$

(5) The computation of $\mathcal{C}_{XY^4}$ gives $\sigma_Y(L^{(8)})$ and so one has to compute $\sigma_X\rho_Y(L^{(8)}) = \rho_Y(L^{(7)}) + \rho_Y(L^{(4)}) = L^{(9)} + L^{(6)}$ from which one gets $\mathcal{C}_{XY^4} = \rho_Y(L^{(8)}) + \rho_X(L^{(X9)}) + \rho_X(L^{(X6)})$

Figure 1: The example

$\mathbf{t}$	Δ		$\sigma_X(\Delta)$	$\sigma_Y(\Delta)$	$\sigma_X\rho_Y(\Delta)$	$\Delta(f_1)(0)$	$\Delta(f_2)(0)$	$\Delta(f_3)(0)$	
1	$L^{(1)}$	$D(1)$	0	0	0	0	0	0	
X	$L^{(2)}$	$\rho_X(L^{(1)})$	$L^{(1)}$	0	$\rho_Y(L^{(1)})$	0	0	0	
X^2	$\mathcal{C}_{X^2}$	$\rho_X(L^{(2)})$	$L^{(2)}$	0	$\rho_Y(L^{(1)})$	-1	0	0	
Y	$L^{(3)}$	$\rho_Y(L^{(1)})$	0	$L^{(1)}$	0	0	0	0	
XY	$L^{(4)}$	$\rho_Y(L^{(2)})$	$L^{(3)}(\mathbf{1})$	$L^{(2)}$	$\rho_Y(L^{(3)})(\mathbf{2})$	0	0	0	
Y^2	$\mathcal{C}_{Y^2}$	$\rho_Y(L^{(3)})$	0	$L^{(3)}$	0	1	0	0	
	$L^{(5)}$	$\mathcal{C}_{Y^2}+\mathcal{C}_{X^2}$	$L^{(2)}$	$L^{(3)}$	$\rho_Y(L^{(2)})$	0	0	0	
XY^2	$\mathcal{C}_{XY^2}$	$\rho_Y(L^{(4)})+\rho_X(L^{(X5)})$	$L^{(5)}$	$L^{(4)}$	$\rho_Y(L^{(5)})$	-1	0	0	(**3**)
	$L^{(6)}$	$\mathcal{C}_{XY^2}+\mathcal{C}_{X^2}$	$L^{(5)}+L^{(2)}$	$L^{(4)}$	$\rho_Y(L^{(5)})+\rho_Y(L^{(2)})$	0	0	0	
Y^3	$L^{(7)}$	$\rho_Y(L^{(5)})$	$L^{(4)}$	$L^{(5)}$	$\rho_Y(L^{(4)})$	0	0	0	
XY^3	$L^{(8)}$	$\rho_Y(L^{(6)})$	$L^{(7)}+L^{(4)}(\mathbf{4})$	$L^{(6)}$	$\rho_Y L^{(7)})+\rho_Y L^{(4)})$	0	0	0	
Y^4	$L^{(9)}$	$\rho_Y(L^{(7)})+\rho_X(L^{(X6)})$	$L^{(6)}$	$L^{(7)}$	$\rho_Y L^{(8)})$	-1	0	0	
XY^4	$\mathcal{C}_{XY^4}$	$\rho_Y(L^{(8)})+\rho_X(L^{(X9)})+\rho_X(L^{(X6)})$	$L^{(9)}+L^{(6)}$	$L^{(8)}$	$\rho_Y(L^{(9)})+\rho_Y(L^{(6)})$	-1	1	0	(**5**)
Y^5	$\mathcal{C}_{Y^5}$	$\rho_Y(L^{(9)})+\rho_X(L^{(X9)})+\rho_X(L^{(X6)})$	$L^{(8)}+L^{(6)}$	$L^{(9)}$	$\rho_Y(C_{XY^4})_{\leq Y}$	0	0	-1	

- the assigment of a_i for some i,
- the sum, difference or the product of two arithmetical expressions,
- the inverse of a non-zero arithmetical expression,

and an "arithmetical operation" is either one of the four elementary operations (to which one could add extractions of p-th roots over fields of finite characteristic p) or testing whether an arithmetical expression is 0.

Observe, however, that an "arithmetical expression" is not exactly an algebraic number in $k[a_1,\ldots,a_n]$, it is rather a set of instructions in prescribed order which, applied to $(a_1,\ldots,a_n)$ produce such an algebraic number, and these instructions could include "branching" ones, like

$$\textbf{if } exp_1 = 0 \textbf{ then } exp_2 := exp_3 \textbf{ else } exp_2 = (exp_1)^{-1}.$$

In fact a likely scenario is one in which the same complex computation is to be performed over *all* roots of a 0-dimensional ideal, but, due to the different arithmetical behaviour of different roots, branchings occur and lead to totally different computations.

Example 9.1 For instance one could ask whether the polynomial $g_a(Z) = Z^3 + 3aZ^2 + 12Z + 4a$ is squarefree, where a is *any* root of $f(X) = X^4 - 13X^2 + 36$, i.e. $a = \pm 2, \pm 3$. This requires computing $\gcd(g_a, g_a')$ and testing if it is constant.

It is easy to verify that the remainder of the division of g_a by g_a' is $(8-2a^2)Z$, so the remainder is 0 (and $g_a = (Z+a)^3$) if $a = \pm 2$, while it is non-zero if $a = \pm 3$ requiring an (obvious!) further polynomial division to find that g_a is squarefree.

Our interest will be therefore to describe representations for the algebraic numbers which are obtained by evaluating an arithmetical expression in one or all the roots of a zero-dimensional ideal, and to evaluate the space complexity of such a representation and the time complexity for performing an arithmetical operation over two algebraic numbers so represented. Let us fix a 0-dimensional $\mathcal{I} \subset \mathcal{P}$ and a root $\mathbf{a} = (a_1,\ldots,a_n) \in \mathbf{k}^n$ of $\mathcal{I}$. We will denote $K = k(a_1,\ldots,a_n)$ the minimal algebraic extension of k containing $\mathbf{a}$, $\mathbf{n} = (X_1 - a_1,\ldots,X_n - a_n) \subset \mathcal{P}_K$ the linear maximal ideal whose root is $\mathbf{a}$, $\mathbf{p}$ the $\mathbf{n}$-primary component of $\mathcal{I}_K$, $\mathbf{m} = \mathbf{n} \cap \mathcal{P}$ the maximal ideal in $\mathcal{P}$ whose roots are $\mathbf{a}$ and its k-conjugates, $\mathbf{q} = \mathbf{p} \cap \mathcal{P}$ the $\mathbf{m}$-primary component of $\mathcal{I}$.

Moreover we will set $t := t_{\mathbf{a}} := \dim_k(K) = \mathrm{mult}(\mathbf{m})$, the number of roots which are k-conjugate to $\mathbf{a}$,

$$v := v_{\mathbf{a}} := \mathrm{mult}(\mathbf{p}), \quad r := r_{\mathbf{a}} := tv = \mathrm{mult}(\mathbf{q})$$

and since we are interested in the cost of a same computation over all roots of $\mathcal{I}$, we set $u := \mathrm{mult}(\sqrt{\mathcal{I}})$, which is the number of different roots.

If $\mathcal{A}$ is a set containing a single element from each set of k-conjugate roots of $\mathcal{I}$, one has

$$u = \sum_{\mathbf{a}\in\mathcal{A}} t_{\mathbf{a}}, \quad s = \sum_{\mathbf{a}\in\mathcal{A}} r_{\mathbf{a}} = \sum_{\mathbf{a}\in\mathcal{A}} t_{\mathbf{a}} v_{\mathbf{a}}.$$

Depending on the representation of roots, we get different complexities for the arithmetical operations.

9.1 Representation by a tower of algebraic extensions

The classical way to represent $\mathbf{a}$ is Kronecker's representing of K as a tower of simple algebraic extensions. Let $K_i := k(a_1,\ldots,a_i)$, with $K_0 = k$ and $K = K_n$, $d_i := \dim_{K_{i-1}}(K_i)$, $\phi_i : k[X_1,\ldots,X_n] \longrightarrow K_i[X_{i+1},\ldots,X_n]$.

Then, for each i, there is a unique monic polynomial $f_i \in K(X_1,\ldots,X_{i-1})[X_i]$ s.t.

- $\phi_{i-1}(f_i)$ is the minimal polynomial of a_i over K_{i-1}, so that $K_i \simeq K_{i-1}[X_i]/f_i$,
- $\deg_{X_j}(f_i) < d_j$ for $j < i$, $\deg_{X_i}(f_i) = d_i$,
- $\mathbf{m} = (f_1,\ldots,f_n)$ (this last assertion is known as "Nulldimensionaler Primbasissatz").

As a k-vector space, K is identifiable with the subspace of $\mathcal{P}$ whose basis is the set of terms $\mathbf{N}(\mathbf{d})$, $\mathbf{d} = (d_1,\ldots,d_n)$, so to represent each element of K one needs to store $t = \prod d_i$ elements in k and the information needed to encode K (i.e. the $f_i's$) requires storing $\mathcal{O}(nt)$ elements of k.

This identification is extended to a field isomorphism by defining recursively product and inverse computation over $\mathrm{Span}_{K_{i-1}}(1,\ldots,X_i^{d_i-1})$ by division-with-remainder and by

Bezout identity (i.e. by the half-extended euclidean algorithm). Both algorithms have a complexity of $\mathcal{O}(d_i^2)$ arithmetic operations over K_{i-1} so an arithmetic operation in K has a cost of $\mathcal{O}(t^2)$ operations in k. In this representation an element is 0 if and only if it is represented as such.

If $\mathbf{b} = (b_1, \ldots, b_n)$ is a k-conjugate root of $\mathbf{a}$, i.e. an other root of $\mathbf{m}$, then $k(b_1, \ldots, b_i) \simeq K_i$; therefore in this model one needs to represent only one root for each conjugacy class for a total space requirement of $\sum_{\mathbf{a} \in \mathcal{A}} \mathcal{O}(nt) = \mathcal{O}(nu)$ elements in k; to represent an arithmetic expression over each root of $\mathcal{I}$ one needs to represent it once for each conjugacy class, for a total storage of $u = \sum_{\mathbf{a} \in \mathcal{A}} t_{\mathbf{a}}$ elements in k and to perform an arithmetical operation one needs $\sum_{\mathbf{a} \in \mathcal{A}} \mathcal{O}(t_{\mathbf{a}}^2) \leq \mathcal{O}(u^2)$ operations in k.

Remark that given $\mathcal{I}$, to be able to represent its roots in this model, one needs to perform a primary decomposition of $\mathcal{I}$ or a prime decomposition of $\sqrt{\mathcal{I}}$ and this requires the ability of factorizing univariate polynomials over simple algebraic extensions of k; while algorithms to do that are known, they can hardly be considered efficient.

9.2 Representation by a simple algebraic extension

Let $\mathbf{c} = (c_2, \ldots, c_n) \in k^{n-1}$ and let $L_{\mathbf{c}} : \mathcal{P} \longrightarrow \mathcal{P}$ be the linear change of coordinates defined by:

$$L_{\mathbf{c}}(X_i) = \begin{cases} X_1 + \sum_{j=2}^{n} c_j X_j & \text{i =1} \\ X_i & i > 1 \end{cases}$$

If $(a_1, \ldots, a_n)$ is a root of $\mathcal{I}$ the corresponding root of $L_{\mathbf{c}}(\mathcal{I})$ is then $(a_1 - \sum_{i=2}^{n} c_i a_i, a_2, \ldots, a_n)$.

By the (misnomed) Primitive Element Theorem, denoting $a^{(\mathbf{c})} := a_1 - \sum_{i=2}^{n} c_i a_i$, there is a Zariski open set $U \subset k^{n-1}$ s.t. $\forall \mathbf{c} \in U$, $K = k[a^{(\mathbf{c})}]$ and two different roots of $L_{\mathbf{c}}(I)$ have different first coordinates.

For such a $\mathbf{c}$ there are therefore a monic irreducible polynomial $g_1 \in k[X_1]$ of degree t, and polynomials $g_2, \ldots, g_n \in k[X_1]$ of degree less than t, s.t.

- g_1 is the minimal polynomial of $a^{(\mathbf{c})}$,
- $\forall i > 1$, $a_i = g_i(a^{(\mathbf{c})})$,
- $L_{\mathbf{c}}(\mathbf{m}) = (g_1, X_2 - g_2, \ldots, X_n - g_n)$ (this last assertion is known as "nulldimensionaler allgemeiner Primbasissatz").

The field K can be identified as in the paragraph above with the vector space $\mathrm{Span}_k(1, X_1, \ldots, X_1^{t-1})$; the storage requirements are therefore still $\mathcal{O}(nt)$ for the field, and t for an arithmetic expression and the cost of the arithmetics $\mathcal{O}(t^2)$ ($\mathcal{O}(nu)$, u and $\mathcal{O}(u^2)$ respectively over all the roots); remark however that the coefficients of the g_i's are usually much larger than those of the f_i's of the previous paragraph. On the other side, extracting a root of $L_{\mathbf{c}}(I)$ requires now only polynomial factorization over k.

9.3 Representation by a squarefree triangular set

In order to avoid the requirement for costly polynomial factorization, Duval [D] proposed her "dynamic-evaluation" model, which started a series of "weak" models for the arithmetics of algebraic numbers recently introduced.

Let us first describe how to represent a simple algebraic extension $k[a]$ in this model and then we will see how to represent towers. Let $f \in k[X_1]$ be a squarefree polynomial of degree d s.t. $f(a) = 0$, let $f = f_1 \cdots f_l$ be its factorization (introduced only for theoretical purposes, since the aim of this model is to avoid factorization at all); let a_i be a root of f_i and to fix notation let us assume that $a = a_1$; then by the Chinese Remainder Theorem one has:

$$k[X_1]/f \simeq \bigoplus_{i=1}^{l} k[X_1]/f_i \simeq \bigoplus_{i=1}^{l} k[a_i]$$

so that, denoting by ψ the canonical projection of $k[X_1]/f$ over $k[a]$, each element of the latter field can be (non u/nique/-ly) represented by any counterimage in $k[X_1]/f$, requiring the storage of d elements in k.

Since ψ is a ring morphism the three ring operations over $k[a]$ can be performed over $\mathrm{Span}_k(1, X_1, \ldots, X_1^{d-1})$ as we have seen in the preceding models at a cost of $\mathcal{O}(d^2)$ arithmetical operations in k. However, since $k[X_1]/f$ has zero divisors, testing for equality to zero and inverting an element of $k[a]$ is no more evident.

Example 9.2 Let us go back to the preceding example, where we were computing $\gcd(g_a, g_a')$ for $g_a(Z) = Z^3 + 3aZ^2 + 12Z + 4a$, where a is *any* root of $f(X) = X^4 - 13X^2 + 36$, and let us perform it with coefficients in $k[X]/f$. The first polynomial division requires only the ring arithmetics of $k[X]/f$ and produces

$$g_a(Z) = \frac{1}{3}(Z + a) g_{\mathbf{a}}'(Z) + (8 - 2a^2)Z$$

The next division requires dividing g_a' by $(8 - 2a^2)Z$, so that we first need to know whether $8 - 2a^2$ is zero or not, since:

- if $8 - 2a^2 = 0$, then the euclidean algorithm is ended, $\gcd(g_a, g_a') = g_a'$, whence $g_a = (Z + a)^3$
- if $8 - 2a^2 \neq 0$, then, after inverting it, a further (obvious) division is needed (again requiring only ring operations in $k[X]/f$), which produces

$$g_a'(Z) = (8 - 2a^2)^{-1}(3Z + 6a)(8 - 2a^2)Z + 12$$

whence one concludes $\gcd(g_a, g_a') = 1$.

Of course, the answer depends by which root of f a is: in fact if $a = \pm 2$ then $8 - 2a^2 = 0$, if $a = \pm 3$ then $8 - 2a^2 \neq 0$.

The "pons asinorum" here is that there is no need to compute the roots of f in order to answer: in fact, since a is a root of f, $h(a) = 0$ if and only if a is a root of $f^{(0)} = \gcd(f, h)$ while $h(a) \neq 0$ if a is a root of $f^{(1)} = f/f^{(0)}$, in which case its inverse can be computed by the half-extended Euclidean algorithm applied to h and $f^{(1)}$.

Example 9.2 (cont'd) In the above example one gets $f^{(0)} = gcd(X^4 - 13X^2 + 36, 8 - 2X^2) = X^2 - 4$, $f^{(1)} = f/f^{(0)} = X^2 - 9$, finding a partial factorization of f with no recourse to a factorization algorithm.

Anytime one needs to test if an expression $h(a)$ is zero, one therefore has to perform the computation $\gcd(f, h)$ and if the result is non trivial one obtains a partial decomposition

$$k[X_1]/f = k[X_1]/f^{(0)} \oplus k[X_1]/f^{(1)}.$$

The computation can then be continued on the summand of which a is a root (if this can be decided, say e.g. if a is the only real, or the only positive, root of f) or separately on both summands.

Having discussed in detail Duval's model for a simple extension, let us discuss its multivariate generalization. In Duval's model a root $\mathbf{a} = (a_1, \ldots, a_n)$ is given if monic polynomials $f_i \in k(X_1, \ldots, X_{i-1})[X_i]$ are given s.t.

- $\forall (b_1, \ldots, b_{i-1})$ root of $(f_1, \ldots, f_i) \subset k[X_1, \ldots, X_n]$ the polynomial $f_i(b_1, \ldots, b_{i-1}, X_i)$ is squarefree (a condition which can be tested by a gcd computation over $k[b_1, \ldots, b_i]$ so that the test can be inductively performed in this model)
- $\deg_{X_i}(f_j) < d_i \ \forall j > i$
- $f_i(a_1, \ldots, a_i) = 0 \ \forall i$

This allows to represent elements of $k[a_1, \ldots, a_n]$ by elements of $\mathrm{Span}_k(\mathbf{N}(\mathbf{d}))$, $\mathbf{d} = (d_1, \ldots, d_n)$ and to perform there ring operations. However anytime a zero-testing or an inversion is needed, this is performed by gcd computations over $k(a_1, \ldots, a_{n-1})[X_n]$ and this could lead to a splitting $f_n = f_n^{(0)} f_n^{(1)}$.

Remark that such gcd computations require the field arithmetics of $k(a_1, \ldots, a_{n-1})$, which is performed recursively in the representation $k[X_1, \ldots, X_{n-1}]/(f_1, \ldots, f_{n-1})$ and so could itself, recursively, produce splitting at lower levels.

A set of polynomials $\{f_1, \ldots, f_n\}$ satisfying the conditions above is known as a *triangular set*; algorithms ([L89, M]) are known which given a (Gröbner) basis of a zero-dimensional ideal $\mathcal{I}$ allow to produce a family of triangular sets whose roots are disjoint and such that each root of $\mathcal{I}$ is a root of one of them. The sum of the k-dimensions of these triangular sets is therefore exactly u, so that representing the triangular sets requires storing $\mathcal{O}(nu)$ elements in k, representing an arithmetical expression of a root (or of all roots) requires storing u elements in k and performing an arithmetical operation over all roots $\mathcal{O}(u^2)$ arithmetical operations in k.

9.4 Representation by the Shape Lemma

As with the classical model, the Primitive Element Theorem allows to avoid recursion also in the model above; in fact an obvious generalization of it, the so-called Shape Lemma ([GM]) asserts that if $\mathcal{I}$ is a radical zero-dimensional ideal (and each ideal generated by a triangular set is such), then there is a Zariski open set $U \subset k^{n-1}$ s.t. $\forall \mathbf{c} \in U$, $\mathrm{L}_c(I) = (g_1(X_1), X_2 - g_2(X_1), \ldots, X_n - g_n(X_1))$ where g_1 is monic and squarefree and $deg(g_i) < deg(g_1) \ \forall i$.

This allows to represent $k[\mathbf{a}]$ à la Duval by $k[X_1]/f_1$. Again, the advantage (if any) of avoiding recursive splitting is to be compensated by the larger coefficients appearing in g_1 and in the g_i's.

The space and time complexity of this model are again $\mathcal{O}(nu), \mathcal{O}(u), \mathcal{O}(u^2)$ respectively.

9.5 Representation by a simple squarefree extension

At least the disadvantage represented by the size of the coefficients of the g_i's , $i > 1$, in the model above can be circumvented by a proposal contained in [ABRW]. The polynomial g_i is just needed to give a representation of a_i as an expression in $a_\mathbf{c} = a_1 - \sum_{i=2}^{n} c_i a_i$. Any other representation of the form f/h where $h, f \in k[X_1]/g_1$ and h is invertible is equally good. They show in particular that there are polynomials f_i s.t. $a_i = f_i(a_\mathbf{c})/g_1'(a_\mathbf{c})$ and that they usually have much smaller coefficients than the g_i's. On the one hand the coefficient operations are simpler by dealing with shorter coefficients, on the other hand the coefficients are here rational numbers with denominators from $S := \{g_1'(a_\mathbf{c})^i | i \geq 0\}$. For getting the complexity, one needs a more detailed analysis. This is not yet done.

9.6 Representation by a radical border basis

If $\mathcal{I}$ is a zero-dimensional ideal, the artinian algebra $A = \mathcal{P}/\mathcal{I}$ is isomorphic as a k-vector space to $\mathrm{Span}_k(\mathbf{N}(\mathcal{I}))$ and as a k-algebra to $\bigoplus_{\mathbf{a} \in \mathcal{A}} \mathcal{P}/\mathbf{q_a}$ where $\mathbf{q}_a$ is the primary component of $\mathcal{I}$ whose roots are $\mathbf{a}$ and its conjugates. Therefore one has

$$\mathrm{Span}_k(\mathbf{N}(\sqrt{\mathcal{I}})) \simeq \mathcal{P}/\sqrt{\mathcal{I}} \simeq \bigoplus_{\mathbf{a} \in \mathcal{A}} \mathcal{P}/\mathbf{m_a} \simeq \bigoplus_{\mathbf{a} \in \mathcal{A}} k[\mathbf{a}]$$

so that, exactly as in Duval's model, denoting ψ the canonical morphism of $\mathrm{Span}_k(\mathbf{N}(\sqrt{\mathcal{I}}))$ over $k[\mathbf{a}]$, each element of the latter field can be (non uniquely) represented by any counterimage in $\mathrm{Span}_k(\mathbf{N}(\sqrt{\mathcal{I}}))$, requiring the storage of $\mathrm{card}(\mathbf{N}(\sqrt{\mathcal{I}})) = \mathrm{mult}(\sqrt{\mathcal{I}}) = u$ elements in k. This representation has been proposed in [MT] where it is called the "natural" representation.

The multiplication in $\mathcal{P}/\sqrt{\mathcal{I}}$ can be performed in the isomorphic copy $\mathrm{Span}_k(\mathbf{N}(\sqrt{\mathcal{I}}))$ by Gröbner basis techniques: if $f, g \in \mathrm{Span}_k(\mathbf{N}(\sqrt{\mathcal{I}}))$, then $Can(fg, \sqrt{\mathcal{I}})$ is in the same residue class as fg and belongs to $\mathrm{Span}_k(\mathbf{N}(\sqrt{\mathcal{I}}))$; if the *border basis* of $\sqrt{\mathcal{I}}$ is stored (i.e. the set $\{\tau - Can(\tau, \sqrt{\mathcal{I}}) : \tau \in \mathbf{B}(\sqrt{\mathcal{I}}) \backslash \mathbf{N}(\sqrt{\mathcal{I}})\}$), the product can be computed by linear algebra techniques with $\mathcal{O}(u^3)$ complexity; to store a border basis one needs to store $\mathcal{O}(nu^2)$ elements in k.

Inversion and zero-testing presents the same difficulty that in Duval's model, and it is done by the ideal theoretic generalization of gcd's: if $h(X_1, \ldots, X_n) \in \mathrm{Span}_k(\mathbf{N}(\sqrt{\mathcal{I}}))$, then:

- $h(\mathbf{a}) = 0$ if and only if $\mathbf{a}$ is a root of $\mathcal{J}^{(0)} := \sqrt{\mathcal{I}} + (\sqrt{h})$,
- $h(\mathbf{a}) \neq 0$ if and only if $\mathbf{a}$ is a root of $\mathcal{J}^{(1)} := \sqrt{\mathcal{I}} : h = \{f \in \mathcal{P} : hf \in \sqrt{\mathcal{I}}\}$,
- $\mathcal{P}/\sqrt{\mathcal{I}} = \mathcal{P}/\mathcal{J}^{(0)} \oplus \mathcal{P}/\mathcal{J}^{(1)}$.

A representation by border bases of both $\mathcal{P}/\mathcal{J}^{(0)}$ and $\mathcal{P}/\mathcal{J}^{(1)}$ can be computed by linear algebra techniques at a $\mathcal{O}(nu^3)$ complexity.

The flexibility of this presentation (any Gröbner basis can be used instead than the lexicographical one, implicitly used in Duval's model) and the absence of recursion, are compensated by a higher complexity: $\mathcal{O}(nu^2)$ to store the field, $\mathcal{O}(u)$ to store a single element, $\mathcal{O}(nu^3)$ for arithmetical operations.

9.7 Representation by a border basis

With the "natural" representation, one is not restricted to work with radical ideals. In fact, similar to 2.6 one has

$$\mathrm{Span}_k(\mathbf{N}(\mathcal{I})) \simeq \mathcal{P}/\mathcal{I} \simeq \bigoplus_{\mathbf{a} \in \mathcal{A}} \mathcal{P}/\mathbf{q_a} \xrightarrow{\pi} \bigoplus_{\mathbf{a} \in \mathcal{A}} k[\mathbf{a}],$$

with a projection π.
For polynomials $h(X_1, \ldots, X_n) \in \mathrm{Span}_k(\mathbf{N}(\mathcal{I}))$, the following holds:

- $h(\mathbf{a}) = 0$ if and only if $\mathbf{a} \in \mathcal{A}$ is a root of $\mathcal{I} + (h)$
- $h(\mathbf{a}) \neq 0$ if and only if $\mathbf{a} \in \mathcal{A}$ is a root of $\mathcal{I} : h^* := \{f \in \mathcal{P} : \exists \mu \ h^\mu f \in \mathcal{I}\}$.

There is an integer s s.t. $\mathcal{I} : h^* = \{f \in \mathcal{P} : h^s f \in \mathcal{I}\} =: \mathcal{I} : h^s$. Using $\mathcal{I}^{(0)} := \mathcal{I} + (h^s) \subset \mathcal{I} + (h)$ and $\mathcal{I}^{(1)} := \mathcal{I} : h^s$, one gets $\mathcal{I} = \mathcal{I}^{(0)} \cup \mathcal{I}^{(1)}$ with

$$\mathrm{Span}_k(\mathbf{N}(\mathcal{I}^{(0)})) \oplus \mathrm{Span}_k(\mathbf{N}(\mathcal{I}^{(1)})) \simeq$$

$$\simeq \mathcal{P}/\mathcal{I}^{(0)} \oplus \mathcal{P}/\mathcal{I}^{(1)} \simeq \mathcal{P}/\mathcal{I} \simeq \bigoplus_{\mathbf{a} \in \mathcal{A}} \mathcal{P}/\mathbf{q_a} \xrightarrow{\pi} \bigoplus_{\mathbf{a} \in \mathcal{A}} k[\mathbf{a}]$$

and multiplicities of the roots are preserved.

The complexity of this model, whose interest seems to be in preservation of multiplicities, is therefore $\mathcal{O}(ns^2)$ to store the field, $\mathcal{O}(s)$ to store a single element, $\mathcal{O}(ns^3)$ for arithmetical operations.

Summing up: complexity

Let us now summarize the complexity of representing the roots of an ideal in any of the models above as well as the complexity of representing an arithmetical expression and of performing an arithmetical operation.

We have that the storage for representing all the roots of $\mathcal{I}$ is $\mathcal{O}(nu)$ for all the models except 9.6, which requires $\mathcal{O}(nu^2)$ and 9.7, which requires $\mathcal{O}(ns^2)$; storing an arithmetical expression requires $\mathcal{O}(u)$ for all the models except 9.7, which requires $\mathcal{O}(s)$; performing an arithmetical operation has a time complexity of $\mathcal{O}(u^2)$ for all the models except 9.6, which requires $\mathcal{O}(u^3)$ and 9.7, which requires $\mathcal{O}(s^3)$.

Summing up: "solving" a system

According to the Kronecker - Duval phylosophy about solving systems of equation, which we have discussed above, a group $\mathcal{R}$ of roots of the ideal $\mathcal{I}$ is therefore given by giving

- an artinian ring A
- n elements $\alpha_1, \ldots, \alpha_n \in A$

s.t. if we denote

- $A = \bigoplus_{i=1}^{\tau} A_i$ the decomposition of A into irreducible algebras,
- K_i the residue field of A_i
- $\psi_i : A \longrightarrow K_i$ the canonical projection,
- $\mathbf{a}_i := (\psi_i(\alpha_1), \ldots, \psi_i(\alpha_n)) \in K_i^n$

we have

$$\mathcal{R} = \{\mathbf{a}_i : i = 1 \ldots \tau\}.$$

Also, any algorithm to "solve" the ideal $\mathcal{I}$ is just required to returns a finite set of groups of roots $\mathcal{R}$ representing them as above; eg following §9.6, we could assume that "solving" $\mathcal{I}$ requires just to return a Gröbner basis of $\mathcal{I}$, so that $A = \mathcal{P}/\mathcal{I}$ and α_i is the class of X_i; in this way of course *all* the roots of $\mathcal{I}$ are represented by $(\alpha_1, \ldots, \alpha_n)$.

10 "Distinct power factorization" of multivariate polynomial 0-dim. ideals

When Duval [D] introduced her model for roots of univariate polynmial, she strikng showed that applying her model to compute $\gcd(f(X-\alpha), f'(X-\alpha)) \in k[\alpha]$ for each root α of $f(X) \in k[X]$ produced the distinct power factorization of $f(X)$.

It is quite evident that according to the Kronecker-Duval approach to polynomial system solving, if we are given an ideal $\mathcal{I} = \{f_1, \ldots, f_m\}$, and we

1) "solve" it in the sense above (i.e. we give an arthinian ring A and elements $\alpha_1, \ldots, \alpha_n \in A$ for each grups of roots $\mathcal{R}$
2) consider the ideal $\mathcal{I}_A = \mathcal{I}A[X_1, \ldots, X_n]$ and perform the translation $X_j \to X_j - \alpha_j$, so that the "generic" root $\mathbf{a}_j \in \mathcal{R}$ is moved to the origin and so the primary component of $\mathcal{I}_A$ relative to it is now a primary at the origin.
3) perform the algorithm described in §8

then as a consequence, we obtain

- a split of the given set of roots as $\mathcal{R} = \cup \mathcal{R}^j$, each subset $\mathcal{R}^j$ being represented as above by an artinian ring A^j and "roots" $\alpha_k^j \in A^j$
- closed subsets $V^j \subset \mathrm{Span}_{A^j}(\mathbf{D})$ of differential conditions, so that with the same notation as above for each root $\mathbf{a}_k^j \in \mathcal{R}^j$, the subset $\psi_i^j(V^j) \subset \mathrm{Span}_{K_i^j}(\mathbf{D})$ is such that $\psi_i^j(V^j) = \Delta(\mathcal{I})$, where of course $\psi_i^j : \mathrm{Span}_{A^j}(\mathbf{D}) \longrightarrow \mathrm{Span}_{K_i^j}(\mathbf{D})$ is the obvious extension of $\psi_i^j : A^j \longrightarrow K_i^j$

In other words, the algorithm described in §8 using the Kronecker-Duval approach to represent roots, is nothing more than the generalization to the multivariate case of the Duval algorithm to compute the distinct-power-factorization of a univariate polynomial.

That this approach could be applied in a natural way to ideal factorization is so obvious that deserve at most this little remark [5]

References

[ABRW] M. E. Alonso, E. Becker, M.-F. Roy, T. Wörmann, *Zeroes, multiplicities and idempotents for zerodimensional systems*, Proc. MEGA '94 (eds.: T. Recio and L. Gonzalez-Vega), to appear.

[BK] S. Beck, M. Kreuzer *How to compute the canonical module of a set of points* Proc. MEGA '94 (eds.: T. Recio and L. Gonzalez-Vega), to appear.

[C] J. P. Cardinal *Dualité et algorithmes interactifs pour la résolution de systèmess polynomiaux*, Thèse, Rennes I (1993)

[D] D. Duval, *Diverses questions rélatives au calcul formel avec de nombres algébriques*, Thèse d'État, Grenoble 1987.

[5] whose aim is to allow us to claim in this note that we hope to be able to apply more seriously Gröbner Duality to the factorization problem

[FGLM] J.C. Faugère, P. Gianni, D. Lazard, T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, J.Symb.Comp. 1994.

[FGS] N. Fitchas, M.Giusti, F. Smietanski, *Sur la complexité du théorème des zéros*, to appear in Proc. 2nd International Conference on Non-Linear Optimization and Approximation, La Habana, September 1993 (Cuba), edited by J. Guddat and Brosowski, Peter Lange Verlag, Frankfurt am Main.

[G] A. Galligo, *A propos du Théorème de Préparation de Weierstrass*, L.N. Math **409** (1974), pp. 543–579.

[GM] P.Gianni, T.Mora, *Algebraic solution of systems of polynomial equation using Gröbner bases*, Proc. AAECC 5, LNCS **356** (1989), 247–257.

[Gr] W. Gröbner, *Algebraische Geometrie II*, B.I, Hochschultaschenbücher, vol 737/737a, Bibliogr. Inst. Mannheim (1970).

[L89] D. Lazard, *Solving zero-dimensional algebraic systems*, J. Symb. Comp. **13** , 117 – 131 (1987). (1989).

[L93] D. Lazard, *Systems of algebraic equations (algorithms and complexity)*, in D. Eisenbud, L. Robbiano Eds. *Computational Algebraic Geometry and Commutative Algebra*, D. Eisenbud, L. Robbiano Eds., Cambridge (1993), 106–150.

[MMM1] M.G.Marinari, H.M. Möller, T. Mora, *Gröbner bases of ideals defined by functionals with an application to ideals of projective points*, AAECC **4** (1993), 103–145.

[MMM2] M.G.Marinari, H.M. Möller, T. Mora, *On multiplicity in polynomial system solving* , preprint.

[MS] H.M. Möller, H.J. Stetter, *Multivariate polynomial equations with multiple zeros solved by matrix eigenproblems*, to appear in Numerische Mathematik.

[M] H.M. Möller, *On decomposing systems of polynomial equations with finitely many solutions*, J. Appl. Algebra **4** (1993), 217–230.

[MT] T. Mora, C. Traverso, *Natural representation of algebraic numbers*, in preparation.