TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 348, Number 8, August 1996

ON MULTIPLICITIES IN POLYNOMIAL SYSTEM SOLVING

M. G. MARINARI, H. M. MÖLLER, AND T. MORA

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 and of algorithms which perform transformations between the different representations.

Introduction

When solving a system of polynomial equations (which in this paper will always have a 0-dimensional set of zeroes and will be called "0-*dimensional system*"), it is often satisfactory to know the zeroes of the system, in such a way to be able to perform arithmetical operations on the coordinates of each root.

There is of course a stream of research about methods for solving systems of equations (for a survey we refer to [L93]). There is also a "reflection" about the "meaning" of solving a system, taking place within some research groups more interested in effective methods for algebraic geometry. The philosophy essentially goes back to Kronecker: a system is solved if each root is represented in such a way as to allow the performance of 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 of 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 system and allowing efficient arithmetical operations over their expressions.

In this context 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 suitable approaches to this question based on different models for computing solutions (i.e. without multiplicity).

The "arithmetical" multiplicity of a primary at the origin can be easily computed since it is read from the leading term of the Hilbert polynomial but this doesn't give a sufficient description of the "algebraic" information. In fact it is known that up

Received by the editors December 20, 1994.

1991 *Mathematics Subject Classification.* Primary 14M05, 13P99, 13H15, 14B10.

The first author was partially supported by European Community contract CHRX-CT94-0506.

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 $(X, Y)^2$.

Since, coming from the Hilbert polynomial, the "arithmetical" multiplicity is only an asymptotic information, one could however hope that more accurate invariants could allow to distinguish primary ideal which are locally isomorphic, e.g. the Hilbert function (remark that of course it allows to discriminate the two classes above).

Unfortunately an example by Galligo [G] drops some doubts on this hope: it implies the existince of two primary ideals of the same multiplicity, which are not locally isomorphic and are not distinguishable by the Hilbert function and the Betti numbers.

On the basis of this, in our opinion, in order to describe thoroughly multiplicities of roots, it is preliminary to begin 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.

A way of representing primaries at a root is a classical approach proposed by Gröbner in order to reinterpret Macaulay notion of inverse sistems. 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 $\mathbf{a} \in \bar{k}^n$ is a common root of polynomials $f_1, \dots, f_r \in k[X_1, \dots, X_n]$ (k any field of characteristic 0 and $\bar{k}$ its algebraic closure), then there are finitely many linear combinations D_i of partial derivatives $\frac{\partial^{i_1+\cdots+i_n}}{\partial x_1^{i_1} \cdots \partial x_n^{i_n}}$, such that every polynomial f in the ideal $(f_1, \dots, f_r)$ 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 exacly the primary component at $\mathbf{a}$ of the ideal $(f_1, \dots, f_r)$. 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 of this (whose theory is presented in section 3.3 and detailed in [MMM]), it is natural to describe a primary by a closed subset of differential conditions.

The outstanding Gröbner bases relevance for the effective risolution of algebriac geometry problems implies that a primary ideal can be assumed as represented by a Gröbner basis. Moreover, since the problem we are studying is "local" and standard bases are the usual counterpart of Gröbner bases for local problems, a primary ideal can likely be assumed as represented by a standard basis.

As a consequence, in this paper we study three ways of representing a primary ideal $\mathbf{q} \subset k[X_1, \dots, X_n]$, and so of describing the multiplicity of a root of a system, i.e. via

- the closed subspace of differential conditions corresponding to $\mathbf{q}$,
- a Gröbner basis of $\mathbf{q}$,
- a standard basis of $\mathbf{q}$.

Our major interest is about algorithms for computing a representation of a primary of a root of a system and how to transform any such representation into another one.

This kind of study, of course, poses questions about time and space complexity, both of the algorithms and of our proposals for representing primaries. Some related problems challenged us, for instance:

- while space complexity of representing a Gröbner (or standard) basis of a primary ideal in $k[X_1, \dots, X_n]$ having multiplicity s is $\mathbf{O}(ns^2)$, a naif approach to represent differential conditions has too high space complexity: we had to find a "clever" way of representing them in order to get the same complexity $\mathbf{O}(ns^2)$;

- while most algorithms for passing from a representation to another one have time polynomial complexity in n and s, transforming a representation to standard bases can have complexity $(O \log^n s)$; we found however an obvious approach which reduces complexity to the polynomial case.

Aside from the complexity aspect, the question of computing the set of differential conditions was quite stimulating for us. Trying to represent them with good complexity, we were able to produce algorithms which given any basis of a primary ideal, compute differential conditions; these algorithms are mainly based on the problem of determining, given a primary at a root, all the primaries containing it and having multiplicity 1 higher than it.

After recalling the notations (§1), we start discussing (§2) the current approaches in representing the roots of a system, following the Kronecker's philosophy: of course we resume Kronecker's approach we also present the important model by Duval ([D]), whose major advantage on Kronecker's is to avoid factorization of polynomials; and produce some more recent approaches to the problem.

Subsequently (§3) we discuss our proposals for representing multiple roots; in particular we discuss a low complexity technique for representing a set of differential conditions and we also discuss how to use this representation for testing if a polynomial is in the ideal (while naively applying the given differential conditions to the polynomial has too bad complexity, we are able to present an algorithm with $\mathbf{O}(ns^2)$ complexity, i.e. exactly the same complexity for testing the same problem using Gröbner bases.

Later (§4) we discuss how to convert a representation into another one: among the results there, we point out algorithms for producing a set of differential conditions given a basis of a primary ideal: they are based on how to determine, given a primary ideal, all primaries containing it and with multiplicity one higher .

Finally (§5) we solve the problem of computing the "algebraic" multiplicity of a root of a system; we assume to be given a 0-dimensional ideal and the set of its (distinct) roots (e.g. by giving its radical) and we discuss how to compute a representation of its primary component at each root.

1. Preliminaries

1.1 Systems and zeroes.

Let k be an effective field of characteristic zero, let $\mathcal{P} := k[X_1, \dots, X_n]$ and let $\mathcal{I}$ be a zero-dimensional ideal.

Since we will often need to extend the base field k to a finite algebraic extension K, or to its algebraic closure $\mathbf{k}$, or to an artinian k-algebra A, we will denote by $\mathcal{P}_K, \mathcal{P}_\mathbf{k}, \mathcal{P}_A$ the polynomial rings $K[X_1, \dots, X_n]$, $\mathbf{k}[X_1, \dots, X_n]$, $A[X_1, \dots, X_n]$ resp., and for an ideal $\mathcal{J} \subset P$ we will correspondingly denote by $\mathcal{J}_K$, $\mathcal{J}_\mathbf{k}$, $\mathcal{J}_A$ the extended ideals $\mathcal{J}\mathcal{P}_K$, $\mathcal{J}\mathcal{P}_\mathbf{k}$, $\mathcal{J}\mathcal{P}_A$.

The 0-dimensional ideal $\mathcal{I}$ has a primary decomposition $\mathcal{I} = \mathbf{q}_1 \cap \dots \cap \mathbf{q}_t$, 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.

If $\mathbf{m}_i$ is linear, $\mathbf{m}_i = (X_1 - a_1, \dots, X_n - a_n)$, $a_i \in k$, then it defines a *rational* root of $\mathcal{I}$, $\mathbf{a} = (a_1, \dots, a_n)$; we will then freely use the notation $\mathbf{m_a}, \mathbf{q_a}$ to denote $\mathbf{m}_i$ and the corresponding primary $\mathbf{q}_i$.

If $\mathbf{m} := \mathbf{m}_i$ is not linear, and $K := \mathcal{P}/\mathbf{m}$, then $\mathbf{m}_K$ has a decomposition into maximal ideals in P_K, $\mathbf{m}_K = \mathbf{n}_1 \cap \dots \cap \mathbf{n}_r$, 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 $\mathcal{I}$, $\mathbf{q}_K$ has a primary decomposition, $\mathbf{q}_K = \mathbf{p}_1 \cap \dots \cap \mathbf{p}_r$, 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 $\operatorname{mult}(\mathbf{q}) := \dim_k(\mathcal{P}/\mathbf{q})$. If $\mathbf{q}$ is an $\mathbf{m}$-primary component of a 0-dimensional ideal $\mathcal{I}$, where the roots of $\mathbf{m}$ are $\mathbf{a}_1, \dots, \mathbf{a}_r \in K^n$, corresponding to primaries $\mathbf{p}_i \in \mathcal{P}_K$, the multiplicity in $\mathcal{I}$ of $\mathbf{a}_i$ is $\operatorname{mult}(\mathbf{a}_i, \mathcal{I}) := \operatorname{mult}(\mathbf{p}_i) = \dim_K(\mathcal{P}_K/\mathbf{p}_i) = \dim_k(\mathcal{P}/\mathbf{q})/\dim_k(K)$.

1.2 Some general notation.

We adopt here freely the notation of [MMM]. We therefore denote by $\mathbf{T}$ the semigroup generated by $\{X_1, \dots, X_n\}$. If $<$ is a semigroup ordering on $\mathbf{T}$, i.e. an ordering s.t.

$$t_1 < t_2 \Rightarrow tt_1 < tt_2\ \forall t, t_1, t_2 \in \mathbf{T},$$

then $T(f)$ denotes the maximal term of a polynomial f w.r.t. $<$, $lc(f)$ its leading coefficient, i.e. the coefficient of $T(f)$, $T(\mathcal{J}) := \{T(f) := f \in \mathcal{J}\}$ the ideal of maximal terms of the ideal $\mathcal{J}$, $\mathbf{N}(\mathcal{J}) := \mathbf{T} \setminus \mathbf{T}(\mathcal{J})$, $\mathbf{B}(\mathcal{J}) := \{X_i\tau : i = 1 \dots n, \tau \in \mathbf{N}(\mathcal{J})\}$, $\operatorname{Can}(f, \mathcal{J}) \in \operatorname{Span}_k(\mathbf{N}(\mathcal{J}))$ the canonical form of f w.r.t. $\mathcal{J}$ (and the ordering $<$).

The notation $\mathbf{N}(\mathbf{d}) := \mathbf{N}(X_1^{d_1}, \cdots, X_n^{d_n})$ will be used to denote the set of terms $\{X_1^{e_1} \cdots X_n^{e_n} : e_i < d_i\ \forall i\}$. By abuse of notation if $t = X_1^{d_1} \dots X_n^{d_n}$ instead of $\mathbf{N}(\mathbf{d})$ we will also write $\mathbf{N}(t)$. By $\overline{\mathbf{N}(\mathbf{d})}$ we mean the "closure " of $\mathbf{N}(\mathbf{d})$, $\{X_1^{e_1} \cdots X_n^{e_n} : e_i \le d_i\ \forall i\}$. Using this notation, we can write $\mathbf{N}(\mathcal{J}) = \bigcup_{g \in G} \mathbf{N}(T(g))$ if G is a Gröbner basis of the ideal $\mathcal{J}$ (This can also be considered as a definition of a Gröbner basis G for an ideal $\mathcal{J}$ if G is a finite subset of $\mathcal{J} \setminus \{0\}$.) If a polynomial f is represented sparsely as $f = \sum_{i=1}^{\mu} c_i\tau_i$, $c_i \neq 0\ \forall i$, $\tau_j \neq \tau_j$ for $i \neq j$, then we will denote $\sum(f)$ the set $\bigcup_i \overline{\mathbf{N}(\tau_i)}$, and call it (see [MT]) *staircase generated by* f.

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

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

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

We moreover denote $\mathcal{D} := \{D(t) : t \in \mathbf{T}\}$ and $\operatorname{Span}_K(\mathcal{D})$ the K-vector space generated by $\mathcal{D}$, where K is a finite extension of k; the order of an element $\delta = \sum c_i D(t_i) \in \operatorname{Span}_K(\mathcal{D})$, with $c_i \neq 0\ \forall i$, is $\max(ord(D(t_i)))$.

Applying $D(X_j)$ to a term $X_1^{e_1} \dots X_n^{e_n}$, one has:

$$D(X_j)(X_1^{e_1} \cdots X_n^{e_n}) = \begin{cases} e_j X_1^{e_1} \cdots X_j^{e_j - 1} \cdots X_n^{e_n} & \text{if } e_j > 0, \\ 0 & \text{otherwise.} \end{cases}$$

and therefore for $t = X_1^{d_1} \cdots X_n^{d_n}, \tau = X_1^{e_1} \cdots X_n^{e_n}$:

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

where $\binom{\tau}{t} := \binom{e_1}{d_1} \cdots \binom{e_n}{d_n}$. Therefore if $f = \sum_{\tau \in \mathbf{T}} c_\tau \tau \in \mathcal{P}_K$ and $L = \sum_{\tau \in \mathbf{T}} b_\tau D(\tau) \in \mathrm{Span}_K(\mathcal{D})$, 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

$$\begin{aligned} f(X_1 + a_1, \dots, X_n + a_n) &= \sum_{\tau \in \mathbf{T}} D(\tau)(f)(a_1, \dots, a_n)\tau \\ &= \sum_{\tau \in \mathbf{T}} \tau \sum_{\substack{i=1 \\ \tau | t_i}}^{\mu} c_i \binom{t_i}{\tau} \frac{t_i}{\tau}(a_1, \dots, a_n). \end{aligned}$$

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

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

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 $j = 1, \dots, n$, the linear map $\rho_{X_j} : \mathrm{Span}_K(\mathcal{D}) \to \mathrm{Span}_K(\mathcal{D})$ s.t.:

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

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 $\sigma_j := \sigma_{X_j}$, $\rho_j := \rho_{X_j}$. The following relations hold:

$$\sigma_j \rho_j = \mathrm{Id}\, \forall j,$$

$$\lambda_j(D(i_1, \dots, i_n)) := \rho_j \sigma_j(D(i_1, \dots, i_n)) = \begin{cases} D(i_1, \dots, i_j, \dots, i_n) & \text{if } i_j > 0, \\ 0 & \text{otherwise,} \end{cases}$$

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

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

$$L_1 < L_2 \Rightarrow \rho_i(L_1) < \rho_i(L_2)\ \forall i, \forall L_1, L_2 \in \mathcal{D}.$$

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

A basis $\Gamma = (L_1, \dots, L_r)$ of a vector space $V \subset \mathrm{Span}_K(\mathcal{D})$ 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 $c_{i\kappa} \neq 0,\ D_{i\kappa} \neq T(L_j)\ \forall i, j, \kappa$.

Having any basis of V, such a Gauss basis can obviously be obtained by complete Gaussian elimination.

For a finite-dimensional vector space V generated by $\{v_1, \dots , v_m\}$, we will use the notation $V = \langle v_1, \dots , v_m\rangle$.

Let $\mathcal{I} \subset \mathcal{P}$ be a zero-dimensional ideal, given through a basis $\{f_1, \dots , f_m\}$. Let $\mathbf{q}$ be a primary in the decomposition of $\mathcal{I}_K$, corresponding to a zero which is rational over the finite algebraic extension $K \supset k$. 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
- Σ the sum of the cardinalities of $\Sigma(f_i)$ for f_i in the input basis.

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

Further appropriate "local" notation will be introduced in each single section.

2. Representation of roots

In this section, we will recall briefly different ways to represent the roots of a zero-dimensional ideal, and indicate how to perform arithmetical operations over arithmetical expressions of its roots.

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

- 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 $k[a_1, \dots , a_n]$, it is rather a set of instructions in prescribed order which, applied to $(a_1, \dots , a_n)$ produce such an algebraic number, and these instructions could include "branching" ones, like

if $\mathit{expr}_1 = 0$ **then** $\mathit{expr}_2 := \mathit{expr}_3$ **else** $\mathit{expr}_2 = (\mathit{expr}_1)^{-1}$.

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 2.1. 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 a further polynomial division (an obvious one, but computers are not smart) 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 $\mathbf{a} = (a_1, \dots, a_n) \in \mathbf{k}^n$ of $\mathcal{I}$. We will denote

- $K = k(a_1, \dots, a_n)$ the minimal algebraic extension of k containing $\mathbf{a}$,
- $\mathbf{n} = (X_1 - a_1, \dots, X_n - a_n) \subset \mathcal{P}_K$ 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

$t := t_{\mathbf{a}} := \dim_k(K) = \operatorname{mult}(\mathbf{m})$, the number of roots which are k-conjugate to $\mathbf{a}$,
$v := v_{\mathbf{a}} := \operatorname{mult}(\mathbf{p})$,
$r := r_{\mathbf{a}} := tv = \operatorname{mult}(\mathbf{q})$,

and since we are interested in the cost of a same computation over all roots of $\mathcal{I}$, we set

$u := \operatorname{mult}(\sqrt{\mathcal{I}})$, 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.

2.1 Representation by a tower of algebraic extensions.

The classical way to represent $\mathbf{a}$ is by representing K as a tower of simple algebraic extensions. Let $K_i := k(a_1, \dots, a_i)$, with $K_0 = k$ and $K = K_n$, $d_i := \dim_{K_{i-1}}(K_i)$. Let $\phi_i : k[X_1, \dots, X_n] \longrightarrow K_i[X_{i+1}, \dots, X_n]$ be defined by $\phi_i(X_j) := a_j$ if $i \leq j$ otherwise $\phi_i(X_j) := X_j$. Then, for each i, there is a unique monic polynomial $f_i \in K(X_1, \dots, X_{i-1})[X_i]$ 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 $j < i$, $\deg_{X_i}(f_i) = d_i$,
- $\mathbf{m} = (f_1, \dots, f_n)$ (this last assertion is known as "Nulldimensionaler Primbasissatz").

As a k-vector space, K can then be identified with the subspace of $\mathcal{P}$ whose basis is the set of terms $\mathbf{N}(\mathbf{d})$, $\mathbf{d} = (d_1, \dots, d_n)$, so in order 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 $\operatorname{Span}_{K_{i-1}}(1, \dots, X_i^{d_i - 1})$ 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 $\mathbf{b} = (b_1, \dots, b_n)$ is a k-conjugate root of $\mathbf{a}$, i.e. another root of $\mathbf{m}$, then $k(b_1, \dots, b_i) \simeq K_i, \forall i$; therefore in this model one needs to represent only one root for each conjugacy class for a total space requirement of $\sum_{\mathbf{a}\in\mathcal{A}} \mathcal{O}(nt_{\mathbf{a}}) = \mathcal{O}(nu)$ 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.

2.2. Representation by a simple algebraic extension.

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

$$L_{\mathbf{c}}(X_1) = X_1 + \sum_{i=2}^{n} c_i X_i,$$
$$L_{\mathbf{c}}(X_i) = X_i \quad \forall i > 1.$$

If $(a_1, \dots, a_n)$ is a root of $\mathcal{I}$ the corresponding root of $L_{\mathbf{c}}(\mathcal{I})$ is then

$$(a_1 - \sum_{i=2}^{n} c_i a_i, a_2, \dots, a_n).$$

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.

- $\forall \mathbf{c} \in U$, $K = k[a^{(\mathbf{c})}]$,
- $\forall \mathbf{c} \in U$, two different roots of $L_{\mathbf{c}}(\mathcal{I})$ have different first coordinates.

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

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

As in the previous section the field K can be identified with the vector space $\mathrm{Span}_k(1, X_1, \dots, X_1^{t-1})$; storage requirements are therefore still $\mathcal{O}(nt)$ for the field, and t for an arithmetic expression. Moreover the cost of arithmetics is $\mathcal{O}(t^2)$ ($\mathcal{O}(nu)$, 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 $L_{\mathbf{c}}(\mathcal{I})$ requires now only polynomial factorization over k.

2.3 Representation by a squarefree triangular set.

In order to avoid the requirement for costly polynomial factorization, "weak" models for the arithmetics of algebraic numbers have been introduced recently. The most widespread is the "dynamic-evaluation" or "Duval" model [D].

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 uniquely) 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 longer evident.

Example 2.2. Let us go back to the preceding example, where we were computing $\gcd(g_a, g'_a)$ for $g_a(Z) = Z^3 + 3aZ^2 + 12Z + 4a$, with a *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 on 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 an expression $h(a)$ is zero if and only if a is a root of $f^{(0)} = \gcd(f, h)$ while $h(a)$ is not zero 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 2.2 (cont'd). In the above example one gets

$$f^{(0)} = \gcd(X^4 - 13X^2 + 36, 8 - 2X^2) = X^2 - 4, \quad f^{(1)} = f/f^{(0)} = X^2 - 9,$$

finding a partial factorization of f without 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

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

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 $\mathbf{a} = (a_1, \dots, a_n)$ is given if monic polynomials $f_i \in k(X_1, \dots, X_{i-1})[X_i]$ are given s.t.

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

This allows us to represent elements of $k[a_1, \dots, a_n]$ by elements of $\mathrm{Span}_k(\mathbf{N}(\mathbf{d}))$, $\mathbf{d} = (d_1, \dots, d_n)$ and to perform there ring operations. However anytime a zero-testing or an inversion is needed, this is performed by gcd computations over $k(a_1, \dots, a_{n-1})[X_n]$ 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 $k(a_1, \dots, a_{n-1})$, which is recursively performed in the representation $k[X_1, \dots, X_{n-1}]/(f_1, \dots, f_{n-1})$ and therefore could itself, recursively, produce splitting at lower levels.

An ordered set of polynomials $(f_1, \dots, f_n)$ satisfying the conditions above is known as a *triangular set*. Given a (Gröbner) basis of a zero dimensional ideal, by only gcd computations, it is possible (see [L] for the algorithms) 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. (Alternatively, one could use the decomposition into triangular sets by ideal quotienting, [hmm].) 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 needs $\mathcal{O}(u^2)$ arithmetical operations in k.

2.4 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 so), then there is a Zariski open set $U \subset k^{n-1}$ s.t. $\forall \mathbf{c} \in U$, $\text{Ł}_c(\mathcal{I}) = (g_1(X_1), X_2 - g_2(X_1), \dots, X_n - g_n(X_1))$ 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 $k[X_1]/(g_1)$. 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.

2.5 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.

2.6 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 by 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

$$\mathrm{card}(\mathbf{N}(\sqrt{\mathcal{I}})) = \mathrm{mult}(\sqrt{\mathcal{I}}) = u \text{ elements in } k.$$

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 $\mathrm{Span}_k(\mathbf{N}(\sqrt{\mathcal{I}}))$ 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 $\{\tau - Can(\tau, \sqrt{\mathcal{I}}) : \tau \in \mathbf{B}(\sqrt{\mathcal{I}})\}$), 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 present the same difficulty as in Duval's model, and are 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 $\mathcal{I}^{(0)} := \sqrt{\mathcal{I}} + (h)$,
- $h(\mathbf{a}) \neq 0$ if and only if $\mathbf{a}$ is a root of $\mathcal{I}^{(1)} := \sqrt{\mathcal{I}} : h = \{f \in \mathcal{P} : hf \in \sqrt{\mathcal{I}}\}$,
- $\mathcal{P}/\sqrt{\mathcal{I}} \simeq \mathcal{P}/\mathcal{I}^{(0)} \oplus \mathcal{P}/\mathcal{I}^{(1)}$.

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

The flexibility of this presentation (any Gröbner basis can be used instead of 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.

2.7 Representation by a border basis.

With the "natural" representation, one is not restricted to work with radical ideals. In fact $s = \operatorname{mult}(\mathcal{I}) \geq \operatorname{mult}(\mathbf{q_a}) \forall \mathbf{a} \in \mathcal{A}$; one has

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

with a projection π.

For a polynomial $h(X_1, \dots, X_n) \in \operatorname{Span}_k(\mathbf{N}(\mathcal{I}))$, the following hold:

- $h(\mathbf{a}) = 0$ if and only if $h \in \mathbf{p_a} = \sqrt{\mathbf{q_a}}$ iff $h^s \in \mathbf{p}_{\mathbf{a}}^s \subset \mathbf{q_a}$
- $h(\mathbf{a}) = 0$ if and only if $\mathbf{q_a} : h^s = \mathcal{P}$
- $h(\mathbf{a}) \neq 0$ if and only if $\mathbf{q_a} : h^s = \mathbf{q_a}$.

Denoting:

$$\mathcal{I}^{(0)} := \mathcal{I} + (h^s),$$

$$\mathcal{I}^{(1)} := \mathcal{I} : h^s = \{f \in \mathcal{P} : h^s f \in \mathcal{I}\}.$$

One has that:

- $h(\mathbf{a}) = 0$ if and only if $\mathbf{a}$ is a root of $\mathcal{I}^{(0)}$
- $h(\mathbf{a}) \neq 0$ if and only if $\mathbf{a}$ is a root of $\mathcal{I}^{(1)}$
- $\mathcal{I} = \mathcal{I}^{(0)} \cap \mathcal{I}^{(1)}$ so that

$$\begin{aligned}\operatorname{Span}_k(\mathbf{N}(\mathcal{I}^{(0)})) \oplus \operatorname{Span}_k(\mathbf{N}(\mathcal{I}^{(1)})) &\simeq \mathcal{P}/\mathcal{I}^{(0)} \oplus \mathcal{P}/\mathcal{I}^{(1)} \\ &\simeq \mathcal{P}/\mathcal{I} \simeq \bigoplus_{\mathbf{a}\in\mathcal{A}} \mathcal{P}/\mathbf{q_a} \xrightarrow{\pi} \bigoplus_{\mathbf{a}\in\mathcal{A}} k[\mathbf{a}]\end{aligned}$$

  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.

3. Representation of multiple points

In this section we will consider a linear maximal ideal $\mathbf{m} = (X_1 - a_1, \dots, X_n - a_n) \subset \mathcal{P}_K$, where $K \supset k$ is a finite algebraic extension and an $\mathbf{m}$-primary ideal $\mathbf{q}$; up to a translation $(X_i \mapsto X_i + a_i)$ we can assume $a_i = 0, \forall i$, 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. We recall that $s = \operatorname{mult}(\mathcal{I})$, $r = \operatorname{mult}(\mathbf{q})$, $t = \dim_k(K)$.

For the following complexity discussion we will need 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 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 the space complexity is still bounded by s and the time complexity is $\mathcal{O}(t^2 s^2)$.

3.1 Representation by a Gröbner basis.

The primary ideal $\mathbf{q}$ is of course completely characterized by its reduced Gröbner basis with respect to any ordering $<$.

The set $\mathbf{N}(\mathbf{q})$ is a K-basis of $P_K/\mathbf{q}$ and has therefore cardinality r; the reduced Gröbner basis of $\mathbf{q}$ has cardinality bounded by $nr + 1 - r$. Therefore storing the reduced Gröbner basis of $\mathbf{q}$ requires storing at most $\mathcal{O}(nr^2)$ elements of K and so at most $\mathcal{O}(ntr^2)$ elements of k.

One could wish to represent $\mathbf{q}$ by its border basis instead of by a Gröbner basis, see [MMM] . Since the cardinality of the border basis has the same bound as that of a Gröbner basis, the theoretical storage requirements are not changing (while in practice, of course, a border basis is quite larger than a Gröbner one).

A Gröbner (or border) basis representation is particularly suitable to test if a given polynomial $f \in \mathcal{P}$ vanishes at the zero of $\mathbf{q}$ with the proper multiplicity. This can be done by testing whether $\mathrm{Can}(f, \mathbf{q}) = 0$; for these tests, we refer to [MMM, appendix].

An alternative to Gröbner and border bases are involutive bases. These bases have been recently studied, [ZH]. Experiences show some advantages over Gröbner and border bases in producing polynomials with shorter coefficient vectors and/or lesser terms. Discussions about complexity, especially including coefficient length, have not yet been published.

3.2 Representation by a standard basis.

Standard bases can be defined for polynomial ideals as well as for ideals in other rings like the ring of formal power series. These bases are more or less like Gröbner bases with the main difference, that here the semigroup ordering is not a well-ordering, and that for polynomial ideals $\mathcal{I}$ a standard basis is not necessarily an ideal basis of $\mathcal{I}$.

More formally, here are a definition and some basic properties of standard bases.

One considers a semigroup ordering $<$ on $\mathbf{T}$, s.t. $X_i < 1 \; \forall i$, and defines $T(f), T(\mathcal{I}), \mathbf{N}(\mathcal{I})$ as usual.

For an ideal $\mathcal{I} \subset \mathcal{P}$ a standard basis is a set $F \subset \mathcal{I}$ s.t. $T(\mathcal{I})$ is generated by $\{T(f) : f \in F\}$.

Let $\hat{\mathcal{P}} := k[[X_1, \dots , X_n]]$, let $\mathcal{P}_0 = \{\frac{f}{1+g} : f, g \in \mathcal{P}, g(0) = 0\}$ and let $\mathrm{cl}(\mathcal{I})$ be the intersection of all primary components of $\mathcal{I}$ through the origin.

Theorem 3.1. *The following hold:*

1) *If $G = \{g_1, \dots , g_\rho\}$ is a standard basis of $\mathcal{I}$, then it is a basis of $\mathcal{I}\hat{\mathcal{P}} = \mathrm{cl}(\mathcal{I})\hat{\mathcal{P}}$ and of $\mathcal{I}\mathcal{P}_0 = \mathrm{cl}(\mathcal{I})\mathcal{P}_0$ and a standard basis of $\mathrm{cl}(\mathcal{I})$.*
2) *For each $f \in \hat{\mathcal{P}}$, there is a unique $\mathrm{Can}(f, \mathcal{I}) \in \hat{\mathcal{P}}$ s.t.*
   - *the coefficient of each $\tau \in T(\mathcal{I})$ in $\mathrm{Can}(f, \mathcal{I})$ is 0,*
   - *$f - \mathrm{Can}(f, \mathcal{I}) = \sum_i h_i g_i$ with $h_i \in \hat{\mathcal{P}}$ and $T(h_i g_i) \le T(f) \forall i$.*
3) *For each $f \in \mathcal{P}$, $f \in \mathrm{cl}(\mathcal{I})$ if and only if $f = \sum_i h_i g_i$ with $h_i \in \mathcal{P}_0$ and $T(h_i g_i) \le T(f) \; \forall i$.*

For a 0-dimensional ideal $\mathcal{I}$ the situation is more interesting: $\mathrm{cl}(\mathcal{I})$ is the primary component of $\mathcal{I}$ at the origin and as such it contains a power $\mathbf{m}^d$ of the maximal ideal $\mathbf{m}$, which implies that $\mathbf{N}(\mathcal{I})$ is finite, since all terms of degree at least d are in $\mathrm{cl}(\mathcal{I})$ and so in $T(\mathcal{I})$. Therefore $\forall f, \mathrm{Can}(f, \mathcal{I})$ is a polynomial. Moreover one can choose d to be the least integer s.t. $\mathbf{m}^d \subset T(\mathcal{I})$, or, equivalently $d = \max_{\tau \in \mathbf{N}(\mathcal{I})}(\deg(\tau)) + 1$.

Proposition 3.1. *Let $\{\tau_1, \dots, \tau_\rho\}$ be the (unique) minimal set of generators of $T(\mathcal{I})$ and let $G := \{\tau_i - \mathrm{Can}(\tau_i, \mathcal{I}) : i = 1 \dots \rho\}$. Then:*

1) *$\forall h \in \mathcal{P}$, $h - \mathrm{Can}(h, \mathcal{I})$ is in $\mathrm{cl}(\mathcal{I})$.*
2) *$G \cup \{\tau : \deg(\tau) = d\}$ is a basis of $\mathrm{cl}(\mathcal{I})$.*

Proof. Let $h \in \mathcal{P}$, $f := h - \mathrm{Can}(h, \mathcal{I})$; one has $f \in \mathrm{cl}(\mathcal{I})\hat{\mathcal{P}} \cap \mathcal{P} = \mathrm{cl}(\mathcal{I})\mathcal{P}_0 \cap \mathcal{P}$. Therefore there is g, $g(0) = 0$, s.t. $(1 - g)f \in \mathrm{cl}(\mathcal{I})$; this implies $(1 - g^d)f \in \mathrm{cl}(\mathcal{I})$, and, since $g^d \in \mathbf{m}^d \subset \mathrm{cl}(\mathcal{I})$, one concludes $f \in \mathrm{cl}(\mathcal{I})$.

Denoting $g_i := \tau_i - \mathrm{Can}(\tau_i, \mathcal{I})$, one has therefore $g_i \in \mathrm{cl}(\mathcal{I})$. So the ideal generated by $G \cup \{\tau : \deg(\tau) = d\}$ is contained in $\mathrm{cl}(\mathcal{I})$. Conversely, if $h \in \mathrm{cl}(\mathcal{I})$, one has $h = \sum_i h_i g_i$ for some $h_i \in \hat{\mathcal{P}}$. Writing $h_i = h_i^{(1)} + h_i^{(2)}$, where $h_i^{(1)} \in \mathcal{P}$, $\deg(h_i^{(1)}) < d$ and $h_i^{(2)} \in \mathbf{m}^d\hat{\mathcal{P}}$, one has $h - \sum_i h_i^{(1)} g_i \in \mathbf{m}^d\hat{\mathcal{P}} \cap \mathcal{P} = \mathbf{m}^d$. So h is in the ideal generated by $G \cup \{\tau : \deg(\tau) = d\}$. □

Example 3.1. Remark that in general G is not a basis of $\mathrm{cl}(\mathcal{I})$, as shown by the following example, for which we are indebted to G. Pfister.

Let $\mathcal{P} = \mathbb{Q}[X, Y]$, $\mathcal{I} = (X^4 - X^3Y^2, Y^4 - X^2Y^3)$, $\mathbf{q}_1 = (X^5, X^4 - X^3Y^2, Y^4 - X^2Y^3)$, $\mathbf{q}_2 = (X - 1, Y - 1)$, $\mathbf{q}_3 = (Y + X + 1, X^2 + X + 1)$. Then $\mathcal{I} = \mathbf{q}_1 \cap \mathbf{q}_2 \cap \mathbf{q}_3$, $\mathbf{q}_1$ is primary at the origin, $\mathbf{q}_2$ is the maximal at $(1, 1)$, $\mathbf{q}_3$ is the maximal at the pair of conjugate points (ω, ω^2), (ω^2, ω), where ω is the primitive 3^{rd} root of unity. Hence $\mathbf{q}_1 = \mathrm{cl}(\mathcal{I})$.

$G = \{X^4 - X^3Y^2, Y^4 - X^2Y^3\}$ is the reduced standard basis of $\mathbf{q}_1$ and a basis of $\mathcal{I}$. Remark that $X^5 \in \mathbf{q}_1$ and $X^5 = \frac{X+Y^2}{1-Y^3}(X^4 - X^3Y^2) + \frac{X^3}{1-Y^3}(Y^4 - X^2Y^3)$ is a representation of it in terms of G as element of $\mathcal{I}\hat{\mathcal{P}} = \mathbf{q}_1\hat{\mathcal{P}}$, but it doesn't have any representation in terms of G with polynomial coefficients.

Standard bases can be used in the same way as Gröbner bases to test whether a polynomial f vanishes at the point with proper multiplicity. This happens if and only if $Can(f, \mathbf{q}) = 0$. Remark that $f \in \mathbf{q}$ if and only if $f_d \in \mathbf{q}$ where f_d is the truncation of f at degree $d - 1$ and d is the least value s.t. $\mathbf{m}^d \subset \mathbf{q}$. However, this algorithm is most effective if $\mathbf{m} = (X_1, \dots, X_n)$ or (in case $\mathbf{m} = \mathbf{m_a}$) if f is given as a polynomial in $X_1 - a_1, \dots, X_n - a_n$. Then by the algorithm in [MMM], $Can(f, \mathbf{q})$ can be computed in $\mathcal{O}(\mu_d \delta r^2)$ where μ_d is the number of terms in f_d, and $\delta = \min(d - 1, deg(f))$.

The main interest of standard bases is however when one considers elements of $\mathcal{P}_K/\mathbf{q}$, i.e. “functions from the multiple point to K”. Then one is interested in knowing the “infinitesimal order” of $\phi \in \mathcal{P}_K/\mathbf{q}$. This is the proper generalization of the usual notion of infinitesimal order related to Taylor expansions and it is defined to be the maximum of $\mathrm{ord}(g)$ where $g \in \mathcal{P}_K$ runs among the elements in the residue class ϕ and $\mathrm{ord}(g)$ is its usual infinitesimal order i.e. the degree of the minimal non-vanishing homogeneous form in its development. It can be proved that the order of ϕ is $\mathrm{ord}(\mathrm{Can}(f, \mathbf{q}))$, where f is any element in the residue class ϕ, see [M].

3.3 Representation by differential conditions.

Characterization of primaries.

In this section we recall some results from [MMM].

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

- If $\Gamma = (L_1, \dots, L_r)$ is a *Gauss basis* of a closed vector space $V \subset \mathrm{Span}_K(\mathcal{D})$, then it turns out from the definitions (see also subsect.1.2), that $L_1 = Id$ and each $\langle L_1, \dots, L_j \rangle$ is closed $\forall j \in \{1, \dots, r\}$.
- $\Im(V) := \{f \in \mathcal{P}_K : L(f)(\mathbf{0}) = 0 \ \forall L \in V\}$
- If $\mathcal{I} \subset \mathbf{m}$ (as usual $\mathbf{m}$ is the maximal ideal with root in 0) define

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

  it turns out that this is a non-zero vector subspace of $\mathrm{Span}_K(\mathcal{D})$ satisfying the condition $\sigma_t(L) \in \Delta(\mathcal{I}) \forall t \in \mathbf{T}, \forall L \in \Delta(\mathcal{I})$, but one is not guaranteed about its finite dimensionality, however:

Theorem 3.2. *There is a biunivocal correspondence between* $\mathbf{m}$*-primary ideals of* P_K *and closed subspaces of* $\mathrm{Span}_K(\mathcal{D})$.

More exactly, every $\mathbf{m}$*-primary ideal* $\mathbf{q}$ *corresponds to the closed subspace* $\Delta(\mathbf{q})$*, and every closed subspace* $V \subset \mathrm{Span}_K(\mathcal{D})$ *corresponds to the* $\mathbf{m}$*-primary ideal* $\Im(V)$*, so that* $\mathbf{q} = \Im(\Delta(\mathbf{q}))$ *and* $V = \Delta(\Im(V))$.

Moreover $\dim_K(\Delta(\mathbf{q})) = \mathrm{mult}(\mathbf{q})$, $\mathrm{mult}(\Im(V)) = \dim_K(V)$ *and, more in general, for a* 0*-dimensional ideal* $\mathcal{I}$*, whose* $\mathbf{m}$*-primary component is* $\mathbf{q}$*, one has* $\Delta(\mathcal{I}) = \Delta(\mathbf{q})$*,* $\mathbf{q} = \Im(\Delta(\mathcal{I}))$.

This provides an alternative representation of an $\mathbf{m}$-primary ideal $\mathbf{q}$, by giving a basis of the closed subspace $\Delta(\mathbf{q})$.

This representation is suitable for stating multivariate interpolation problems, when either one requires a polynomial to vanish at given points with assigned multiplicities, or one requires the polynomial and some combinations of partial derivatives of the polynomial to assume given values at the point. For finding an interpolating polynomial, however one moves to a border basis of the corresponding ideal, computing at the same time a "biorthogonal set" (for details *cf.* [MMM]).

One can of course use this representation for testing whether a polynomial f is in $\mathbf{q}$ by testing whether $L(f) \in \mathbf{m}$ for each L in a basis of $\Delta(\mathbf{q})$.

There is however a major problem with this representation: it can be space-exponential in $\mathrm{mult}(\mathbf{q})$.

Example 3.2. Consider the ideal $\mathbf{q} := (X_1^r, X_2 - X_1, \dots, X_n - X_1)$. Then $\Delta(\mathbf{q})$ is generated by $\{L_0 \dots L_{r-1}\}$, where $L_0 = D(1) = \mathrm{Id}$, $L_1 = D(X_1) + \dots + D(X_n)$, 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 $\mathbf{q} = (Y_1^r, Y_2, \dots, Y_n)$ and $\Delta(\mathbf{q})$ is now generated by $\{D(Y_1^i) : i = 0 \dots r-1\}$. Notice, however that it doesn't apply to the next one

Example 3.3. Consider now the ideal $\mathcal{I}$ of the rational normal curve with parameteric equations $X_1 = t, X_2 = t^2, \dots, X_n = t^n$ 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 $\{L_0, \dots, L_{r-1}\}$, requiring the storage of $\mathcal{O}((r/n)^n)$ elements of K and that this basis is the less space-consuming.

An alternative representation of closed subspaces.

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

We start by discussing projections via dual bases. So let $\{X_{i_1},\dots,X_{i_d}\}$ be a subset of variables of $\{X_1,\dots,X_n\}$ and let $\mathcal{P}' := k[X_{i_1},\dots,X_{i_d}]$, $\mathbf{T}'$ the semigroup of terms of $\mathcal{P}'$, $\mathcal{D}' := \{D(t) : t \in \mathbf{T}'\}$ and let $\pi : \mathrm{Span}_K(\mathcal{D}) \to \mathrm{Span}_K(\mathcal{D}')$ be the canonical projection.

Proposition 3.2. *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 $L \in \mathrm{Span}_K(\mathcal{D})$, 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 $L' \in \pi(V)$. For each $L \in V$ we know $L(f') = \pi(L)(f')$ and $\pi(L)(f') = 0$ as $\pi(L) \in \pi(V)$, 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 get $\pi(V) = \Delta\Im(\pi(V)) \supset \Delta(\mathbf{q}')$. □

Each element $L \in \mathrm{Span}_K(\mathcal{D} \setminus \{Id\})$ can be uniquely written as $L = L_1 + \cdots L_n$ where $L_j \in Span_K(\mathcal{D}_j)$, and $\mathcal{D}_j := \{D(0,\dots,0,i_j,\dots,i_n) : i_j \neq 0\}$. 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 by the definitions given in 1.2, we immediately get the following.

Lemma 3.1. *Let $L = L_1 + \cdots L_n \in \mathrm{Span}_K(\mathcal{D} \setminus \{Id\})$. The following hold:*

(1) $$\lambda_i(L) = \lambda_i(L_1) + \cdots + \lambda_i(L_{i-1}) + L_i,$$

(2) $$(\lambda_i(L))_j = \begin{cases} \lambda_i(L_j) & \text{if } j < i, \\ L_j & \text{if } j = i, \\ 0 & \text{if } j > i, \end{cases}$$

(3) $$L_i = \lambda_i(L_{\geq i}) = (\lambda_i(L))_{\geq i}.$$

Proposition 3.3. *Let U be a closed subspace of $\mathrm{Span}_K(\mathcal{D})$, let $\Gamma := \{L^{(1)},\dots,L^{(r)}\}$ 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 4.3: 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:

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

Corollary 3.1. *A closed vector space $V \subset \mathrm{Span}_K(\mathcal{D})$ of dimension r can be represented by $\mathcal{O}(nr^2)$ elements in K.*

Proof. Let $\Gamma := \{L^{(1)},\dots,L^{(r)}\}$ be a basis of V, where, w.l.o.g. (see the beginning of subsections 1.2 and 3.3) $L^{(1)} = \mathrm{Id}$ and each $\langle L^{(1)},\dots,L^{(\ell)}\rangle$ 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. □

The following variant of the above representation is useful for performing Gaussian elimination:

Corollary 3.2. *Let U be a closed subspace of* $\mathrm{Span}_K(\mathcal{D})$*, let* $\Gamma_1 := \{L^{(11)}, \dots, L^{(1r_1)}\}$ *be a basis of U, let* $\Gamma_j := \{L^{(j1)}, \dots, L^{(jr_j)}\}$ *be a basis of* $U_j = \{L_{\geq j} : L \in U\}$ *for each* $j = 2, \dots, n$*. 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 3.3, $L_j = \rho_j(\sum_i c_{ij} L^{(i)}_{\geq j})$. Since $\sum_i c_{ij} L^{(i)}_{\geq j} \in U_j$ the assertion follows. □

Gaussian elimination with the alternative representation.

Technically, we will need often to perform Gaussian elimination within a closed subspace $V \subset \mathrm{Span}_K(\mathcal{D})$, using the alternative representation discussed in a previous section and we will have to do so with respect to some given ordering on $\mathcal{D}$. So let us discuss how to do that.

Lemma 3.2. *If Γ is a Gauss basis of a closed subspace V of* $\mathrm{Span}_K(\mathcal{D})$*, then* $T(\Gamma)$*, the vector space generated by* $\{T(L) : L \in \Gamma\}$*, is closed.*

Proof. It is obvious since either $\sigma_{X_i}(T(L)) = 0$ or $\sigma_{X_i}(T(L)) = T(\sigma_{X_i}(L))$. □

Lemma 3.3. *Let U be a closed subspace of* $\mathrm{Span}_K(\mathcal{D})$*, let* $\Gamma_j := \{L^{(j1)}, \dots, L^{(jr_j)}\}$ *be a Gauss basis of U_j for each* $j = 1 \dots n$*, and let L be s.t.* $V := U + \langle L \rangle$ *is closed. Then* $B_U := \{\rho_j L^{(ji)} : j = 1, \dots, n,\ i = 1, \dots, r_j\}$ *is a Gauss basis for the vector space it generates.*

Proof. We have seen that each element of V can be represented as

$$\sum_{j=1}^{n} \rho_j(\sum_{i=1}^{r_j} c_{ij} L^{(ji)})$$

with suitable c_{ji}. What we have to prove is that if $b_1, b_2 \in B_U$ are s.t. $T(b_1) = T(b_2)$, then $b_1 = b_2$. Remark that $\rho_j(L^{(ji)}) \in \mathrm{Span}_K(\mathcal{D}_j)$, so $T(\rho_j(L^{(ji)})) \in \mathcal{D}_j$ and $T(\rho_j(L^{(ji)})) \neq T(\rho_\mu(L^{(\mu l)}))$ for $\mu \neq j$. 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. □

The vector space generated by B_U contains $V := U + \langle L \rangle$. If a vector $w \in V$ and a basis of V are represented in terms of B_U, then we can perform Gaussian elimination for w in V at a cost of $\mathcal{O}(n^2r^2)$ operations in K, $\mathcal{O}(t^2n^2r^2)$ operations in k, since $\dim(\langle B_U \rangle) = \mathcal{O}(nr)$.

Testing ideal membership with this alternative representation.

The representation discussed in Proposition 3.3 is suitable for testing ideal membership of a polynomial f particularly if f is given by a "recursive Horner representation", i.e.

- 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.
- a polynomial f in $X_1, \dots, X_i$ of degree d in X_i is represented as $f = p_0 + X_i f_1$ where p_0 is a polynomial in $X_1, \dots, X_{i-1}$, f_1 is a polynomial in $X_1, \dots, X_i$ 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 $f_i \in K[X_1, \dots, X_i]$. Denote $\wp_0(f) := f_0$, $\wp_1(f) := f_1$, $\dots$, $\wp_i(f) := f_i$, $\dots$, $\wp_n(f) := f_n$. We will also write $\mathbf{T}_i$ for the semigroup generated by $\{X_1, \dots, X_i\}$.

Given a pointer to a list representation of f, one can extract $\wp_0(f)$ and the pointers to $\wp_n(f), \dots, \wp_1(f)$ 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 using Taylor formula and it is easy to see that computations can be arranged "à la FGLM" so to obtain $f(X+\mathbf{a})$ directly in recursive Horner representation, still at a cost of $\mathcal{O}(t^2\mu\sigma)$ operations in k . We can therefore assume that f is given in recursive Horner representation in the new frame.

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

$$\alpha^{(\ell)}_{j\tau} = \begin{cases} 0 & \text{if } \tau \text{ is no multiple of } X_j \ , \\ \sum_{i<\ell}\sum_{\nu=j}^{n} c_{ij}\alpha^{(i)}_{\nu\omega} & \text{if } \tau = X_j \cdot \omega \ . \end{cases}$$

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

Lemma 3.4. *The following hold for each j, for each ℓ:*

1) $\left(L^{(\ell)}_j(f)\right)(\mathbf{0}) = f^{(\ell)}_j(\mathbf{0})$,
2) $f^{(\ell)}_j = \sum_{i<\ell}\sum_{\nu=j}^{n} c_{ij}\wp_j(f^{(i)}_\nu)$.

Proof. As for 1): $\left(L^{(\ell)}_j(f)\right)(\mathbf{0}) = \sum_{\tau\in\mathbf{T}} \alpha^{(\ell)}_{j\tau} a_\tau = f^{(\ell)}_j(\mathbf{0})$.
As for 2): Let's remark that $\wp_j(f^{(i)}_\nu) = \sum\limits_{\omega\in\mathbf{T}_j} \omega \sum\limits_{\tau\in\mathbf{T}} a_{\tau X_j\omega}\alpha^{(i)}_{\nu\tau}$. Hence, one has

$$f^{(\ell)}_j = \sum_{\omega\in\mathbf{T}_j} \omega \sum_{\tau\in\mathbf{T}} a_{\tau\omega}\alpha^{(\ell)}_{j\tau} = \sum_{\omega\in\mathbf{T}_j} \omega \sum_{\tau\in\mathbf{T}} a_{\tau X_j\omega} \sum_{i<\ell}\sum_{\nu=j}^{n} c_{ij}\alpha^{(i)}_{\nu\tau}$$

$$= \sum_{i<\ell}\sum_{\nu=j}^{n} c_{ij} \sum_{\omega\in\mathbf{T}_j} \omega \sum_{\tau\in\mathbf{T}} a_{\tau X_j\omega}\alpha^{(i)}_{\nu\tau} = \sum_{i<\ell}\sum_{\nu=j}^{n} c_{ij}\wp_j(f^{(i)}_\nu). \qquad \square$$

Because of the recursive definition of $f^{(\ell)}_j$ implied by Lemma 3.3.2), accessing each $f^{(\ell)}_j$ 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:

$$0 = \left(L^{(\ell)}(f)\right)(\mathbf{0}) = \sum_j \left(L^{(\ell)}_j(f)\right)(\mathbf{0}) = \sum_j f^{(\ell)}_j(\mathbf{0}) = \sum_j \wp_0(f^{(\ell)}_j).$$

The test $\sum_j \wp_0(f_j^{(\ell)}) = 0\ \forall\ell$ requires again $\mathcal{O}(nr^2)$ arithmetical operations in K, $\mathcal{O}(nt^2r^2)$ arithmetical operations in k.

4. Conversion between representations

4.1 From differential conditions to a Gröbner basis.

The problem of finding the reduced Gröbner (or the border) basis of $\mathbf{q}$, once a basis of $\Delta(\mathbf{q})$ is known, is solved in [MMM] as a particular case of the more general problem of finding the Gröbner basis of a 0-dimensional ideal $\mathcal{I}$ of which a dual basis is known, i.e. a basis $\{L_1, \dots, L_r\}$ of the K-vector space of those linear functionals $L : \mathcal{P}_K \longrightarrow K$ s.t. $L(f) = 0\ \forall f \in \mathcal{I}$.

The algorithm produces the terms (in increasing order) which are either in $\mathbf{N}(\mathcal{I})$ or minimal generators of $T(\mathcal{I})$, and for each of them, say τ, it computes the vector $v(\tau) = (L_1(\tau), \dots, L_r(\tau))$ and tests if it is not linearly dependent over $\{v(\omega) : \omega \in \mathbf{N}(\mathcal{I}), \omega < \tau\}$. If this is the case, then $\tau \in \mathbf{N}(\mathcal{I})$, otherwise there is a relation $v(\tau) = \sum c_\omega v(\omega)$ and then $\tau - \sum c_\omega \omega$ is an element of the reduced Gröbner basis of $\mathcal{I}$.

The complexity of the algorithm depends on the costs of evaluating $L_i(\omega)$; for this particular case, the complexity is $\mathcal{O}(nr^3)$, *cf.* [MMM].

4.2 From a standard basis to a Gröbner basis.

Let us assume we are given the reduced standard basis of $\mathbf{q}$ w.r.t. an ordering $<$ with $X_i < 1\ \forall i$. Once the border basis of $\mathbf{q}$ is known, the algorithm of Section 4.1 can be directly applied to compute the reduced Gröbner (or the border) basis of $\mathcal{I}$ for any given ordering, with $\mathcal{O}(nr^3)$ computations in K. In fact, let the mappings $L_\tau : \mathcal{P}_K \longrightarrow K$ be given by

$$\mathrm{Can}_<(f, \mathbf{q}) = \sum_{\tau \in \mathbf{N}(\mathbf{q})} L_\tau(f)\tau.$$

These L_τ are linear functionals and constitute a dual basis of $\mathbf{q}$ since

$$f \in \mathbf{q} \iff \mathrm{Can}_<(f, \mathbf{q}) = 0 \iff L_\tau(f) = 0\ \forall \tau \in \mathbf{N}(\mathbf{q}).$$

However, the FGLM approach to obtain the border basis from the reduced standard basis of $\mathbf{q}$ doesn't work directly anymore. In fact it is based on the formula

$$\mathrm{Can}(\omega, \mathbf{q}) = \sum_{\tau \in \mathbf{N}(\mathbf{q})} L_\tau(\omega)\tau \Longrightarrow \mathrm{Can}(X_i\omega, \mathbf{q}) = \sum_{\tau \in \mathbf{N}(\mathbf{q})} L_\tau(\omega)\,\mathrm{Can}(X_i\tau, \mathbf{q}).$$

which allows to compute $\mathrm{Can}(\omega, \mathbf{q})$ for all $\omega \in \mathbf{B}(\mathcal{I})$ in increasing order (N.B. this holds in the case $X_i > 1, \forall i$), since

$$\omega < X_i\omega, \quad L_\tau(\omega) \neq 0 \Longrightarrow \tau < \omega, \quad \text{and} \quad X_i\tau < X_i\omega,$$

so that when $\mathrm{Can}(X_i\omega, \mathbf{q})$ is computed , both $\mathrm{Can}(\omega, \mathbf{q})$ and $\mathrm{Can}(X_i\tau, \mathbf{q})$ for all $\tau \in N(\mathbf{q})$, $\tau < X_i\omega$ are already known. This is the case, when all $\mathrm{Can}(\tau, \mathbf{q})$ are computed by increasing τ.

With an ordering $<$ s.t. $X_i < 1$ instead one has

$$X_i\omega < \omega, \quad L_\tau(\omega) \neq 0 \Longrightarrow \tau < \omega, \quad \text{and} \quad X_i\tau < X_i\omega,$$

so that, when computing $\mathrm{Can}(X_i\omega, \mathbf{q})$, one either doesn't know $\mathrm{Can}(\omega, \mathbf{q})$ — if working by increasing order — or $\mathrm{Can}(X_i\tau, \mathbf{q})$ — if working by decreasing order. We therefore have to modify the FGLM algorithm to apply also to this case.

Let us begin by indexing $\mathbf{N}(\mathbf{q})$ as $\{\tau_1, \dots, \tau_r\}$ where $1 = \tau_1 > \tau_2 > \dots > \tau_r$, by denoting $\mathbf{m}^{[i]}$ the $\mathbf{m}$-primary ideal generated by $\{\omega : \omega < \tau_i\}$ and by $\mathbf{q}^{[i]}$ the $\mathbf{m}$-primary component $\mathbf{q} + \mathbf{m}^{[i]}$; remark that $\mathbf{m}^{[1]} = \mathbf{q}^{[1]} = \mathbf{m}$ and $\mathbf{q}^{[r]} = \mathbf{q}$. We will show how to compute $\mathrm{Can}(\tau, \mathbf{q}^{[i]})$ for each $\tau \in \mathbf{B}(\mathbf{q})$ assuming $\mathrm{Can}(\tau, \mathbf{q}^{[i-1]})$ known for each $\tau \in \mathbf{B}(\mathbf{q})$. Since $\mathbf{B}(\mathbf{q}) \subset \mathbf{m}^{[1]}$ one has $\mathrm{Can}(\tau, \mathbf{q}^{[1]}) = 0\ \forall \tau \in \mathbf{B}(\mathbf{q})$, allowing initialization of the inductive process. Remark that all we have to compute is $L_{\tau_i}(\tau)\,\forall \tau \in \mathbf{B}(\mathbf{q}), \tau > \tau_i$; we will do that, by increasing order of the τ's. There are two cases:

- if τ is a minimal generator of $T(\mathbf{q})$, then $Can(\tau, \mathbf{q})$ and so $L_{\tau_i}(\tau)$ is known,
- otherwise, $\tau = X_l \omega$ for some $\omega \in \mathbf{B}(\mathbf{q})$; then

$$L_{\tau_i}(X_l\omega) = \sum_{\sigma \in \mathbf{N}(\mathbf{q})} L_\sigma(\omega) L_{\tau_i}(X_l \sigma) = \sum_{\substack{\sigma \in \mathbf{N}(\mathbf{q}) \\ X_l\sigma \geq \tau_i}} L_\sigma(\omega) L_{\tau_i}(X_l\sigma).$$

Since $L_\sigma(\omega) \neq 0$ implies $\sigma < \omega$ and so $X_l\sigma < X_l\omega = \tau$ and $X_l\sigma \geq \tau_i$ implies $\sigma \geq \tau_{i-1}$, both $L_\sigma(\omega)$ and $L_{\tau_i}(X_l\sigma)$ are known for all σ s.t. $L_\sigma(\omega) \neq 0$.

The cost of computing $L_{\tau_i}(\tau)$ is therefore $\mathcal{O}(r)$ and so the total cost of computing the border basis of $\mathbf{q}$ is $\mathcal{O}(nr^3)$; in fact the computations are the same required by the FGLM approach, just ordered differently.

4.3 From a basis of a zero-dimensional ideal to a Gauss basis of differential conditions at a multiple point.

Preliminaries.

Let us recall the following easy consequence of the Leibniz formula:

$$\forall L \in \mathrm{Span}_K(\mathcal{D}), \forall f, g \in \mathcal{P}_K \quad L(fg) = \sum_{\tau \in \mathbf{T}} D(\tau)(g)\ \sigma_\tau(L(f))$$

which enables us to work with bases instead of the corresponding vector spaces:

Lemma 4.1 [MS]. *Let $\{L^{(1)}, \dots, L^{(r)}\}$ be a basis of a closed space V and let $\{f_1, \dots, f_s\}$ be any basis of the ideal $\mathcal{I} \subset \mathcal{P}_K$.*

If $L^{(i)}(f_j)(\mathbf{0}) = 0$, $\forall i, j$, then $L(f)(\mathbf{0}) = 0$, $\forall f \in \mathcal{I}$, $\forall L \in V$.

Proof. Let $f = \sum_j g_j f_j$ and let $L \in V$. Then $\sigma_\tau(L) \in V$, since V is closed and therefore $(\sigma_\tau(L)(f_j))(\mathbf{0}) = 0\ \forall \tau \in \mathbf{T}$, $\forall j$. By the Leibniz formula, then

$$L(f) = \sum_j L(g_j f_j) = \sum_j \sum_\tau D(\tau)(g_j) \sigma_\tau(L)(f_j).$$

Evaluation at $\mathbf{0}$ gives the assertion. □

Let us recall the representation of differential conditions discussed in subsection 3.3.

Let $\mathcal{I}$ be a zero-dimensional ideal, let $V := \Delta(\mathcal{I})$ and let $\Gamma := \{L^{(1)}, \dots, L^{(r)}\}$ be a Gauss basis of V. Then $\forall \ell$, there are $c_{ij} \in K$ s.t.

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

Moreover if for some i, j there is an l s.t. $T(L^{(l)}) = \rho_j T(L^{(i)}_{\geq j})$, then any occurrence of $\rho_j(L^{(i)}_{\geq j})$ in the formula above can be replaced by Gaussian reduction with $L^{(l)}$.

So in the representation of a basis element only terms $\rho_j(L^{(i)}_{\geq j})$ can appear s.t. $\rho_j T(L^{(i)}_{\geq j}) \notin \{T(L^{(1)}), \dots, T(L^{(\ell-1)})\}$.

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

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

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

Let now U be the closed vector space generated by $\{L^{(1)}, \dots, L^{(\ell-1)}\}$; to find the next generator $L^{(\ell)}$ of $\Delta(\mathcal{I})$, one could try to produce an element

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

whose leading term is the minimal $D(t)$ among the possible candidates, and check whether $L(f)(\mathbf{0}) = 0$ for all f 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.

By our experiences, it seems to be more efficient to test first the existence of L s.t. $\sigma_i(L) \in U \ \forall i$ and then to check whether $L(f)(\mathbf{0}) = 0$ for all f in the given basis, than to try to find first an L satisfying $L(f)(\mathbf{0}) = 0$ for all basis elements f and then to check whether $U + \langle L\rangle$ is closed. We observed, that more frequently $\sigma_i(L) \notin U$ for an i than $L(f) \neq 0$ for a basis element f. This can be seen also in the following example.

Example 4.1. Let $\mathcal{I}$ be the ideal $(X - YZ, Y - Z^2, Y^2)$ and let $<$ be the lexicographical term ordering with $X > Y > Z$. An initial segment of the reduced Gauss basis of $\Delta(\mathcal{I})$ is $L^{(1)} = \mathrm{Id}$, $L^{(2)} = D(Z)$, $L^{(3)} = D(Y) + D(Z^2)$, $L^{(4)} = D(X)+D(YZ)+D(Z^3)$. The leading term of the next element in the basis, if any, is necessarily either $D(XZ), D(XY), D(X^2)$, which are the only $D(t) > D(X)$ s.t. $\forall i \ \sigma_i(D(t)) = T(L^{(j_i)})$ for some j_i.

If we take for the next L one of the following $\rho_X(L^{(2)}) = D(XZ)$, or $\rho_X(L^{(3)}) = D(XY) + D(XZ^2)$, or $\rho_X(L^{(4)}) = D(X^2) + D(XYZ) + D(XZ^3)$, then $L(f)(\mathbf{0}) = 0$ for all f in the given basis; however $\sigma_Z\rho_X(L^{(2)})$, $\sigma_Z\rho_X(L^{(3)})$, $\sigma_Y\rho_X(L^{(4)})$ are not in the vector space U generated by $\{L^{(1)}, L^{(2)}, L^{(3)}, L^{(4)}\}$; for $t = XY, X^2$ there is no element L s.t. $T(L) = D(t)$ and $\sigma_i(L) \in U \ \forall i$; only for $t = XZ$ there is an element L s.t. $T(L) = D(XZ)$ and $\sigma_i(L) \in U \ \forall i$, which is $L := D(XZ) + D(Y^2) + D(YZ^2) + D(Z^4)$ for which however $L(Y^2)(\mathbf{0}) = 1$. This allows to conclude that $U = \Delta(\mathcal{I})$.

Continuations of a closed vector space.
The problem to be solved first is as follows:
Given a closed vector space $U \subset \mathrm{Span}_K(\mathcal{D})$, find all $L \in \mathrm{Span}_K(\mathcal{D}) \setminus U$ s.t. $V = U + \langle L\rangle$ is closed.

Let $<$ be a term ordering on $\mathbf{T}$ and let $\Gamma = \{L^{(1)}, \dots, L^{(r)}\}$ be the reduced Gauss basis of U, so that necessarily $L^{(1)} = \mathrm{Id}$. As shown in Lemma 3.2, the space $T(U) = \langle T(L^{(1)}), \dots, T(L^{(r)})\rangle$ is a closed subspace.

If $L \in \mathrm{Span}_K(\mathcal{D}) \setminus U$ 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

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

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

Let $D(t) \in \mathcal{C}(U)$; an element $L \in \mathrm{Span}_K(\mathcal{D})$ s.t. c1) $T(L) = D(t)$

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

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

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 4.2. *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 4.3. *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 4.1. *If a continuation of U at t exists, then 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 $L' = D(t) + \sum c_i D(\tau_i)$ 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 4.1. *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 any continuation of U is a linear combination of elementary continuations of it. □

Here is an example which shows that a continuation of U at t could not exist.

Example 4.2. Let $<$ be the lexicographical ordering s.t. $X > Y > Z$ and let U be generated by

$$\Gamma := \{\mathrm{Id}, D(Z), D(Y), D(Y^2), D(YZ), D(X), D(XY) + D(XZ)\}.$$

Then $\mathcal{C}(U) = \{D(Z^2), D(Y^3), D(Y^2Z), D(XZ), D(XY^2), D(X^2)\}$.

It is easy to verify that $D(Z^2), D(Y^3), D(Y^2Z), D(XZ), D(X^2)$ are elementary continuations of U.

For $D(t)$ to appear in the elementary continuation L of U at XY^2, it must occur that

- $D(t) \notin T(U)$
- $D(t) \notin \mathcal{C}(U)$, since all elements in $\mathcal{C}(U)$ less than $D(XY^2)$ have a continuation
- $\sigma_i(D(t)) \in T(U) \cup \{D(XZ)\}, \forall i$; in fact $\sigma_i(L)$ must be a linear combination of the elements of Γ.

So necessarily $L = D(XY^2)$; but then $\sigma_Y(L) = D(XY) \notin U$.

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 whether the elementary continuation of U at t exists, which is easily transformed into an algorithm to compute it.

Theorem 4.1. *Let $D(t) \in \mathcal{C}(U) \cap \mathcal{D}_\kappa$ 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 $I(j)$ denote the set of indices i s.t.

- *$T(\rho_j(L^{(i)})) \notin T(U)$,*
- *$T(\rho_j(L^{(i)})) < D(t)$ (which implies $L^{(i)} \in \mathrm{Span}_K(\mathcal{D}_\kappa)$),*
- *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 linear equations has solutions $d_{(j,i)} \in K$:*

$$C^{(\kappa)} = \rho_\kappa(L^{(i_\kappa)}) + \sum_{i \in I(\kappa)} d_{(\kappa,i)} \rho_\kappa(L^{(i)}) \qquad (c_\kappa)$$

$$\sigma_{\kappa+1}(C^{(\kappa)}) = \sum_{i \in I(\kappa+1)} d_{(\kappa+1,i)} L^{(i)}_{\leq \kappa} \qquad (d_{\kappa+1})$$

$$C^{(\kappa+1)} = \sum_{i \in I(\kappa+1)} d_{(\kappa+1,i)} \rho_{\kappa+1}(L^{(i)}_{\geq \kappa+1}) \qquad (c_{\kappa+1})$$

$$\vdots$$

$$\sigma_j(\sum_{l=\kappa}^{j-1} C^{(l)}) = \sum_{i \in I(j)} d_{(j,i)} L^{(i)}_{\leq j-1} \qquad (d_j)$$

$$C^{(j)} = \sum_{i \in I(j)} d_{(j,i)} \rho_j(L^{(i)}_{\geq j}) \qquad (c_j)$$

$$\vdots$$

$$\sigma_{n-1}(\sum_{l=\kappa}^{n-2} C^{(l)}) = \sum_{i \in I(n-1)} d_{(n-1,i)} L^{(i)}_{\leq n-2} \qquad (d_{n-1})$$

$$C^{(n-1)} = \sum_{i \in I(n-1)} d_{(n-1,i)} \rho_{n-1}(L^{(i)}_{\geq n-1}) \qquad (c_{n-1})$$

$$\sigma_n(\sum_{l=\kappa}^{n-1} C^{(l)}) = \sum_{i\in I(n)} d_{(n,i)} L^{(i)}_{\leq n-1} \qquad (d_n)$$

$$C^{(n)} = \sum_{i\in I(n)} d_{(n,i)} \rho_n(L^{(i)}_{\geq n}) \qquad (c_n)$$

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 $C_\kappa = \rho_\kappa(L^{(i_\kappa)}) + \sum_i d_{(\kappa,i)}\rho_\kappa(L^{(i)}) =: C^{(\kappa)}$. We notice that in the sum, 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

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

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

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

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; so C is the elementary continuation of U at t. □

Remark that, in general, the above set of equations could have no solution s.t. $d_{(\kappa,i)} = 0 \ \forall i$ even in case $T(L^{(i)}_\kappa) \in \mathcal{C}(U)$ and no continuation of U at $T(L^{(i)}_\kappa)$ exists. This can be seen by the following:

Example 4.3. Let us find the continuation at X^2Y of the closed space $V = U + \langle L^{(8)}\rangle$, where U is the space of Example 4.2, generated by

$$\Gamma := \{\mathrm{Id}, D(Z), D(Y), D(Y^2), D(YZ), D(X), D(XY) + D(XZ)\}$$

whose elements will be listed in order $L^{(1)}, \dots, L^{(7)}$ and where $L^{(8)} := D(X^2) + aD(XZ)$ which is a continuation of U at X^2.

Recall that $D(Z^2), D(Y^3), D(Y^2Z), D(XZ)$ are elementary continuations of U and so of V and that there is no continuation of U (and so of V) at XY^2. The next points in the corner set of V are X^2Y and X^3.

At X^2Y one has $I(X) = \{4, 5, 7\}$, $I(Y) = \{7, 8\}$, $I(Z) = \{5, 7, 8\}$.

We have:

$$\begin{aligned}
C^{(X)} =& \rho_X(L^{(7)} + d_{(5,X)}L^{(5)} + d_{(4,X)}L^{(4)})\\
=& D(X^2Y) + D(X^2Z) + d_{(5,X)}D(XYZ) + d_{(4,X)}D(XY^2),\\
\sigma_Y(C^{(X)}) =& D(X^2) + d_{(5,X)}D(XZ) + d_{(4,X)}D(XY)\\
=& d_{(8,Y)}L^{(8)}_{\geq X} + d_{(7,Y)}L^{(7)}_{\geq X}\\
=& d_{(8,Y)}D(X^2) + ad_{(8,Y)}D(XZ) + d_{(7,Y)}D(XY) + d_{(7,Y)}D(XZ),
\end{aligned}$$

whence $d_{(8,Y)} = 1, d_{(5,X)} = a + d_{(7,Y)}, d_{(4,X)} = d_{(7,Y)}$ and, using $d := d_{(7,Y)}$ for short,

$$\begin{aligned}
C^{(Y)} =& \rho_Y(L^{(8)}_{\geq Y} + dL^{(7)}_{\geq Y}) = 0,\\
\sigma_Z(C^{(X)} + C^{(Y)}) =& D(X^2) + (a + d)D(XY)\\
=& d_{(8,Z)}L^{(8)}_{\leq Y} + d_{(7,Z)}L^{(7)}_{\leq Y} + d_{(5,Z)}L^{(5)}_{\leq Y}\\
=& d_{(8,Z)}D(X^2) + d_{(8,Z)}aD(XZ)\\
&+ d_{(7,Z)}D(XY) + d_{(7,Z)}D(XZ) + d_{(5,Z)}D(YZ),
\end{aligned}$$

whence we find $d_{(8,Z)} = 1$, $ad_{(8,Z)} + d_{(7,Z)} = 0$, $d_{(7,Z)} = a + d$, $d_{(5,Z)} = 0$ so that

$$d_{(7,Z)} = -a, \quad d = -2a, \quad d_{(5,X)} = -a, \quad d_{(4,X)} = -2a$$

gives the solution

$$C = D(X^2Y) + D(X^2Z) - aD(XYZ) - 2aD(XY^2)$$

In fact

$$\sigma_X(C) = D(XY) + D(XZ) - aD(YZ) - 2aD(Y^2) = L^{(7)} - aL^{(5)} - 2aL^{(4)},$$

$$\sigma_Y(C) = D(X^2) - aD(XZ) - 2aD(XY) = L^{(8)} - 2aL^{(7)},$$

$$\sigma_Z(C) = D(X^2) - aD(XY) = L^{(8)} - aL^{(7)}. \qquad \square$$

In order to solve the above system of equations with good complexity, one must however use the Gauss basis B_V. So, adopting freely the notation of Corollary 3.2, one also needs to know:

- a representation of each $L^{(i)}_{\geq j}$ in terms of 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) $\forall j$, $\forall \lambda > j$, a representation of $\sigma_\lambda \rho_j(C_{\geq j})$ in terms of B_V.

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 4.1; from the Gaussian representation $C_{\geq j} = \sum c_{\mu\kappa}\rho_\mu(L^{(\mu\kappa)})$ one obtains

$$\sigma_\lambda\rho_j(C_{\geq j}) = \rho_j\Big(\sum c_{\mu\kappa}\sigma_\lambda\rho_\mu(L^{(\mu\kappa)})\Big).$$

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 4.1, assuming the knowledge above. While the linear system of equations of Theorem 4.1 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 $\rho_j(L_\nu^{(i)})$ 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. As for problem b) it is again a set of Gaussian eliminations and so the complexity is the same.

To illustrate our procedure, let us explicitly compute an example:

Example 4.4. We have $\Gamma_1 = \{L^{(X1)}, \dots, L^{(X6)}\}$, $\Gamma_2 = \{L^{(Y1)}, \dots, L^{(Y6)}\}$, $\Gamma_3 = \{L^{(Z1)}, \dots, L^{(Z6)}\}$, where:

$$\begin{aligned}
L^{(X1)} =& \mathrm{Id}\\
L^{(Y1)} =& \mathrm{Id}\\
L^{(Z1)} =& \mathrm{Id}
\end{aligned}$$

$$\begin{aligned}
L^{(X2)} =& \rho_Z(L^{(Z1)}) = D(Z)\\
L^{(Y2)} =& \rho_Z(L^{(Z1)}) = D(Z)\\
L^{(Z2)} =& \rho_Z(L^{(Z1)}) = D(Z)
\end{aligned}$$

$$\begin{aligned}
L^{(X3)} =& \rho_Y(L^{(Y1)}) + \rho_Z(L^{(Z2)}) = D(Y) + D(Z^2)\\
L^{(Y3)} =& \rho_Y(L^{(Y1)}) + \rho_Z(L^{(Z2)}) = D(Y) + D(Z^2)\\
L^{(Z3)} =& \rho_Z(L^{(Z2)}) = D(Z^2)
\end{aligned}$$

$$\begin{aligned}
L^{(X4)} =& \rho_X(L^{(X1)}) + \rho_Y(L^{(Y2)}) + \rho_Z(L^{(Z3)}) = D(X) + D(YZ) + D(Z^3)\\
L^{(Y4)} =& \rho_Y(L^{(Y2)}) + \rho_Z(L^{(Z3)}) = D(YZ) + D(Z^3)\\
L^{(Z4)} =& \rho_Z(L^{(Z3)}) = D(Z^3)
\end{aligned}$$

$$\begin{aligned}
L^{(X5)} =&\rho_X(L^{(X2)}) + \rho_Y(L^{(Y3)}) + \rho_Z(L^{(Z4)})\\
=&D(XZ) + D(Y^2) + D(YZ^2) + D(Z^4)\\
L^{(Y5)} =&\rho_Y(L^{(Y3)}) + \rho_Z(L^{(Z4)}) = D(Y^2) + D(YZ^2) + D(Z^4)\\
L^{(Z5)} =&\rho_Z(L^{(Z4)}) = D(Z^4)
\end{aligned}$$

$$\begin{aligned}
L^{(X6)} =&\rho_X(L^{(X3)}) + \rho_Y(L^{(Y4)}) + \rho_Z(L^{(Z5)})\\
=&D(XY) + D(XZ^2) + D(Y^2Z) + D(YZ^3) + D(Z^5)\\
L^{(Y6)} =&\rho_Y(L^{(Y4)}) + \rho_Z(L^{(Z5)}) = D(Y^2Z) + D(YZ^3) + D(Z^5)\\
L^{(Z6)} =&\rho_Z(L^{(Z5)}) = D(Z^5)
\end{aligned}$$

We have also:

$$\begin{aligned}
\sigma_Y\rho_X(L^{(X1)}) =&0\\
\sigma_Z\rho_X(L^{(X1)}) =&0\\
\sigma_Z\rho_Y(L^{(Y1)}) =&0
\end{aligned}$$

$$\begin{aligned}
\sigma_Y\rho_X(L^{(X2)}) =&0\\
\sigma_Z\rho_X(L^{(X2)}) =&\rho_X(L^{(X1)}) = D(X)\\
\sigma_Z\rho_Y(L^{(Y2)}) =&\rho_Y(L^{(Y1)}) = D(Y)
\end{aligned}$$

$$\begin{aligned}
\sigma_Y\rho_X(L^{(X3)}) =&\rho_X(L^{(X1)}) = D(X)\\
\sigma_Z\rho_X(L^{(X3)}) =&\rho_X(L^{(X2)}) = D(XZ)\\
\sigma_Z\rho_Y(L^{(Y3)}) =&\rho_Y(L^{(Y2)}) = D(YZ)
\end{aligned}$$

$$\begin{aligned}
\sigma_Y\rho_X(L^{(X4)}) =&\rho_X(L^{(X2)}) = D(XZ)\\
\sigma_Z\rho_X(L^{(X4)}) =&\rho_X(L^{(X3)}) = D(XY) + D(XZ^2)\\
\sigma_Z\rho_Y(L^{(Y4)}) =&\rho_Y(L^{(Y3)}) = D(Y^2) + D(YZ^2)
\end{aligned}$$

$$\begin{aligned}
\sigma_Y\rho_X(L^{(X5)}) =&\rho_X(L^{(X3)}) = D(XY) + D(XZ^2)\\
\sigma_Z\rho_X(L^{(X5)}) =&\rho_X(L^{(X4)}) = D(X^2) + D(XYZ) + D(XZ^3)\\
\sigma_Z\rho_Y(L^{(Y5)}) =&\rho_Y(L^{(Y4)}) = D(Y^2Z) + D(YZ^3)
\end{aligned}$$

$$\begin{aligned}
\sigma_Y\rho_X(L^{(X6)}) =&\rho_X(L^{(X4)}) = D(X^2) + D(XYZ) + D(XZ^3)\\
\sigma_Z\rho_X(L^{(X6)}) =&\rho_X(L^{(X5)}) = D(X^2Z) + D(XY^2) + D(XYZ^2) + D(XZ^4)\\
\sigma_Z\rho_Y(L^{(Y6)}) =&\rho_Y(L^{(Y5)}) = D(Y^3) + D(Y^2Z^2) + D(YZ^4)
\end{aligned}$$

It is easy to verify that $D(Z^2)$, $D(YZ) + D(Z^3)$, $D(Y^2) + D(YZ^2) + D(Z^4)$ are elementary continuations. We look for an elementary continuation at the next admissible term, i.e. X^2. We have $I(X) = \{4\}$, $I(Y) = \{5, 6\}$, $I(Z) = \{5, 6\}$.

We have:

$$\begin{aligned}
C^{(X)} =& \rho_X(L^{(X4)}),\\
\sigma_Y(C^{(X)}) =& \sigma_Y\rho_X(L^{(X4)}) = \rho_X(L^{(X2)}) = L^{(X5)}_{\leq X},\\
L^{(X5)}_{\geq Y} =& \rho_Y(L^{(Y3)}) + \rho_Z(L^{(Z4)}) = L^{(Y5)},\\
C^{(Y)} =& \rho_Y(L^{(Y5)}),\\
\sigma_Z(C^{(X)} + C^{(Y)}) =& \sigma_Z\rho_X(L^{(X4)}) + \sigma_Z\rho_Y(L^{(Y5)})\\
=& \rho_X(L^{(X3)}) + \rho_Y(L^{(Y4)}) = L^{(X6)}_{\leq Y},\\
L^{(X6)}_{\geq Z} =& \rho_Z(L^{(Z5)}) = L^{(Z6)},\\
C^{(Z)} =& \rho_Z(L^{(Z6)}),
\end{aligned}$$

so that

$$\begin{aligned}
C &= \rho_X(L^{(X4)}) + \rho_Y(L^{(Y5)}) + \rho_Z(L^{(Z6)})\\
&= D(X^2) + D(XYZ) + D(XZ^3) + D(Y^3) + D(Y^2Z^2) + D(YZ^4) + D(Z^6).
\end{aligned}$$

As for the auxiliary problems, it is immediate that $C^{(X)}$, $C^{(Y)}$, $C^{(Z)}$ are reduced w.r.t. Γ_i. Also, from the computations above one reads directly that:

$$\begin{aligned}
\rho_X\sigma_Y(C) =& \rho_X(L^{(X5)}),\\
\rho_X\sigma_Z(C) =& \rho_X(L^{(X6)}),\\
\rho_Y\sigma_Z(C) =& \rho_Y(L^{(Y6)}). \qquad \square
\end{aligned}$$

Computing elementary continuations under any 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 4.1 is lost. We have however:

Proposition 4.2. *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 has solutions $c_{(ji)}, d_{\mu i} \in K$:*

$$\sigma_\mu\rho_\kappa(L^{(\kappa\lambda)}) + \sum_{j=1}^{n}\sum_{i\in J(j)} c_{(ji)}\sigma_\mu\rho_j(L^{(ji)}) = \sum_{i=1}^{r_1} d_{\mu i}L^{(1i)}, \qquad \mu = 2, \dots, n.$$

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 requires solving $\mathcal{O}(n^2 r)$ equations in $\mathcal{O}(nr)$ unknowns and so $\mathcal{O}(n^4 r^3)$ arithmetical operations in K.

Example 4.5. Let us now consider Example 4.4 with the lexicographical ordering s.t. $Y > X > Z$.

One can easily verify that Γ_1, Γ_2, Γ_3 are Gauss bases of U also under this ordering; only the leading terms change; they are:

$$\begin{array}{lll}
T(L^{(X1)}) = D(1) & T(L^{(Y1)}) = D(1) & T(L^{(Z1)}) = D(1)\\
T(L^{(X2)}) = D(Z) & T(L^{(Y2)}) = D(Z) & T(L^{(Z2)}) = D(Z)\\
T(L^{(X3)}) = D(Y) & T(L^{(Y3)}) = D(Y) & T(L^{(Z3)}) = D(Z^2)\\
T(L^{(X4)}) = D(YZ) & T(L^{(Y4)}) = D(YZ) & T(L^{(Z4)}) = D(Z^3)\\
T(L^{(X5)}) = D(Y^2) & T(L^{(Y5)}) = D(Y^2) & T(L^{(Z5)}) = D(Z^4)\\
T(L^{(X6)}) = D(Y^2Z) & T(L^{(Y6)}) = D(Y^2Z) & T(L^{(Z6)}) = D(Z^5)
\end{array}$$

Therefore we can use the information already derived in Example 4.4.

One has $\mathcal{C}(U) = \{D(Z^2), D(X), D(Y^3)\}$. It is easy to verify that $D(Z^2)$ and $D(X)$ are elementary continuation. So let us look for an elementary continuation at $D(Y^3) = \rho_Y(T(L^{(Y5)})$.

One has $J(X) = \{2,3,4,5,6\}$, $J(Y) = \emptyset$, $J(Z) = \{3,4,5,6\}$. Therefore, we make the Ansatz:

$$\begin{aligned}
C =& \rho_Y(L^{(Y5)}) + c_{X6}\rho_X(L^{(X6)}) + c_{X5}\rho_X(L^{(X5)}) + c_{X4}\rho_X(L^{(X4)})\\
&+ c_{X3}\rho_X(L^{(X3)}) + c_{X2}\rho_X(L^{(X2)})\\
&+ c_{Z6}\rho_Z(L^{(Z6)}) + c_{Z5}\rho_Z(L^{(Z5)}) + c_{Z4}\rho_Z(L^{(Z4)}) + c_{Z3}\rho_Z(L^{(Z3)}).
\end{aligned}$$

One has

$$\begin{aligned}
\sigma_Y(C) = & \rho_Y(L^{(Y3)}) + \rho_Z(L^{(Z4)}) + c_{X6}\rho_X(L^{(X4)}) + c_{X5}\rho_X(L^{(X3)})\\
&+ c_{X4}\rho_X(L^{(X2)}) + c_{X3}\rho_X(L^{(X1)}).
\end{aligned}$$

Gaussian elimination by Γ_1 gives

$$c_{X6} = 0, \quad c_{X5} = 0, \quad c_{X4} = 1, \quad c_{X3} = 0,$$

and $\sigma_Y(C) = L^{(X5)}$. Also

$$\begin{aligned}
\sigma_Z(C) =& \rho_Y(L^{(Y4)}) + \rho_X(L^{(X3)}) + c_{X2}\rho_X(L^{(X1)}) + c_{Z6}\rho_Z(L^{(Z5)})\\
&+ c_{Z5}\rho_Z(L^{(Z4)}) + c_{Z4}\rho_Z(L^{(Z3)}) + c_{Z3}\rho_Z(L^{(Z2)}).
\end{aligned}$$

Gaussian elimination by Γ_1 gives

$$c_{X2} = 0, \quad c_{Z6} = 1, \quad c_{Z5} = 0, \quad c_{Z4} = 0, \quad c_{Z3} = 0,$$

and $\sigma_Z(C) = L^{(X6)}$.

We obtain therefore $C = \rho_Y(L^{(Y5)}) + \rho_X(L^{(X4)}) + \rho_Z(L^{(Z6)})$ i.e. the same element as in Example 4.4, so that the auxiliary problems are solved as in the previous example. □

An algorithm to pass from a basis of a zero-dimensional ideal to differential conditions for a primary component. The algorithm takes in input a basis $\{f_1, \dots, f_m\}$ of a 0-dimensional ideal and returns a Gauss basis of the closed vector space of differential conditions defining the primary component of the ideal at the origin.

It uses the following data:

- $\Gamma_i = \{L^{(i1)}, \dots, L^{(i\kappa_i)}\}$, Gauss bases for the projections U_i of a closed space U of differential conditions, $i = 1, \dots, n$,
- $\Lambda := \{C_{U,\tau} : D(\tau) < T(L^{(\kappa)})\}$,
- $\mathcal{B} := \{\tau \in \mathcal{C}(U) : D(\tau) > T(L^{(\kappa)})\}$.

At initialization: $\Gamma_i := \{L^{(i1)}\}$ where $L^{(i1)} = Id$, $\Lambda := \emptyset$, $\mathcal{B} := \{D(X_i) : i = 1, \dots, n\}$.

At termination, Γ_1 is the reduced Gauss basis of $\Delta(\mathcal{I})$, $\Lambda := \{C_{U,\tau} : \tau \in \mathcal{C}(U)\}$, $\mathcal{B} := \emptyset$.

The algorithms outlined in the previous section are used to compute $C_{U,\tau}$ for each $\tau \in \mathcal{C}(U)$.

```
Repeat
  $t := \min_{\mathcal{B}}(\tau)$
  $\mathcal{B} := \mathcal{B} \setminus \{t\}$
  If $C_{U,t}$ exists then
    If $\exists c_\tau \in K : C_{U,t}(f_j)(\mathbf{0}) = \sum_{C_{U,\tau}\in\Lambda} c_\tau C_{U,\tau}(f_j)(\mathbf{0}), j = 1, \dots, m$, 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 $j = 2 \dots n$ do
        Let $L$ be the Gaussian reduction of $L_{\geq j}^{(1\kappa_1)}$ w.r.t. $\Gamma_j$
        If $L \neq 0$ then
          $\kappa_j := \kappa_j + 1$, $L^{(j\kappa_j)} := L$, $\Gamma_j := \Gamma_j \cup \{L^{(j\kappa_j)}\}$
      $\mathcal{B} := \mathcal{B} \cup \{\rho_j(D(t)) : j = 1, \dots, n, X_j t \in \mathcal{C}(U)\}$
    else
    $\Lambda := \Lambda \cup \{C_{U,t}\}$
until $\mathcal{B} = \emptyset$
```

Complexity of the algorithm.

We will measure space and time complexity of the algorithm above in terms of the following values:

- n, the number of variables,
- $t := \dim_k(K)$,
- r, the multiplicity of the primary component,
- m, the cardinality of the given basis $\{f_1, \dots, f_m\}$ of $\mathcal{I}$,
- $\Sigma := \sum_{i=1}^{m} \#(\Sigma_i)$ where Σ_i is the staircase generated by f_i.

Let us first discuss space complexity:

- each Γ_i requires $\mathcal{O}(ntr^2)$ elements in k (see Corollary 3.1);
- for each $L^{(ji)} \in \Gamma_j$ one needs to store $\sigma_\lambda \rho_j(L^{(ji)})$ for $\lambda > j$; all these data require $\mathcal{O}(n^3tr^2)$ elements in k;
- the cardinality of Λ is at most nr and the storage of each element $C \in \Lambda$ requires $\mathcal{O}(ntr)$ elements in k;

- the storage of $\sigma_\lambda\rho_j(C_{\geq j})$ for each $C \in \Lambda$ requires $\mathcal{O}(n^3tr^2)$ elements in k;
- for each element $L \in \Gamma_1 \cup \Lambda$ we need to access $L(f_i)(\mathbf{0}), i = 1 \dots m$; by the techniques of Section 3, this requires $\mathcal{O}(nr\Sigma)$ pointers to the list representation of the f_i's and $\mathcal{O}(ntr\Sigma)$ elements in k;
- the cardinality of $\mathcal{B}$ is at most nr and each element is an n-tuple of integers.

The total space complexity is then $\mathcal{O}(n^3tr^2) + \mathcal{O}(ntr\Sigma)$.
Let us consider now the time complexity:

- Computing $C_{U,t}$ requires $\mathcal{O}(n^4t^2r^2)$ arithmetical operations in k and at most $\mathcal{O}(n^3t^2r^2)$ arithmetical operations in k if the ordering is lexicographical.
- Computing $\sigma_\lambda\rho_j((C_{U,t})_{\geq j})$ requires $\mathcal{O}(n^2t^2r^2)$ arithmetical operations.
- Computing $C_{U,t}(f_j)$ requires taking nr linear combinations of vectors of length Σ for $\mathcal{O}(nt^2r\Sigma)$ operations in k.
- Solving the system
$$C_{U,t}(f_j)(\mathbf{0}) = \sum_{C_{U,\tau}\in\Lambda} c_\tau C_{U,\tau}(f_j)(0), \qquad j = 1, \dots, m,$$
which has nr unknowns and m equations requires
$$\min\{\mathcal{O}(nt^2rm^2), \mathcal{O}(n^2t^2r^2m)\}$$
operations.
- Gaussian reduction of $L_{\geq j}^{(1\kappa_1)}$ w.r.t. Γ_j requires $\mathcal{O}(nt^2r^2)$ arithmetical operations.
- To update $\mathcal{B}$ one can simply store a larger set $\mathcal{B}'$, where at each update all $\rho_j(D(t))$ are inserted, remove duplicates and keep a count of the number of insertions; when the least element is removed from $\mathcal{B}'$, it is in $\mathcal{B}$ if it has been inserted as many times as the number of variables on which it explicitly depends, *cf.* also [FGLM]; updating $\mathcal{B}'$ has then a cost of $\mathcal{O}(n^2r^2)$ operations on integers.

The total complexity of the algorithm is therefore $\mathcal{O}(n^5t^2r^3) + \mathcal{O}(n^2tr^3\Sigma) + \mathcal{O}(\min\{n^3t^2r^3m, n^2t^2r^2m^2\})$.

4.4 From a Gröbner basis to differential conditions.

There is no theoretical advantage in using a Gröbner basis of $\mathcal{I}$ as input to the algorithm of section 4.3. We can however get a tighter estimate for the complexity, since we have $\Sigma = \mathcal{O}(ns^2)$ and $m = \mathcal{O}(ns)$ giving: $\mathcal{O}(n^5t^2r^3) + \mathcal{O}(n^4t^2r^2s^2) + \mathcal{O}(n^3tr^3s^3)$.

4.5 From a standard basis to differential conditions.

A marginal advantage is instead obtained if the input is a standard basis of $\mathbf{q}$ for an ordering $<$ s.t. $X_i < 1\ \forall i$. In this case in fact, let $<^{-1}$ be the inverse ordering of $<$, i.e. the ordering s.t. $\tau_1 <^{-1} \tau_2 \iff \tau_1 > \tau_2$, which is then a well-ordering. Let Γ be the Gauss basis of $\Delta(\mathbf{q})$ w.r.t. $<^{-1}$ and let $T(\Delta(\mathbf{q})) = \{T(L) : L \in \Gamma\}$ and $\mathbf{N}(\mathbf{q}) = \mathbf{N}_<(\mathbf{q})$.

Lemma 4.4. $T(\Delta(\mathbf{q})) = \mathbf{N}(\mathbf{q})$.

Proof. We have to prove that $T(\Delta(\mathbf{q})) \cap T(\mathbf{q}) = \emptyset$, since then $\mathrm{card}(T(\Delta(\mathbf{q}))) = \mathrm{card}(\mathbf{N}(\mathbf{q}))$ allows to conclude.

Recall that for $f = \sum_{\tau\in\mathbf{T}} c_\tau\tau \in \mathcal{P}_K$ and $L = \sum_{\tau\in\mathbf{T}} b_\tau D(\tau) \in \mathrm{Span}_K(\mathcal{D})$, one has $L(f)(\mathbf{0}) = \sum_{\tau\in\mathbf{T}} c_\tau b_\tau$. If now $\omega \in T(\Delta(\mathbf{q})) \cap T(\mathbf{q})$, let $f = \sum_{\tau\in\mathbf{T}} c_\tau\tau \in \mathbf{q}$ be s.t. $T(f) = \omega$ and $L = \sum_{\tau\in\mathbf{T}} b_\tau D(\tau) \in \Gamma$ be s.t. $T(L) = \omega$. Then if $\tau > \omega$,

$c_\tau = 0$ while if $\tau < \omega$, i.e. $\omega <^{-1} \tau$, $b_\tau = 0$, while $c_\omega \neq 0$, $b_\omega \neq 0$ so that $0 = L(f) = c_\omega b_\omega \neq 0$, a contradiction. □

4.6 From a Gröbner basis of a zero-dimensional ideal to a standard basis at a multiple point.

This is a particular instance of the problem of computing a standard basis for the primary component $\mathbf{q}$ at the origin of a zero-dimensional ideal $\mathcal{I}$ which is known by a dual basis $\{L_1, \dots, L_s\}$. The algorithm in [MMM] (*cf.* 4.1) can of course be adapted to this situation, but there is an important difference, which allows exponentiality in n to creep into the picture. We can avoid it by an indirect approach using the algorithms of [MMM] and of Sections 4.4 and 4.7 to pass from the dual basis to a Gröbner basis, from this to a dual basis for $\mathbf{q}$ consisting of differential conditions and from it to a standard basis, in this way a polynomial algorithm can be provided for this problem too.

The important difference is that in order to evaluate the functionals at terms, one has to process the terms so that when a term ω is processed all its divisors have been already processed; since the ordering is such that $X_i < 1\ \forall i$, then divisors of ω are *larger* than ω so that when $v(\omega)$ is processed and a relation $v(\omega) = \sum c_\tau v(\tau)$ is found where τ runs among the terms already processed, the leading term of $\omega - \sum c_\tau \tau$ is *not* ω but one of the τ's, say σ; this means in particular that multiples of σ could have been processed before ω, so that there are terms processed which are neither in $\mathbf{N}(\mathbf{q})$ nor minimal generators of $T(\mathbf{q})$.

Let us describe with some more details the resulting algorithm: terms are processed according to some ordering $\prec$ s.t. if τ divides ω then $\tau \prec \omega$; in particular therefore $\prec$ is not the ordering $<$ w.r.t. which we are computing the standard basis of $\mathbf{q}$.

When processing a term ω we know a set $\mathbf{N}$ consisting of terms τ s.t.:

1) $\tau \prec \omega$ for all $\tau \in \mathbf{N}$,
2) the set $\{v(\tau) : \tau \in \mathbf{N}\}$ is linearly independent,
3) as a consequence $\operatorname{card}(\mathbf{N}) \leq s$,
4) if $\tau \in \mathbf{N}$ then each divisor of τ is in $\mathbf{N}$,
5) if $\tau \prec \omega$, $\tau \notin \mathbf{N}$, then $\tau \in T(\mathbf{q})$.

Remark however that unlike in the MMM algorithm, it is possible that $\mathbf{N} \cap T(\mathbf{q}) \neq \emptyset$.

When ω is processed, one first computes $v(\omega) = (L_1(\omega), \dots, L_s(\omega))$ — in the case in which the functionals are L_i s.t. $\operatorname{Can}(f, \mathcal{I}) = \sum L_i(f)\tau_i$ this is done by the formula $\operatorname{Can}(X_l\sigma, \mathcal{I}) = \sum L_i(\sigma) \operatorname{Can}(X_l\tau_i, \mathcal{I})$ with σ s.t. $\omega = X_l\sigma$.

There are two cases:

- if $v(\omega)$ is linearly independent over $\{v(\tau); \tau \in \mathbf{N}\}$, then ω is added to $\mathbf{N}$,
- otherwise a linear relation $\sum_{\tau \in \mathbf{N} \cup \{\omega\}} c_\tau v(\tau)$ is found; let then
$$\sigma = \max_{\prec}\{\tau \in \mathbf{N} \cup \{\omega\} : c_\tau \neq 0\};$$
then the polynomial $f_\sigma = \sum_{\tau \in \mathbf{N} \cup \{\omega\}} c_\tau \tau$ is in $\mathbf{q}$ and $T(f_\sigma) = \sigma$; then σ and all its multiples are removed from $\mathbf{N}$.

Remark that f_σ is not necessarily an irredundant element in the standard basis of $\mathbf{q}$ and that, at termination, even irredundant elements in the standard basis could be not in the reduced form $T(f) - \operatorname{Can}(f, \mathbf{q})$ so that some postprocessing is still needed.

It consists in

- removing those basis elements whose maximal terms are not minimal generators of $T(\mathbf{q})$
- computing $\mathrm{Can}(\sigma, \mathbf{q})$ for each σ which has been processed by the algorithm and is not in $\mathbf{N}(\mathbf{q})$ and substituting it to σ in the elements of the standard basis; this can be done with an obvious adaptation of the algorithm for producing a border basis described in Section 4.2.

The same arguments as in [MMM] allow to prove that the complexity of the algorithm is $\mathcal{O}(Rr^2) + \mathcal{O}(\ell Rr)$ where R is the cardinality of the set $\mathbf{N}_\infty$ of terms processed by the algorithm and ℓ is the cost of computing $L_i(\tau)$ for a functional L_i and a term $\tau \in \mathbf{N}_\infty$, (in the case we have a border basis as input it is $\ell = r$).

We are therefore left with the problem of estimating R. Let us call *Ferrers subset* a subset $\mathbf{N}$ of $\mathbf{T}$ s.t. if $\tau \in \mathbf{N}$ then all its divisors are in $\mathbf{N}$ too and let us denote by $\mathbf{N}^{(m,n)}$ the union of all Ferrers subsets of cardinality m in n variables. Because of conditions 3), 4) above whenever ω is processed $\mathbf{N} \cup \{\omega\}$ is a Ferrers subset with at most $s+1$ elements, so that $\mathbf{N}_\infty \subseteq \mathbf{N}^{(s+1,n)}$. Let us therefore estimate the cardinality of $\mathbf{N}^{(m,n)}$.

Proposition 4.3. $\mathrm{card}(\mathbf{N}^{(m,n)}) \le m(1+\log m)^{n-1}$.

Proof. By induction on n, the number of variables in $\mathcal{P}_K$. For $n = 1$, $\mathbf{N}^{(m,1)} = \{1, X_1, \dots, X_1^{m-1}\}$ so $\mathrm{card}(\mathbf{N}^{(m,1)}) = m \le m(1+\log m)^{n-1}$.

Let us therefore assume the result proved for all m and for $n-1$. Let us denote by $\mathbf{T}_{(n-1)}$ the set of terms in $X_1, \dots, X_{n-1}$ and by $\mathbf{N}_i^{(m,n)}$ the set $\{\tau \in \mathbf{T}_{(n-1)} : X_n^i\tau \in \mathbf{N}^{(m,n)}\}$ and let us remark that:

- if $\tau \in \mathbf{N}^{(m,n)}$ then $\deg_{X_n}(\tau) < m$
- for $\tau \in \mathbf{T}_{(n-1)}$: $X_n^i\tau \in \mathbf{N}^{(m,n)} \iff \tau \in \mathbf{N}^{(\mu,n-1)}, \mu = \mu(i) = \lfloor \frac{m}{i+1} \rfloor$
- $\mathbf{N}^{(m,n)} = \{X_n^j\tau : j < m, \tau \in \mathbf{N}^{(\mu(j),n-1)}\}$.

To prove the second statement, remark that if $X_n^i\tau \in \mathbf{N}^{(m,n)}$ and $\mathbf{N}$ is a Ferrers subset containing it, then $X_n^j\omega \in \mathbf{N}$ for all $j \le i$ and ω dividing τ, so that $\{\omega : \omega|\tau\}$ is a Ferrers subset with at most μ elements, so $\tau \in \mathbf{N}^{(\mu,n-1)}$. Conversely if $\tau \in \mathbf{N}^{(\mu,n-1)}$ let $\mathbf{N}$ be a Ferrers subset with cardinality μ and containing τ, then $\{X_n^j\omega : \omega \in \mathbf{N}, j \le i\}$ is a Ferrers subset with $\mu i \le m$ elements so $X_n^i\tau \in \mathbf{N}^{(m,n)}$.

As a consequence we have:

$$\begin{aligned}\mathrm{card}(\mathbf{N}^{(m,n)}) &= \sum_{j=0}^{m-1} \mathrm{card}(\mathbf{N}^{(\mu(j),n-1)}) \le \sum_{j=0}^{m-1} \mu(j)(1+\log\mu(j))^{n-2} \\ &\le m(1+\log(m))^{n-2}\sum_{j=1}^{m}\frac{1}{j} \le m(1+\log m)^{n-2}\left(1+\int_1^m \frac{1}{t}\,dt\right) \\ &= m(1+\log m)^{n-1}. \quad \square\end{aligned}$$

We can therefore conclude that the complexity of passing from a Gröbner basis to a standard basis is $\mathcal{O}(r^2 s \log^{n-1} s)$.

4.7 From differential conditions to a standard basis.

The situation is different if one computes a standard basis w.r.t. $<$ for the primary component $\mathbf{q}$ at the origin of a zero-dimensional ideal $\mathcal{I}$ which is known by a dual basis $\{L_1, \dots, L_r\}$ and the set $\mathbf{N}(\mathbf{q})$ is already known. This happens for instance, because of Lemma 4.4., if the input is a Gauss basis of differential conditions w.r.t. the inverse ordering $<^{-1}$.

In fact in this case, one has just to compute $v(\tau)$ for $\tau \in \mathbf{N}(\mathbf{q})$ or τ a minimal generator of $T(\mathbf{q})$, and this can be done by taking the terms in increasing order w.r.t. $<^{-1}$ and then by computing the linear dependencies of the $v(\tau)$'s with τ a minimal generator of $T(\mathbf{q})$ over the set $\{v(\tau) : \tau \in \mathbf{N}(\mathbf{q})\}$.

The complexity is therefore $\mathcal{O}(nr^3)$ since in this case $R = \mathcal{O}(nr)$ and $\ell = \mathcal{O}(r)$.

4.8 From a Gröbner basis to a different Gröbner basis.

This is the problem solved in [FGLM] and is a particular case of the problem of computing a Gröbner basis of an ideal knowing a dual basis for it. The complexity is $\mathcal{O}(ns^3)$.

4.9 From a standard basis to a different standard basis.

This too is a particular case of the problem discussed in Section 4.6, so it has exponential complexity if performed directly but a polynomial one if performed indirectly.

4.10 From a Gauss basis of differential conditions to a Gauss basis for a different ordering.

Assume we are given, w.r.t. to a fixed ordering $<$, a Gauss basis of differential conditions for the ideal $\mathbf{q}$ in the representation we are using throughout the paper, i.e. we are given coefficients $c_{ji}^{(\mu\kappa)}$, $b_{\lambda i}^{(\mu\kappa)}$ s.t. denoting:

- $L^{(\mu 1)} = \mathrm{Id}\ \forall\mu$,
- $L^{(\mu\kappa)} = \sum_{j\geq\mu}\sum_{i<\kappa} c_{ji}^{(\mu\kappa)} \rho_j(L^{(ji)})$,

one has:

- $\{L^{(1\kappa)} : 1 \leq \kappa \leq r_1\}$ is a Gauss basis w.r.t. $<$ of $\Delta(\mathbf{q}) = U$,
- $\{L^{(\mu\kappa)} : 1 \leq \kappa \leq r_\mu\}$ is a Gauss basis w.r.t. $<$ of $U_\mu = \{L_{\geq\mu} : L \in U\}$,
- $\forall\mu$, $\forall\lambda > \mu$, $\forall\kappa$, $\sigma_\lambda\rho_\mu(L^{(\mu\kappa)}) = \sum_{i<\kappa} b_{\lambda i}^{(\mu\kappa)} L^{(\mu i)}$.

We want to compute a Gauss basis of $\Delta(\mathbf{q})$ w.r.t. a different ordering $<_1$, i.e. coefficients $\gamma_{ji}^{(\mu\kappa)}$, $\beta_{\lambda i}^{(\mu\kappa)}$ s.t. denoting:

- $\Lambda^{(\mu 1)} = \mathrm{Id}\ \forall\mu$,
- $\Lambda^{(\mu\kappa)} = \sum_{j\geq\mu}\sum_{i<\kappa} \gamma_{ji}^{(\mu\kappa)} \rho_j(\Lambda^{(ji)})$.

one has:

- $\{\Lambda^{(1\kappa)} : 1 \leq \kappa \leq r_1\}$ is a Gauss basis w.r.t. $<_1$ of $\Delta(\mathbf{q}) = U$,
- $\{\Lambda^{(\mu\kappa)} : 1 \leq \kappa \leq r_\mu\}$ is a Gauss basis w.r.t. $<_1$ of U_μ,
- $\forall\mu$, $\forall\lambda > \mu$, $\forall\kappa$, $\sigma_\lambda\rho_\mu(\Lambda^{(\mu\kappa)}) = \sum_{i<\kappa} \beta_{\lambda i}^{(\mu\kappa)} \Lambda^{(\mu i)}$.

The algorithm of course goes by induction on the dimension r of U, the case $r = 1$ being settled by definition; so we can assume to have already computed $\gamma_{ji}^{(\mu\kappa)}$, $\beta_{\lambda i}^{(\mu\kappa)}$ for all $\kappa < r$ and to have representations of each $\rho_j(L^{(ji)})$ in terms of the $\rho_j(\Lambda^{(ji)})$'s for $i < r$.

We now consider $L^{(\mu r)} = \sum_{j\geq\mu}\sum_{i<r} c_{ji}^{(\mu r)} \rho_j(L^{(ji)})$, we substitute to each $\rho_j(L^{(ji)})$ its representation in terms of the $\rho_j(\Lambda^{(ji)})$'s and we perform Gaussian reduction over this representation with respect to $\{\Lambda^{(\mu\kappa)} : 1 \leq \kappa \leq r\}$, obtaining:

$$L^{(\mu r)} = \sum_{\kappa} \alpha_\kappa \Lambda^{(\mu\kappa)} + \sum_{ji} \gamma_{ji}^{(\mu r)} \rho_j(\Lambda^{(ji)}).$$

We then set

$$\Lambda^{(\mu r)} = \sum_{ji} \gamma_{ji}^{(\mu r)} \rho_j(\Lambda^{(ji)})$$

and we obtain also the Gauss representation

$$\rho_\mu(L^{(\mu r)}) = \rho_\mu(\Lambda^{(\mu r)}) + \sum_\kappa \alpha_\kappa \rho_\mu(\Lambda^{(\mu\kappa)}).$$

Moreover

$$\begin{aligned}\sigma_\lambda \rho_\mu(\Lambda^{(\mu\kappa)}) &= \sigma_\lambda \rho_\mu(L^{(\mu r)}) - \sum_\kappa \alpha_\kappa \sigma_\lambda \rho_\mu(\Lambda^{(\mu\kappa)}) \\ &= \sum_{i<r} b_{\lambda i}^{(\mu r)} L^{(\mu i)} - \sum_\kappa \alpha_\kappa \sigma_\lambda \rho_\mu(\Lambda^{(\mu\kappa)}).\end{aligned}$$

Substituting in this representation Gauss representations of $L^{(\mu i)}$ and $\sigma_\lambda \rho_\mu(\Lambda^{(\mu\kappa)})$ in terms of $\Lambda^{(ji)}$ we obtain also $\beta_{\lambda i}^{(\mu r)}$.

5. Computing multiplicities

5.1 Primary decomposition.

In this last section, we want to discuss how to compute the roots of a 0-dimensional ideal $\mathcal{I} \subset \mathcal{P}$ together with their algebraic multiplicity.

In some sense, since we use in this paper "algebraic multiplicity" as a synonym for "primary", the question apparently is how to compute a primary decomposition of $\mathcal{I}$. Computing primary decompositions is settled since ten years by [GTZ]; one needs a Gröbner basis of $\mathcal{I}$ and the ability of factorizing.

In the zero-dimensional case, if the artinian structure of $\mathcal{P}/\mathcal{I}$ is known (e.g. if a Gröbner basis of $\mathcal{I}$ is known) the question boils down to computing idempotents of $\mathcal{P}/\mathcal{I}$; this can be done

- as suggested in [ABRW], by choosing a sufficiently generic $u \in \mathcal{P}/\mathcal{I}$, computing by linear algebra a "minimal" polynomial f s.t. $f(u) = 0$ in $\mathcal{P}/\mathcal{I}$, factorizing it and (again by linear algebra) dividing out $\mathcal{P}/\mathcal{I}$ by the image in $\mathcal{P}/\mathcal{I}$ of a sufficiently high power of the cofactor of each irreducible factor of f.
- or, without recourse to factorization, by reduction to the finite field case (where idempotents can be easily generated probabilistically) and then by Hensel lifting, as proposed in [GMT].

If one assumes to know a Gröbner basis of $\mathcal{I}$, then the latter procedure is probably the more effective solution. However computing a Gröbner basis is not necessarily the best method for solving a system of equations; in fact:

- the best theoretical complexity is currently achieved by an "indirect" approach due to Lakshman and Lazard [LL] which is $\mathcal{O}(d^n)$ (as opposed to $\mathcal{O}(d^{n^2})$ for a Gröbner basis computation), where d is maximum of the degrees of the generators of $\mathcal{I}$,
- alternative solution technique are provided by Macaulay and/or sparse resultants which don't preserve multiplicity,
- practical Gröbner basis algorithms for solving such as GROEBNERF in REDUCE, see the Groebner package of [H], extensively apply splittings which again don't preserve multiplicities.

5.2 Root representation and their complexity.

Therefore in this paper, we assume a different scenario: we suppose to be given a basis (not necessarily a Gröbner one) of a 0-dimensional ideal $\mathcal{I}$ and some representation of its roots, and we want to give a representation of each primary of $\mathcal{I}$, in a sense which we have to make precise. First of all we need to discuss what we mean by having "some representation" of the roots of an ideal and this just requires to summarize the discussion in section 2.

All the arithmetical models to represent roots discussed here (with the partial exception of the one in 2.5) share the same structure. A group $\mathcal{R}$ of "weakly conjugate" roots of $\mathcal{I}$ are represented by giving:

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

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
- $\pi_i : A \longrightarrow A_i$ the canonical projection
- $\psi_i : A \longrightarrow K_i$ the canonical projection
- $\phi : k[X_1, \dots, X_n] \longrightarrow A$ the morphism s.t. $\phi(X_j) = \alpha_j \ \forall i$
- $\mathbf{m}_i$ the kernel of $\psi_i \phi : k[X_1, \dots, X_n] \longrightarrow K_i$

then for all i, the following two equivalent conditions hold:

1) $\mathbf{a}_i := (\psi_i(\alpha_1), \dots, \psi_i(\alpha_n)) \in K_i^n$ is a root of $\mathcal{I}$ (so that such are its k-conjugates).
2) $\mathcal{I}$ has an $\mathbf{m}_i$-primary component $\mathbf{q}_i$.

Assigning the finite set of such groups of "weakly conjugate roots" one gets exactly all the roots of $\mathcal{I}$.

In all models we have presented except the last one, we have in fact $A_i = K_i$. For the last model, which allows nilpotent elements, we will make the following further assumption (which is realistic in view of the current solving algorithms, and which we will use to bound the complexity of arithmetical operations): denoting

- $\mathbf{q}'_i$ the kernel of $\pi_i \phi : k[X_1, \dots, X_n] \longrightarrow A_i$

then:

3) $\mathbf{q}'_i \supset \mathbf{q}_i$

i.e. we assume that any manipulation of $\mathcal{I}$ in a solving algorithm has the effect of reducing the multiplicity of roots; of course this assumption is not required in order that our algorithms work properly; it just allows to bound space and time complexity of them in terms of the structure of $\mathcal{I}$.

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 use the same notation of Section 2, so n is the number of variables, $u = \mathrm{mult}(\sqrt{\mathcal{I}})$, $s = mult(\mathcal{I})$; we have that the storage for representing all the roots of $\mathcal{I}$ is $\mathcal{O}(nu)$ for all the models except 2.6, which requires $\mathcal{O}(nu^2)$ and 2.7, which requires $\mathcal{O}(ns^2)$; storing an arithmetical expression requires $\mathcal{O}(u)$ for all the models except 2.7, which requires $\mathcal{O}(s)$; performing an arithmetical operation has a time complexity of $\mathcal{O}(u^2)$ for all the models except 2.6, which requires $\mathcal{O}(u^3)$ and 2.7, which requires $\mathcal{O}(s^3)$.

5.3 Representing roots with multiplicity.

Consistently with the arithmetical models for representing roots, our aim is to "give" the primaries in the decomposition of $\mathcal{I}$, in the following sense; we assume a set of primaries $\mathbf{q}_i$ to be given, if we give

- an artinian ring A,
- n elements $\alpha_1, \ldots, \alpha_n \in A$,
- an ideal $\mathbf{p} \subset A[X_1, \ldots, X_n]$,

s.t. using the notation from 5.2, our data satisfy conditions 1), 2), 3) and moreover:

4) $\psi_i(\mathbf{p}) \subset K_i[X_1, \ldots, X_n]$ is the primary component $\mathbf{p}_i$ of $\mathbf{q}_i K_i[X_1, \ldots, X_n]$ vanishing at $\mathbf{a}_i$ (the other components of $\mathbf{q}_i$ are obtained of course by choosing a different embedding $K_i \subset \mathbf{k}$).

We have still to explain what we mean by a representation of $\mathbf{p}$:

a) by a reduced Gröbner basis: by giving a set of polynomials, whose leading coefficient is 1 and which are a "reduced Gröbner basis" of $\mathbf{p}$. Since we are working on the polynomial ring $\mathcal{P}_A$ over the artinian algebra A, we must specify in detail what we mean by a reduced Gröbner basis. In general whatever generalization of the notion of Gröbner basis is chosen, leading coefficients of Gröbner basis elements could be zero-divisors or even nilpotents in A. Here we are assuming explicitly that this is not the case, since – as in triangular set computation – any time that such a leading coefficient occurs, a splitting will have to be performed. This of course imposes the following restriction on $\mathbf{p}$:

$$\forall \tau \in \mathbf{T}, \{lc(f) : f \in \mathbf{p}, T(f) = \tau\} = A$$

On the other side, for an ideal $\mathbf{p}$ satisfying the condition above, a reduced Gröbner basis can then be defined in the usual way as a set of polynomials G s.t.:

- $\mathbf{T}(\mathbf{p})$ is generated by $\{T(g) : g \in G\}$
- $lc(g) = 1 \ \forall g \in G$
- $\forall g \in G$, $g - T(g) = \sum a_i \tau_i$, $a_i \in A \setminus \{0\}$, $\tau_i \in \mathbf{N}(\mathbf{p})$

The point is of course that if G is the "reduced Gröbner basis" of $\mathbf{p}$, then $\psi_i(G)$ is the reduced Gröbner basis of $\mathbf{p}_i$, which is what we are interested in;

b) by a reduced standard basis: by giving a set of polynomials, whose leading coefficient is 1 and which are a "reduced standard basis" of $\mathbf{p}$; the same discussion as above of course applies; in particular if G is the "reduced standard basis" of $\mathbf{p}$, then $\psi_i(G)$ is the reduced standard basis of $\mathbf{p}_i$;

c) by differential conditions: by giving a set of differential conditions whose image under ψ_i in $\mathrm{Span}_{K_i}(\mathcal{D})$ is a Gauss basis for the closed space $\Delta(\mathbf{p}_i)$; similar remarks as above of course apply.

Notice that, since the approach of this paper is essentially "local", what we obtain is the "absolute" primary decomposition of $\mathcal{I}$, i.e. the primary decomposition of $\mathcal{I}_{\mathbf{k}}$.

Let us briefly discuss how to obtain from it the primary decomposition of $\mathcal{I}$. If we assume to compute in a classical arithmetical model (2.1, 2.2), then A is in fact a field K and $\mathbf{p} = \mathbf{p}_i$. In all the representations above $\mathbf{p}$ is in fact given by a dual basis over K, i.e. by a set of linearly independent functionals $\{L_1, \ldots, L_v\} \subset \mathrm{Hom}(\mathcal{P}_K, K)$, ($v = \mathrm{mult}(\mathbf{p})$) s.t. $\mathbf{p} = \{f \in \mathcal{P}_K : L_i(f) = 0 \ \forall i\}$; they are the differential conditions in the Gauss basis of $\Delta(\mathbf{p})$ in the third representation above and are defined by $Can(f, \mathbf{p}) = \sum L_i(f)\tau_i$, $\tau_i \in \mathbf{N}(\mathbf{p})$ in the Gröbner (standard) representation.

By choosing a k-basis $\gamma_1, \dots, \gamma_t$ of K and representing $L_i = \sum \gamma_j L_{ij}$, then $\{L_{ij} : i = 1, \dots, v, j = 1, \dots, t\} \subset \mathrm{Hom}(\mathcal{P}, k)$ is a dual basis for $\mathbf{q} = \mathbf{p} \cap \mathcal{P}$ from which the representations of $\mathbf{q}$ can be obtained as in [MMM].

Of course, the crucial point in using a weak arithmetical model is in not having to separate useless primary components which are not conjugate, but which behave as if they were so for the computations in which one is interested.

The same technique can be applied (since A is just used to model computation in different fields, the fact that we are computing over an artinian algebra and not over a field is only effective on the terminology and not on the computation), but the result is the intersection of all primaries over the roots represented by A; so it is not a true primary, but what we could call a "Duval" primary.

This preliminary discussion ended, we can now attack our problem, i.e.:

(1) given a basis of a 0-dimensional ideal $\mathcal{I}$ and a subset of its roots (in the sense above) to return (again in the sense above) the primaries of $\mathcal{I}$ corresponding to each root in the subset. Of course this will require further splittings of the input artinian algebra A, which will be governed by the arithmetical operations required by the algorithm.

5.4 Gröbner and standard basis representation.

The problem has been successfully solved by Lakshman [Lak], whose results we will summarize here.

We are given a basis $\{f_1, \dots, f_\tau\}$ of the 0-dimensional ideal $\mathcal{I}$ and we want to compute its primary component $\mathbf{q}$ at a root $\mathbf{a} \in K^n$, which we assume given in anyone of the representations discussed above, and which moreover we can assume, up to a translation, to be the origin, whose maximal ideal we denote $\mathbf{m}$ as usual.

The theoretical basis of Lakshman's algorithm is the fact that if κ is the minimum value s.t. $\mathcal{I} + \mathbf{m}^\kappa = \mathcal{I} + \mathbf{m}^{\kappa+1}$, then $\mathbf{q} = \mathcal{I} + \mathbf{m}^\kappa$. Denoting by $\mathcal{I}^{[\lambda]} = \mathcal{I} + \mathbf{m}^\lambda$, one has $\mathcal{I}^{[\lambda+1]} = \mathcal{I} + \mathbf{m}\mathcal{I}^{[\lambda]}$.

Lakshman algorithm then consists in the following iterative computation:

- let $\{g_1, \dots, g_r\}$ be a border basis of $\mathcal{I}^{[\lambda]}$; by Gaussian elimination obtain from $\mathcal{B} = \{X_i g_j : i = 1, \dots, n, j = 1 \dots, r\}$ a border basis of $\mathbf{m}\mathcal{I}^{[\lambda]}$ at a cost of $\mathcal{O}(n^4 s^3)$ computations where $s = \mathrm{mult}(\mathcal{I})$ – there are at most $n^2 s$ elements in $\mathcal{B}$ all of them being vectors of length at most ns,
- compute $f_i' = \mathrm{Can}(f_i, \mathbf{m}\mathcal{I}^{[\lambda]})\ \forall i$ at a cost of $\mathcal{O}(ns^3)$
- by Gaussian reduction obtain a border basis of $\mathcal{I}^{[\lambda+1]}$ at a cost of $n^3 s^3$,
- check whether $\mathcal{I}^{[\lambda+1]} = \mathcal{I}^{[\lambda]}$.

5.5 Dual basis representation.

It is clear that the algorithms described in Section 4.3 give in fact a solution to this problem, since they just assume the knowledge of the root of the primary and a basis of the ideal.

References

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

[D] D. Duval, *Diverses questions relatives au calcul formel avec de nombres algebriques*, These d'Etat, Grenoble (1987).

[FGLM] J. C. Faugère, P. Gianni, D. Lazard, T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, J. Symbolic Comp. **16** (1993), 329–344.

[G] A. Galligo, *A propos du Théorème de Préparation de Weierstrass*, Lecture Notes in Math **409** (1974), 543–579. MR **53:**5924

[GM] P. Gianni, T. Mora, *Algebraic solution of systems of polynomial equation using Gröbner bases*, Proc. AAECC 5, LNCS **356** (1989), 247–257. MR **91e:**13024

[GMT] P. Gianni, V. Miller, B. Trager, *Decomposition of algebras*, Proc. ISSAC'88, LNCS **358** (1989). MR **91e:**12009

[Gr] W. Gröbner, *Algebraische Geometrie II*, B. I-Hochschultaschenbücher 737/737a Bibliogr. Inst. Mannheim, 1970. MR **48:**8499

[GTZ] P. Gianni, B. Trager, G. Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, J. Symb. Comp. **6** (1988), 149–167. MR **90f:**68091

[H] A. C. Hearn, *REDUCE User's Manual*, Version 3.3, Rand Corp., 1987.

[Lak] Y. Lakshman, *A single exponential bound on the complexity of computing Gröbner bases of zero dimensional ideals*, Proc. MEGA '90, Birkhäuser, 1991, pp. 227–234. MR **92d:**13018

[LL] Y. Lakshman, D. Lazard, *On the complexity of zero-dimensional algebraic systems*, Proc. MEGA '90, Birkhäuser, 1991, pp. 217–225. MR **92d:**13017

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

[L93] D. Lazard, *Systems of algebraic equations* (*algorithms and complexity*), in D. Eisenbud, L. Robbiano, Eds., Computational Algebraic Geometry and Commutative Algebra, Cambridge, 1993, pp. 106–150. MR **94m:**14076

[hmm] H. M. Möller, *On decomposing systems of polynomial equations with finitely many solutions*, J. Appl. Algebra **4** (1993), 217–230. MR **94i:**13014

[MMM] 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. MR **94g:**13019

[MS] H. M. Möller, H. J. Stetter, *Multivariate polynomial equations with multiple zeros solved by matrix eigenproblems*, Numer. Math. **70** (1995), 311–329. CMP 95:12

[M] T. Mora, *La queste del saint Graal*, Disc. Appl. Math **33** (1991), 161–190. MR **92j:**13028

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

[ZH] A. Yu. Zharkov, Yu. A. Blinkov, *Involutive approach to solving systems of algebraic equations*, Proc. IMACS '93, 11 – 16.

(M. Marinari and T. Mora) Department of Mathematics, University of Genova, 16132, Genova, Italy

(H. M. Möller) FernUniversität, FB Mathematik, B Informatik, 5800 Hagen 1, Germany