Journal of Pure and Applied Algebra 77 (1992) 1–38
North-Holland

A computational model for algebraic power series*

Maria Emilia Alonso**
Departamento de Algebra, Facultad de Ciencias Matematicas, Universidad Complutense, 28040 Madrid, Spain

Teo Mora*** and Mario Raimondo***
Dipartimento di Matematica, Univesità di Genova, v.L.B. Alberti 4, I-16132 Genova, Italy

Communicated by M.F. Coste-Roy
Received 23 October 1989
Revised 18 October 1990

Introduction

Up to now, no computational model is known to perform effective commutative algebra for ideals in a computable ring of formal power series, while the theory for this is quite developed at least since [7].

The particular case of algebraic formal power series comes out naturally when studying singular points of algebraic varieties, for instance, in the Newton–Puiseux algorithm for determining the analytic branches of a curve at a singular point and, more generally, when studying analytic components of a complex algebraic variety.

We propose here to develop a computational model for *algebraic* formal power series, already introduced in [1], based on a symbolic codification of the series by means of the Implicit Function Theorem, i.e., we will consider algebraic series as the *unique* solutions of suitable functional equations, which we call Locally Smooth Systems. We then reduce the problem of handling a finite set of algebraic series to some corresponding problem involving suitable polynomial rings.

In this model we will show that most of the usual local commutative algebra can be effectively performed on algebraic series, since we can reduce to the polyno-

* A preliminary draft of this paper appeared as "Computing with algebraic series" in Proc. ISSAC '89 (ACM, New York, 1989).

** Partially supported by CICYT-PB860062 (Spain) and by Accion Integrada Espana–Italia.
*** Partially supported by MPI Funds (40% and 60%), by C.N.R. (progetto strategico 'Matematica Computazionale') and by Azione Integrata Italia–Spagna.

mial case, where the Tangent Cone Algorithm can be used to effectively perform local algebra. We can give a Tangent Cone Algorithm for ideals in the ring of algebraic formal power series, and so compute standard bases and use an effective version of the method of associated graded rings, to deal with basic local ideal theoretical problems. It turns out, however, that much information can be obtained in a direct way, by means of the Bezout Theorem.

The main result of our paper is an effective version of the Weierstrass Preparation Theorem: we are able to prepare a distinguished polynomial and contemporaneously reduce the involved Locally Smooth Systems to ones with one less variable. This theorem will allow us to have an effective version of the Weierstrass Division Theorem, to handle an effective elimination theory for algebraic series and to give an effective version of the Noether Normalization Lemma.

In Section 1 we recall without proofs the basic theory of standard bases in rings of formal power series. The second section is devoted to the presentation of the proposed computational model for algebraic series, based on the concept of *locally smooth systems*. In Section 3 we show how to modify a locally smooth system to effectively compute with algebraic series. In Section 4 we then give an algorithm to compute a standard basis for the ring of algebraic series (and henceforth an effective version of the method of associated graded rings). In Section 5 we give effective versions of the Weierstrass Preparation and Division Theorems, which are used in Section 6 to present algorithms for computing the elimination of variables and the Noether normal position of an ideal of algebraic formal power series. Finally we show in the Appendix how to reduce classically defined algebraic series to our model and conversely, by means of (a constructive version of) the Artin–Mazur Theorem.

We assume that the reader is familiar with the notion and basic properties of Gröbner bases for polynomial ideals [6].

1. Recalls on standard bases

Notation

We fix the following data and notation all over the paper.

Let $\{Z_1, \ldots, Z_m\}$ be a set of variables. We will use Z as a shorthand for $(Z_1, \ldots, Z_m)$ and denote by $\langle Z \rangle = \langle Z_1, \ldots, Z_m \rangle$ the multiplicative semigroup of terms in the Z_i's.

An *admissible term ordering* (of weight L) on $\langle Z \rangle$ is a semigroup total ordering such that there exists a positive linear form $L : \mathbb{N}^m \to \mathbb{N}$, $L(a) = L(a_1, \ldots, a_m) = \sum w_i a_i$, with $Z^a < Z^b$ if $L(a) < L(b)$, where $Z^a := Z_1^{a_1} \cdots Z_m^{a_m}$. We say that w_i is the weight of the variable Z_i, and, by abuse of notation, we will write $L(Z^a)$ for $L(a)$. We remark that, for each $n \in \mathbb{N}$, there are only finitely many terms Z^a with $L(Z^a) = n$.

Let K denote a field of characteristic zero. We require that the field K is computable in a very weak form: all we need is the availability of arithmetical operations in K; we will require availability of a factorization algorithm for polynomials in $K[Z]$ only in the Appendix, where it will be needed to explicitly represent in our computational model an algebraic power series given in the classical way.

Let us denote by $K[[Z]] = K[[Z_1, \ldots, Z_m]]$ the ring of formal power series. We will be specifically interested in the ring

$$K[[Z]]_{\mathrm{alg}} := \{g \in K[[Z]]\colon g \text{ is algebraic over } K[Z]\}$$

of algebraic power series. Let $f \in K[[Z]]$, we write $f = \sum_{a \in \mathbb{N}^m} f_a Z^a$, with $f_a \in K$; then let $f_{(i)} := \sum_{L(a)=i} f_a Z^a$, so that $f = \sum_{i=0}^{\infty} f_{(i)}$. In this setting we denote:

$$\mathrm{Supp}(f) := \{Z^a\colon f_a \neq 0\}\,,$$

$$T(f) := \min_< \{Z^a\colon f_a \neq 0\}, \text{ the } \textit{leading term} \text{ of } f\,,$$

$$M(f) := f_a Z^a, \text{ where } Z^a = T(f), \text{ the } \textit{leading monomial} \text{ of } f\,,$$

$$\mathrm{lc}(f) := f_a, \text{ where } Z^a = T(f), \text{ the } \textit{leading coefficient} \text{ of } f \text{ and}$$

$$\mathrm{in}(f) := f_{(i)}, \text{ where } f_{(j)} = 0\ \forall j < i, \text{ the } \textit{initial form} \text{ of } f\,.$$

Moreover, for any K-algebra R with $K[Z] \subset R \subset K[[Z]]$, we will freely use the following notation, denoting $\mathbf{m} := (Z_1, \ldots, Z_m)K[[Z]] \cap R$:

$$R_{\mathrm{loc}} = R_{1+\mathbf{m}} = \left\{ \frac{a}{1+b} \colon a, b \in R,\, b \in \mathbf{m} \right\}.$$

Standard bases and normal forms

We recall now some basic definitions and results on standard bases for the ring of formal power series and subrings of it.

Definition. Let R be any ring such that $K[Z] \subset R \subset K[[Z]]$. Let I be an ideal in R, $\{g_1, \ldots, g_s\} \subset I$. We say that:

(i) $g \in R$ has an *R-standard representation* in terms of $\{g_1, \ldots, g_s\}$ if $g \in R^*$ and $g = \sum h_i g_i$ with $T(h_i) \cdot T(g_i) \geq T(g)\ \forall i,\ h_i \in R$.

(ii) An element $h \in R$ is an *R-normal form* of g with respect to $\{g_1, \ldots, g_s\}$ if $g - h$ has an R-standard representation in terms of $\{g_1, \ldots, g_s\}$ and either $h = 0$ or $M(h) \not\in (M(g_1), \ldots, M(g_s))$. (We write: $h \in \mathrm{NF}(g, \{g_1, \ldots, g_s\}, R)$.)

Moreover, let us consider: $M(I) := (M(g)\colon g \in I) \subset K[Z]$; we say that:

(iii) $\{g_1, \ldots, g_s\}$ is an *R-standard base* for I if $\{M(g_1), \ldots, M(g_s)\}$ generates the ideal $M(I)$.

Remark. One of the main features of Gröbner bases for polynomial rings consists in the following fact, which gives an effective test for ideal membership:

Let g be a polynomial, I an ideal, $\{g_1, \ldots, g_s\}$ a Gröbner basis of I; then:

$$0 \text{ is a normal form of } g \text{ with respect to } \{g_1, \ldots, g_s\} \text{ if and only if } g \in I ,$$

$$g \text{ has a nonzero normal form with respect to } \{g_1, \ldots, g_s\} \text{ if and only if } g \notin I .$$

A similar result can be obtained also in the case of standard bases; however, without further restrictions, the two cases above are no more mutually exclusive; a third possibility occurs, namely that no normal form of g with respect to the standard basis $\{g_1, \ldots, g_s\}$ exists.

Example 1. Let $m = 1$, $Z = Z_1$, $L(Z) := 1$, $g_1 := Z - Z^2$, $g := Z$, $I := (g_1)K[Z]$. Then $\{g_1\}$ is a standard basis for I. Clearly $Z \notin (Z - Z^2)$, so there is no $K[Z]$-standard representation of g in terms of $\{g_1\}$ and 0 is not a normal form of g with respect to $\{g_1\}$. Moreover, if $h \in K[Z] - \{0\}$ is such that $Z - h \in (g_1)$, then $h(0) = 0$, so $M(h) \in (M(g_1))$; therefore, $\mathrm{NF}(g, \{g_1\}, K[Z]) = \emptyset$.

Definition. We say that the ring R has the property (NF) if, for each $\{g_1, \ldots, g_s\}$, $g \in R$, there is an R-normal form of g with respect to $\{g_1, \ldots, g_s\}$.

Proposition 1.1. *Let R be a ring satisfying* (NF), $g \in R$, $I = (g_1, \ldots, g_s)$ *and assume that* $\{g_1, \ldots, g_s\}$ *is a standard base, then*:

(i) *if* $0 \in \mathrm{NF}(g, \{g_1, \ldots, g_s\}, R)$, *then* $g \in I$; *in this case* $\mathrm{NF}(g, \{g_1, \ldots, g_s\}, R) = \{0\}$;

(ii) *if there is* $h \in \mathrm{NF}(g, \{g_1, \ldots, g_s\}, R) - \{0\}$, *then* $g \notin I$; *in this case if* $h' \in \mathrm{NF}(g, \{g_1, \ldots, g_s\}, R)$, *then* $h' \neq 0$, $M(h) = M(h')$, $T(h) = \max\{T(f) \colon g - f \in I\}$.

Proof. (i) If $0 \in \mathrm{NF}(g, \{g_1, \ldots, g_s\}, R)$, then g has an R-standard representation in terms of $\{g_1, \ldots, g_s\}$ and in particular it belongs to I. Assume there is $f \in \mathrm{NF}(g, \{g_1, \ldots, g_s\}, R)$ and $f \neq 0$, then $g - f$ has an R-standard representation in terms of $\{g_1, \ldots, g_s\}$, hence $g - f \in I$; but also $g \in I$, and thus $f \in I$. This implies $M(f) \in M(I)$, which gives a contradiction, since $M(f) \notin M(I)$ because f is a normal form.

(ii) If there is $h \in \mathrm{NF}(g, \{g_1, \ldots, g_s\}, R) - \{0\}$, then $h \notin I$, because $M(h) \notin M(I)$; since $g - h \in I$, it follows that $g \notin I$ too. By (i) then $0 \notin \mathrm{NF}(g, \{g_1, \ldots, g_s\}, R)$. So if $h' \in \mathrm{NF}(g, \{g_1, \ldots, g_s\}, R)$, then $h' \neq 0$; clearly $h - h' \in I$, and therefore, if $M(h) \neq M(h')$, assuming, e.g., $T(h) \leq T(h')$, we conclude that $M(h - h') = cM(h)$, for some nonzero constant c; hence $M(h) \in M(I)$, a contradiction. Similarly we can see that there are no f with $h - f \in I$ and $T(f) > T(h)$. $\square$

Proposition 1.2. *Let R be a ring satisfying* (NF). *Let $g_1, \ldots, g_s \in R$, $I = (g_1, \ldots, g_s)R$. Then the following conditions are equivalent*:

(a) $\{g_1, \ldots, g_s\}$ *is an R-standard basis of I*,

(b) $\forall g \in R$: $g \in I$ *iff g has an R-standard representation in terms of* $\{g_1, \ldots, g_s\}$,

(c) $\forall g \in R$: $g \in I$ *iff* $0 \in \mathrm{NF}(g, \{g_1, \ldots, g_s\}, R)$.

Proof. (a)$\Rightarrow$(c) This is a direct consequence of Proposition 1.1.

(c)$\Rightarrow$(b) If $g \in I$, then $0 \in \mathrm{NF}(g, \{g_1, \ldots, g_s\}, R)$ and so g has an R-standard representation in terms of $\{g_1, \ldots, g_s\}$. The converse implication is obvious.

(b)$\Rightarrow$(a) Let $g \in I$ and let $g = \sum h_i g_i$ be an R-standard representation. Let $I = \{i: T(h_i)T(g_i) = T(g)\}$. Then $M(g) = \sum_I M(h_i)M(g_i) \in (M(g_1), \ldots, M(g_s))$. $\square$

As a consequence of the above results, if standard bases of ideals and normal forms of elements can be effectively computed, one has an ideal membership test, based on condition (c) above.

Example 1 (continued). Since $\mathrm{NF}(g, \{g_1\}, K[Z]) = \emptyset$, $K[Z]$ does not satisfy (NF). Moreover, in $K[Z]$, $\{g_1\}$ is a standard base of the ideal $J = (g) = (g, g_1)$, without being a basis of it and $g \in J$ without having a standard representation in terms of $\{g_1\}$. In the ring $K[[Z]]$, we have that $(g) = (g, g_1) = (g_1)$ and that $\{g_1\}$ is a standard basis of it. Also $Z = (\sum_{i=0}^{\infty} Z^i)g_1$ is a $K[[Z]]$-standard representation. So g has a $K[[Z]]$-standard representation in terms of $\{g_1\}$ and $0 \in \mathrm{NF}(g, \{g_1\}, K[[Z]])$. If $h \in \mathrm{NF}(g, \{g_1\}, K[[Z]])$, $h \neq 0$, then, again, $h(0) = 0$; so $M(h) \in M(I)$, a contradiction. Therefore, $\mathrm{NF}(g, \{g_1\}, K[[Z]]) = \{0\}$. Moreover, since $\sum_{i=0}^{\infty} Z^i = 1/(1-Z) \in K[Z]_{\mathrm{loc}}$, by the same argument we have: $\mathrm{NF}(g, \{g_1\}, K[Z]_{\mathrm{loc}}) = \{0\}$ and $g = (1/(1-Z))g_1$ is a $K[Z]_{\mathrm{loc}}$-standard representation in terms of $\{g_1\}$.

The Tangent Cone Theorem

The following theorem (cf. [9]), shows that the above example can be generalized and it will be our main computational tool:

Theorem 1.3. (Tangent Cone Theorem and Algorithm).

(1) $K[Z]_{\mathrm{loc}}$ *satisfies* (NF).

(2) *In* $K[Z]_{\mathrm{loc}}$ *conditions* (a), (b), (c) *are equivalent.*

(3) *Given* $G, F_1, \ldots, F_r \in K[Z]_{\mathrm{loc}}$, *there is an algorithm which*:

(i) *computes* polynomials U, H *such that*: U *is a unit in* $K[Z]_{\mathrm{loc}}$, *i.e.*, $U = 1 + U'$ *and* $U'(0) = 0$, $U^{-1}H$ *is a* $K[Z]_{\mathrm{loc}}$-*normal form of G in terms of* $\{F_1, \ldots, F_r\}$,

(ii) *computes* polynomials $G_1, \ldots, G_s$ *such that* $\{G_1, \ldots, G_s\}$ *is a* $K[Z]_{\mathrm{loc}}$-*standard basis for* $(F_1, \ldots, F_r)$,

(iii) *decides whether* $G \in (F_1, \ldots, F_r)$. $\square$

Canonical forms

In the Hironaka classical definition of standard bases (cf. [3, 7]), they use the notion of canonical form which is stronger than the one of normal form (it has the uniqueness properties), but whose existence relies somehow on topological completeness and which has less good computational properties. A similar notion exists also in the theory of Gröbner bases for polynomial rings, where no computability problems arise.

Definition. Let R, I and $\{g_1, \ldots, g_s\}$ as above; we say that an element $h \in R$ is an *R-canonical form* of g with respect to $\{g_1, \ldots, g_s\}$ if $g - h$ has an R-standard representation in terms of $\{g_1, \ldots, g_s\}$ and either $h = 0$ or $\mathrm{Supp}(h) \cap (T(g_1), \ldots, T(g_s)) = \emptyset$.

Let us introduce also the corresponding condition for the ring R:

(Can) for each $\{g_1, \ldots, g_s\}$, $g \in R$, there is an R-canonical form of g with respect to $\{g_1, \ldots, g_s\}$.

Clearly condition (Can) is stronger than (NF), and an R-canonical form is an R-normal form too. Moreover, if R satisfies condition (Can) and $\{g_1, \ldots, g_s\}$ is a standard base of an ideal I, then it is easy to see that:

for each $g \in R$, there is a *unique* R-canonical form h of g with respect to $\{g_1, \ldots, g_s\}$ such that if $h \neq 0$, then $T(h) = \max\{T(h'): g - h' \in I\}$. (We write: $h = \mathrm{Can}(g, \{g_1, \ldots, g_s\}, R)$.)

Therefore, essentially by the same proof as in Proposition 1.2, one has the following proposition:

Proposition 1.4. *Let R be a ring satisfying* (Can). *Let* $g_1, \ldots, g_s \in R$, $I = (g_1, \ldots, g_s)$. *Then the following conditions are equivalent*:

(a) $\{g_1, \ldots, g_s\}$ *is an R-standard basis of I*,

(b) $\forall g \in R$: $g \in I$ *iff* g *has an R-standard representation in terms of* $\{g_1, \ldots, g_s\}$,

(d) $\forall g \in R$: $g \in I$ *iff* $\mathrm{Can}(g, \{g_1, \ldots, g_s\}, R) = 0$. □

In this setting, the main result is Galligo's Division Theorem (cf. [7]), which states that the ring $K[[Z]]$ satisfies the condition (Can).

In the ring $K[[Z]]_{\mathrm{alg}}$ of algebraic power series, in which we are interested, only a weaker version of Galligo's result holds: in fact, the Hironaka's Henselian Division Theorem (cf. [8], and for the genericity [7] and [3]) says that given $\{f_1, \ldots, f_s\} \subset K[[Z]]_{\mathrm{alg}}$, after a *generic* homogeneous linear change C of coordinates, each $g \in K[[Z]]_{\mathrm{alg}}$ has a $K[[Z]]_{\mathrm{alg}}$-canonical form with respect to $\{C(f_1), \ldots, C(f_s)\}$.

The following example shows that Hironaka's result cannot be improved:

Example 2 (Gaber and Kashiwara, cf. [8]). Let us consider two variables Z_1, Z_2 and let $L(Z_i) = 1\ \forall i$; let $g_1 = (Z_1 - Z_2^2)(Z_2 - Z_1^2)$ and $g = Z_1Z_2$. Then $\{g_1\}$ is a standard base for the ideals it generates in $K[[Z]]_{\text{alg}}$ and in $K[[Z]]$. The $K[[Z]]$-canonical form of g with respect to $\{g_1\}$ is $q(Z_1) + q(Z_2)$, where $q(T) = \sum_{i=0}^{\infty} (-1)^i T^{3(2^i)}$, which is not an algebraic power series. So, by the uniqueness of canonical forms with respect to a standard base in $K[[Z]]$, g does not have a $K[[Z]]_{\text{alg}}$-canonical form with respect to the standard base $\{g_1\}$. By the same argument, g does not have a $K[Z]_{\text{loc}}$-canonical form with respect to $\{g_1\}$.

On the other hand, it is clear that $\{g_1\}$ is a standard base for the ideal it generates in $K[Z]$ and in $K[Z]_{\text{loc}}$. A trivial application of the tangent cone algorithm gives: $Z_1Z_2 = g_1 + Z_1^3 + Z_2^3 - Z_1^2Z_2^2$. So $Z_1^3 + Z_2^3 - Z_1^2Z_2^2 \in \text{NF}(g, \{g_1\}, K[Z]_{\text{loc}})$. However, $Z_1^3 + Z_2^3 - Z_1^4Z_2 - Z_1Z_2^4 + Z_1^3Z_2^3$ belongs to $\text{NF}(g, \{g_1\}, K[Z]_{\text{loc}})$ too.

The notion of canonical forms has two main drawbacks:

(1) from a theoretical point of view, since (Can) implies (NF) and the converse is false, canonical forms can be used in less situations than normal forms;

(2) from a computational point of view, it is a nonconstructive notion, in the sense that, up to now, no algorithm is known which, given 'computable' $g, g_1, \ldots, g_s \in K[[Z]]$, allows to decide whether $\text{Can}(g, \{g_1, \ldots, g_s\}, K[[Z]]) = 0$, nor an algorithm to compute $K[[Z]]$-standard bases.

The notion of normal form is theoretically less satisfying, since it explicitly depends on a set $\{g_1, \ldots, g_s\}$ (unlike canonical forms which could be intrinsically defined in terms of an ideal).

However, it gives essentially the same topological information as a canonical form, namely the 'initial term of $g \bmod I$' $\max\{T(h'): g - h' \in I\}$, which is relevant in the method of associated graded rings; also it exists and can be computed in a wider setting, where canonical forms exists (and are not necessarily computable) only for an ideal in generic position.

We will therefore, in this paper, use the weaker condition (NF), and we will show that it will be enough for many purposes. However, in one specific point (the point of the Weierstrass Preparation Algorithm), we will need the full power of Galligo's theorem.

Auxiliary constructions using Buchberger reduction

(1) Although normal forms do not exist for $K[Z]$ (see Example 1), given $G_1, \ldots, G_s \in K[Z]$, if we apply Buchberger reduction (with respect to the converse of $<$) modulo $G_1, \ldots, G_s$ to a polynomial G which is *not* in $(G_1, \ldots, G_s)K[Z]_{\text{loc}}$, it terminates returning a polynomial which is a normal form of G.

(2) Moreover, if $F, F_1, \ldots, F_s$ are given polynomials in $K[Z]$, and $m \in \langle Z \rangle$ is given, it is possible to compute (by truncated Buchberger reduction as above) a

polynomial H such that $F - H$ is in the ideal generated by $\{F_1, \dots, F_s\}$ in $K[[Z]]$ and in $K[Z]_{\mathrm{loc}}$ and moreover it satisfies, for instance, one of the following conditions:

(i) either $M(H)$ is not a multiple of $M(F_i)$ $\forall i$, or $M(H) > m$,

(ii) for each $t \in \mathrm{Supp}(H)$, $t \leq m$ implies t is not a multiple of $M(F_i)$ $\forall i$,

(iii) for each $t \in \mathrm{Supp}(H)$, $L(t) \leq L(m)$ implies t is not a multiple of $M(F_i)$ $\forall i$.

2. A computational model for algebraic series: The locally smooth systems

Let as above K be a computable field, which we assume to be a subfield of the field of complex numbers, let $X = (X_1, \dots, X_n)$ a set of variables and $K[[X]]_{\mathrm{alg}}$ the algebraic closure of $K[X]$ in $K[[X]]$, which is the set of algebraic formal power series. The ring $K[[X]]_{\mathrm{alg}}$ turns out to be the henselization of the ring of polynomials with respect to the maximal ideal corresponding to the origin, and it has many interesting algebraic and analytic properties, e.g., it is a noetherian, regular, factorial, n-dimensional domain, and, on the other hand, it is an henselian ring and the Weierstrass Preparation Theorem and the Implicit Function Theorem hold for it. We refer for these properties to the book by Nagata [11].

We will describe a computational model for working in $K[[X]]_{\mathrm{alg}}$, which is a slight modification of the one introduced in [1] and is based on the Implicit Function Theorem. To do so, we will consider the elements of $K[[X]]_{\mathrm{alg}}$ as unique solutions of polynomial equations by means of the Implicit Function Theorem in the following way:

Let us consider polynomials

$$F_1, \dots, F_r \in K[X_1, \dots, X_n, Y_1, \dots, Y_r]$$

vanishing at the origin and such that the linear terms of the Jacobian of $(F_1, \dots, F_r)$ with respect to $Y_1, \dots, Y_r$ are linearly independent, i.e. if

$$F_i(X, Y_1, \dots, Y_r) = \sum_{j=1}^{r} c_{ij} Y_j + H_i(X, Y_1, \dots, Y_r)$$

with $c_{ij} \in K$, $H_i \in (X, Y^2)$, then $\det(c_{ij}) \neq 0$ (where we denote $Y := (Y_1, \dots, Y_r)$).

Under this assumption, by the Implicit Function Theorem, there are *unique* $f_1, \dots, f_r \in K[[X]]_{\mathrm{alg}}$ such that $f_j(0) = 0$ $\forall j$, and $F_i(X, f_1, \dots, f_r) = 0$ $\forall i$.

Lemma 2.1. *If $F_1, \dots, F_r$ are as above, without loss of generality we can assume that the Jacobian of the F_i's with respect to the Y_j's at the origin is a lower triangular nonsingular matrix, i.e., (c_{ij}) is a lower triangular matrix, i.e., $c_{ij} = 0$ for $i < j$.*

Proof. Applying row Gaussian elimination to the matrix (c_{ij}), one obtains an invertible matrix $D := (d_{ij})$ with entries in K such that $D\ (c_{ij}) = (l_{ij})$ is lower triangular and nonsingular. Let $F_i' := \sum_{j=1}^{r} d_{ij}F_j$. Then $F_i' = \sum_{j=1}^{r} l_{ij}Y_j + H_i'$, with $H_i' \in (X, Y^2)$ and $F_i'(X, f_1, \ldots, f_r) = 0\ \forall i$. $\square$

Definition (cf. [1]). We say that $\mathbf{F} = (F_1, \ldots, F_r)$ is a *locally smooth system* (LSS) if the Jacobian of the F_i's with respect to the Y_j's at the origin is a lower triangular nonsingular matrix.

Let $f_1, \ldots, f_r \in K[[X]]_{\text{alg}}$ be the unique solutions of $F_1 = 0, \ldots, F_r = 0$, which vanish at the origin: we also say that $(F_1, \ldots, F_r)$ is an LSS for the f_i's (or defining the f_i's; or that the f_i's are given by the LSS $(F_1, \ldots, F_r)$, etc.).

The key point of our approach is to obtain results in $K[[X]]_{\text{alg}}$ by working with suitable, and computable, extensions of $K[X]$. Given a locally smooth system $\mathbf{F} = (F_1, \ldots, F_r)$, let us consider the rings $K[X_1, \ldots, X_n, f_1, \ldots, f_r] = K[X, f_1, \ldots, f_r] =: K[X, \mathbf{F}]$ and $K[X, f_1, \ldots, f_r]_{\text{loc}} =: K[X, \mathbf{F}]_{\text{loc}}$ viewed as a subring of $K[[X]]_{\text{alg}}$.

To work in a constructive way with it, let us consider the evaluation map

$$\sigma_{\mathbf{F}} : K[X, Y_1, \ldots, Y_r] \to K[[X]] \quad \text{defined by} \quad \sigma_{\mathbf{F}}(Y_i) = f_i\,.$$

The following hold:

$$\text{(1)} \qquad \ker \sigma_{\mathbf{F}} \supset (F_1, \ldots, F_r)\,, \qquad \operatorname{Im} \sigma_{\mathbf{F}} = K[X, f_1, \ldots, f_r]\,,$$

$$\text{(2)} \qquad (\ker \sigma_{\mathbf{F}})K[X, Y_1, \ldots, Y_r]_{\text{loc}} = (F_1, \ldots, F_r)K[X, Y_1, \ldots, Y_r]_{\text{loc}}\,,$$

$$K[X, \mathbf{F}]_{\text{loc}} = K[X, f_1, \ldots, f_r]_{\text{loc}} \approx \frac{K[X, Y_1, \ldots, Y_r]_{\text{loc}}}{(F_1, \ldots, F_r)}\,.$$

Clearly $\sigma_{\mathbf{F}}$ extends uniquely to a morphism $K[X, Y_1, \ldots, Y_r]_{\text{loc}} \to K[X, f_1, \ldots, f_r]_{\text{loc}}$, which we will still denote by $\sigma_{\mathbf{F}}$. We will also write σ for $\sigma_{\mathbf{F}}$, when no confusion arises.

We propose now some results which will permit us, using only linear algebra, to compute the initial form of an algebraic power series f, and to test whether f is the zero function, or if it is a polynomial or a rational function.

Proposition 2.2. *Let* $\mathbf{F} = (F_1, \ldots, F_r)$ *be an LSS in* $K[X, Y_1, \ldots, Y_r]$ *defining the series* $f_1, \ldots, f_r \in K[[X]]_{\text{alg}}$, $d_i = \text{degree}(F_i)$ *and* $d = \prod d_i$. *Then*:

(a) *For every* i, *there exists a polynomial* $Q_i \in K[X, T]$ *with* $\deg(Q_i) \le d$ *such that* $Q_i(X, f_i(X)) = 0$.

(b) *Given* $H \in K[X, Y_1, \ldots, Y_r]$ *of degree* m, *and* $h = \sigma_{\mathbf{F}}(H)$, *there exists a polynomial* $Q \in K[X, T]$ *with* $\deg(Q) \le md$ *such that* $Q(X, h(X)) = 0$. (*Note*: $h(X) = H(X, f_1(X), \ldots, f_r(X)) \in K[X, \mathbf{F}]$.)

(c) *Let* $H \in K[X, Y_1, \ldots, Y_r]_{\text{loc}}$ *be given by* $H = H_0/(1 + H_1)$ *with* H_0 *and* H_1 *of* *degrees bounded by* m, *and* $h = \sigma_{\mathbf{F}}(H) \in K[X, \mathbf{F}]_{\mathrm{loc}}$, *then there exist a polynomial* $Q \in K[X, T]$ *with* $\deg(Q) \leq (m+1)d$ *such that* $Q(X, h(X)) = 0$.

Proof. (a) Let $Q_i \in K[X, T]$ be an irreducible polynomial with $Q_i(X, f_i(X)) = 0$ (cf. [4, Chapter 8]), and let $V \subset K^{n+r}$ denote the Zariski closure of $\{(X, f_1(X), \ldots, f_r(X))$: X belonging to a neighbourhood of the origin where the f_i's are defined$\}$. Then V is contained in $\{F_1 = \cdots = F_r = 0\}$ and by the Bezout Theorem: $\deg(V) \leq \prod \deg(F_i) = d$.

Now let $W \subset K^{n+1}$ denote the Zariski closure of $\{(X, f_i(X))$: X in a neighbourhood of the origin where f_i is defined$\}$ and $\pi_i : K^{n+r} \to K^{n+1}$ the projection given by $\pi_i(X, Y_1, \ldots, Y_r) = (X, Y_i)$. Then $W \subset \pi_i(V)$ and $\deg(W) \leq \deg(V)$. Finally, since $\{Q_i = 0\}$ is a component of W, $\deg(Q_i) \leq d$.

(b) Let $F_{r+1} := Y_{r+1} - H \in K[X, Y_1, \ldots, Y_{r+1}]$ and apply case (a) to $\mathbf{F}' = (\mathbf{F}, F_{r+1})$ and $f_{r+1} = h$.

(c) As in (b) with $F_{r+1} := (1 + H_1)Y_{r+1} - H_0$. □

Corollary 2.3. *With the notation of the proposition we have that* h *identically vanishes if and only if its Taylor development up to degree* dm *vanishes. This permits us*:

(i) *to have a test for* $h = 0$,

(ii) *to compute the initial form* $\mathrm{in}(h)$.

In particular, we have that $\deg(\mathrm{in}(f_j)) \leq d$ $\forall j$, *provided that* $f_j \neq 0$. □

The above corollary says that we can check whether we are introducing *new* algebraic series which in fact are the zero function. We propose now a test to see whether an algebraic series is a polynomial.

Proposition 2.4. *With the notation of Proposition* 2.2(b), *we have*:

$$h \in K[X] \quad \text{if and only if} \quad h_{(j)} = 0 \ \forall j\colon md < j \leq m^2 d^2 .$$

Proof. By Proposition 2.2(b) there exists an *irreducible* polynomial $Q \in K[X, T]$ with $Q(X, h(X)) = 0$ and $\deg(Q) \leq dm$.

If $h \in K[X]$, then $(T - h)$ is a factor of Q and $\deg(T - h) \leq \deg(Q) \leq dm$.

To show the converse let $h = \sum_{i=0}^{\infty} h_{(i)} = h^* + h^{**}$, where

$$h^* := \sum_{i=0}^{dm} h_{(i)} \quad \text{and} \quad h^{**} := \sum_{i=dm+1}^{\infty} h_{(i)} = \sum_{i=d^2m^2+1}^{\infty} h_{(i)} .$$

Let us write $Q(X, T) := \sum_{i=0}^{dm} q_i(X) T^i$ with $\deg(q_i) \leq dm - i$.

Now,

$$\begin{aligned} 0 &= Q(X, h(X)) = Q(X, h^*(X) + h^{**}(X)) \\ &= Q(X, h^*(X)) + h^{**}(X) g(X) \end{aligned}$$

with some series $g(X)$. It is easy to show that $\deg(Q(X, h^*(X)) \leq d^2m^2$, hence, since h^{**} has order greater than d^2m^2, we have that $Q(X, h^*(X)) = 0$. Therefore, $(T - h^*)$ divides $Q(X, T)$, which is irreducible, and so $(T - h^*) = Q(X, T)$ and $h = h^*$. □

Corollary 2.5. *Let h be as in Proposition 2.2(b), then it is possible to check whether h is a rational function.*

Proof. Let $s = \deg(Q) \leq dm$ and write

$$Q(X, T) = a_0(X)T^s + a_1(X)T^{s-1} + \cdots + a_{s-1}(X)T + a_s(X) \\ \in K[X, T].$$

Let us further consider the following polynomial $Q^* \in K[X, T]$:

$$Q^*(X, T) = T^s + a_1T^{s-1} + a_0a_2T^{s-2} + \cdots + a_0^{s-2}a_{s-1}T + a_0^{s-1}a_s \\ = T^s + \sum_{i=1}^{s} a_0^{i-1}a_iT^{s-i}.$$

Then we obtain that $\deg(Q^*) \leq s(dm - s + 1) \leq (dm + 1)^2/4$. Let us consider $u = ha_0 \in K[[X]]_{\mathrm{alg}}$. Now, if $h(X) = f(X)/g(X) \in K[X]_{\mathrm{loc}}$, it is easy to see that g is a factor of a_0 and therefore we obtain that $u(X) = (a_0(X)/g(X))f(X) \in K[X]$. It is straightforward to see that u is a root of Q^*. Conversely, suppose that u is a polynomial root of Q^* (apply Proposition 2.4), then $h = u/a_0 \in K(X) \cap K[[X]]_{\mathrm{alg}} = K[X]_{\mathrm{loc}}$. In order to apply Proposition 2.4, we need to check whether $u_{(j)} = 0$ for $(dm + 1)^2/4 \leq j \leq (dm + 1)^4/16$, this can be done using suitable linear systems (with the coefficients of a_0 as unknowns), once we know the Taylor expansion of h up to degree $(dm + 1)^4/16$ and we know that $\deg(a_0) \leq dm - s \leq dm$. □

Example 3. The example we propose now will return throughout the paper: it will give an examplification of the main algorithms of the paper.

Let us consider the curve with equation

$$X_2^6 - X_1^4 - X_1^5X_2^3 = 0$$

which has two analytically irreducible branches,

$$X_2^3 - g_1(X_1), \qquad X_2^3 - g_2(X_1),$$

where $g_1, g_2 \in K[[X_1]]_{\mathrm{alg}}$ are the solutions of $T^2 - X_1^4 - X_1^5T = 0$.

By the transformation

$$\begin{cases} X_1 = X_1 \,, \\ T = X_1^2(\pm 1 + Y_1) \,, \end{cases}$$

we obtain an LSS $\mathbf{F}' = (F_1, F_2)$,

$$\mathbf{F}' \quad \begin{cases} F_1 = 2Y_1 - X_1^3 - X_1^3 Y_1 + Y_1^2 \,, \\ F_2 = -2Y_2 + X_1^3 - X_1^3 Y_2 + Y_2^2 \,, \end{cases}$$

defining f_1 and f_2 and such that $g_i = \pm X_1^2 + X_1^2 f_i$.

We intend to perform computations in $K[X_1, g_1]$. To do this it will clearly be enough to compute in $K[X, \mathbf{F}]$ with $\mathbf{F} = (F_1)$.

Remarks 2.6. (1) The classical computational model for algebraic series consists in giving a series $f(X)$ by giving a polynomial $G(X_1, \ldots, X_n, T)$ such that $G(X_1, \ldots, X_n, f(X)) = 0$. However, since there is in general (also in case G is irreducible) more than one series vanishing at the origin and satisfying G, one must give also an algorithm to compute the Taylor expansion of f up to order d, $\forall d$.

(2) Conversely, given a locally smooth system $\mathbf{F} = (F_1, \ldots, F_r)$ defining $f_1, \ldots, f_r$, it is possible to compute the Taylor expansions of the f_i up to any degree. This can be done, for instance, by performing the derivatives of the F_j with respect to the X variables, introducing the formal partial derivatives of the 'functions' Y_i, and evaluating them at the origin (assuming $Y_i(0) = 0$ we obtain the values of $\partial^\alpha Y_i / \partial X^\alpha$ for every multi-index α).

(3) As a consequence of (2) and of Corollary 2.3 we see that the initial forms of the f_j and of h can be calculated as well by truncated Buchberger reduction (cf. auxiliary construction (2) of Section 1 (p. 7)) or by solving suitable linear systems.

(4) We can check in which factor of a polynomial a given algebraic series can vanish. Suppose we are given a reducible polynomial $G(X, T) \in K[X, T]$ and a factor $F(X, T)$ of G of degrees d and m respectively, and a series $h(X)$ such that $G(X, h(X)) = 0$; then, if the Taylor expansion of $F(X, h(X))$ vanishes up to order dm, we have that $F(X, h(X)) = 0$. In fact, take an irreducible factor G_1 of G with $G_1(X, h(X)) = 0$, if $\{F = 0\}$ and $\{G_1 = 0\}$ do not have a common component, there exists a set of linear forms H_j through the origin such that $\{F = 0\} \cap \{G_1 = 0\} \cap \{H_1 = \cdots = H_{n-2} = 0\}$ is a finite set of points with multiplicity at the origin greater than dm, in contradiction with Bezout's Theorem.

(5) In the Appendix, we will show that it is possible, in a constructive way, to reduce this situation to our model, i.e., to give an LSS defining the required f. To do this we will give a constructive version of the Artin–Mazur theorem (cf. the Appendix) which will require factorizations.

3. The approach via standard bases: Standard locally smooth systems

In this section, and in the next one, we are going to develop the theory of standard bases for the ring of algebraic series $k[[X]]_{\mathrm{alg}}$.

As above, given a locally smooth system $\mathbf{F} = (F_1, \ldots, F_r)$, defining the series $f_1, \ldots, f_r$ we will consider the ring $K[X, \mathbf{F}]_{\mathrm{loc}} = K[X, f_1, \ldots, f_r]_{\mathrm{loc}}$ viewed as a subring of $K[[X]]_{\mathrm{alg}}$, and we will work with it in a constructive way by using the evaluation map $\sigma_{\mathbf{F}}$ defined by $\sigma_{\mathbf{F}}(Y_i) = f_i$ (cf. Section 2).

Let $\langle X \rangle = \langle X_1, \ldots, X_n \rangle$ denote the multiplicative semigroup of terms in the X_j's, and let $<$ be an admissible term ordering on $\langle X \rangle$, which we will suppose to be fixed for this and the next section.

In our model we introduce to represent the f_i's a set of new variables $Y_1, \ldots, Y_r$ and consider the following diagram:

$$\begin{tikzcd} K[X, Y]_{\mathrm{loc}} \arrow[r, "\sigma"] \arrow[d] & K[[X]]_{\mathrm{alg}} \arrow[d, phantom, "\cup"] \\ \dfrac{K[X, Y]_{\mathrm{loc}}}{(F)} \arrow[r, phantom, "\cong"] & K[X, \mathbf{F}]_{\mathrm{loc}} \end{tikzcd}$$

and we work in $K[X, Y]_{\mathrm{loc}}$. We will, henceforth, extend the given term-ordering on $\langle X \rangle$ to suitable ones on $\langle X, Y \rangle = \langle X_1, \ldots, X_n, Y_1, \ldots, Y_r \rangle$.

We will introduce two different such extensions: $<_{\mathrm{u}}$ and $<_{\sigma}$.

The second one, denoted $<_{\sigma}$ and called the natural one (or the σ-extension), will be a term ordering compatible with the above diagram, in the sense that the weights of the Y_i's are equal to the weight of the initial form of the f_i's ($= \sigma(Y_i)$), and it can be defined whence we know such initial forms. Let us note that this could be done at once by means of the results of Section 2 (Corollary 2.3), but we prefer to introduce it in next section.

The term ordering $<_{\mathrm{u}}$ (called uniform) can be introduced without any further knowledge on the f_i's but the locally smooth system $\mathbf{F}$ defining them. We will show that this ordering will provide enough information, e.g., in order to give standard representations, standard bases etc. in $K[X, \mathbf{F}]_{\mathrm{loc}}$, moreover, by means of it, it is possible to construct the σ-extension $<_{\sigma}$.

Lemma 3.1. Let $\mathbf{F} = (F_1, \ldots, F_r)$ *be an LSS and let* $<$ *be any admissible term ordering of weight* L *on* $\langle X_1, \ldots, X_n, Y_1, \ldots, Y_r \rangle$ *such that*:

(1) $L(Y_i) = 1 \ \forall i$,

(2) $Y_1 > \cdots > Y_r$,

(3) $\forall m \in \langle X \rangle$, $\forall m' \in \langle X, Y \rangle$, *if* $L(m) = L(m')$ *and* $m < m'$, *then* $m' \in \langle X \rangle$.

Then $\{F_1, \ldots, F_r\}$ *is a standard base with respect to* $<$ *in* $K[X, Y_1, \ldots, Y_r]_{\mathrm{loc}}$ *for the ideal it generates and* $M(F_1, \ldots, F_r) = (M(F_1), \ldots, M(F_r)) = (Y_1, \ldots, Y_r)$.

Proof. If $(F_1, \ldots, F_r)$ is a locally smooth system, then clearly $T(F_i) = Y_i$, and therefore, since $T(F_i)$ and $T(F_j)$ are relatively prime, by the Buchberger criterion [5], $\{F_1, \ldots, F_r\}$ is a standard base for the ideal it generates. □

Definition. A term ordering on $\langle X, Y\rangle$ satisfying the assumptions of the lemma will be called a *uniform term-ordering* on $\langle X, Y\rangle$.

The restriction to $\langle X\rangle$ of such a term ordering on $\langle X, Y\rangle$ is clearly admissible. Conversely, let $<$ be an admissible term ordering on $\langle X\rangle$, then there are uniform term-orderings $<_{\mathrm{u}}$ on $\langle X, Y\rangle$ whose restriction to the terms in $K[X]$ is the given $<$.

We are going to show the existence of uniform term-ordering by constructing a particular one, which will (essentially) depend only on the ordered set of variables Y_j's appearing in the LSS.

Construction. To give explicitly such an extension, we fix arbitrarily any admissible term ordering $<_Y$ on $\langle Y\rangle$ with: $Y_1 > \cdots > Y_r$ and the weight $L(Y_j) := 1$ $\forall j$. We then extend the weight function L by imposing $L_{\mathrm{u}}(X_i) := L(X_i)$ $\forall i$, and $L_{\mathrm{u}}(Y_j) := 1$ $\forall j$. Then, for $m_X, m'_X \in \langle X\rangle$, $m_Y, m'_Y \in \langle Y\rangle$, we define $m_X m_Y <_{\mathrm{u}} m'_X m'_Y$ if

$$
\begin{aligned}
& L_{\mathrm{u}}(m_X m_Y) < L_{\mathrm{u}}(m'_X m'_Y) \\
\text{or} \quad & (L_{\mathrm{u}}(m_X m_Y) = L_{\mathrm{u}}(m'_X m'_Y) \text{ and } m_X < m'_X) \\
\text{or} \quad & (L_{\mathrm{u}}(m_X m_Y) = L_{\mathrm{u}}(m'_X m'_Y)\,,\ m_X = m'_X \text{ and } m_Y <_Y m'_Y)\,.
\end{aligned}
$$

Definition. We call $<_{\mathrm{u}}$ the *uniform extension* of $<$ (constructed over $<_Y$).

Notation. We fix, for the rest of this section, an LSS $\mathbf{F} = (F_1, \ldots, F_r)$ defining $\{f_1, \ldots, f_r\}$, an admissible term ordering $<$ on $\langle X\rangle$ and a uniform extension $<_{\mathrm{u}}$. Then $T_{\mathrm{u}}(H)$, $M_{\mathrm{u}}(H)$, $\mathrm{in}_{\mathrm{u}}(H)$ will denote the leading term, the leading monomial and the initial form of $H \in K[[X, Y]]$ with respect to $<_{\mathrm{u}}$, while $T(H)$, $M(H)$ and $\mathrm{in}(H)$ will denote the corresponding ones of $H \in K[[X]]$ with respect to $<$.

Lemma 3.2. *Let* $G \in K[X, Y_1, \ldots, Y_r]_{\mathrm{loc}}$, *then it is possible to compute* U, G_0 *in* $K[X, Y]$ *such that*

U is a unit in $K[X, Y]_{\mathrm{loc}}$, with $U(0) = 1$,

$\sigma(G_0) = \sigma(U)\sigma(G)$,

either $G_0 = 0$ (in which case $\sigma(G) = 0$) or $M_{\mathrm{u}}(G_0) \in K[X]$ and $M_{\mathrm{u}}(G_0) = M(\sigma(G))$.

Proof. Notice first that we may assume $G \in K[X, Y_1, \ldots, Y_r]$. Then, by the Tangent Cone Algorithm we can compute U, G_0 in $K[X, Y]$ such that U is a unit and $U^{-1}G_0$ is a $K[X, Y_1, \dots, Y_r]_{\mathrm{loc}}$-normal form of G in terms of $\{F_1, \dots, F_r\}$, with respect to $<_{\mathrm{u}}$.

This in particular implies

$$G - U^{-1}G_0 \in (F_1, \dots, F_r)K[X, Y]_{\mathrm{loc}}\,, \quad \text{i.e.,}\ \sigma(G) = \sigma(U^{-1})\sigma(G_0)$$

and

$$\text{if } G_0 \neq 0\,, \quad \text{then } M_{\mathrm{u}}(G_0) \not\in (M_{\mathrm{u}}(F_1), \dots, M_{\mathrm{u}}(F_r)) = (Y_1, \dots, Y_r)\,,$$

so that $M_{\mathrm{u}}(G_0) \in K[X]$, which implies $M_{\mathrm{u}}(G_0) = M(\sigma(G))$. □

Proposition 3.3. *Let* $G_i, U_i \in K[X, Y]$, U_i *units in* $K[X, Y]_{\mathrm{loc}}$ *with* $U_i = 1 + U_i'$, *such that* $U_i^{-1}G_i$ *is a* $K[X, Y_1, \dots, Y_r]_{\mathrm{loc}}$*-normal form of* Y_i *in terms of* $\{F_1, \dots, F_r\}$, *with respect to* $<_{\mathrm{u}}$.
Let $F_i' := (1 + U_i')Y_i - G_i$. *Then*:

(1) $\mathbf{F}' = (F_1', \dots, F_r')$ *is an LSS for the functions* $f_1, \dots, f_r$.

(2) $f_i = 0$ *iff* $G_i = 0$.

(3) *If* $G_i \neq 0$, *then* $F_i' = Y_i(1 + Q_i) - R_i$ *with* $Q_i, R_i \in (X, Y)$, $R_i \in K[X, Y_1, \dots, Y_{i-1}, Y_{i+1}, \dots, Y_r]$ *and* $M_{\mathrm{u}}(R_i) = M(f_i) \in K[X]$.

(4) $\{F_1', \dots, F_r'\}$ *is a standard base for the ideal it generates in* $K[X, Y]_{\mathrm{loc}}$ *for* $<_{\mathrm{u}}$.

Moreover,

(a) *it is possible to decide whether some* $f_i = 0$,

(b) *if* $f_i \neq 0$, *we have* $\mathrm{in}(f_i) = \mathrm{in}_{\mathrm{u}}(R_i)$, *and therefore it is possible to compute* $M(f_i)$, $T(f_i)$ *and* $\mathrm{in}(f_i)$.

Proof. (1) $F_i' \in (F_1, \dots, F_r)K[X, Y]_{\mathrm{loc}} = \mathrm{Ker}(\sigma)$, so $F_i'(X, f_1, \dots, f_r) = 0$. Since $G_i = 0$ or, by Lemma 3.2, $T(\sigma(G_i)) = T_{\mathrm{u}}(G_i) > Y_i$, one has that $G_i \in (X, Y)$ and $Y_j \not\in \mathrm{Supp}(G_i)$ for $j > i$, so $F_i' = Y_i - \sum c_{ij}Y_j + S_i$ with $c_{ij} \in K$, $c_{ij} = 0$ if $j > i$, $S_i \in (X, Y^2)$.

(2) If $f_i = 0$, $Y_i \in \mathrm{Ker}(\sigma) = (F_1, \dots, F_r)K[X, Y]_{\mathrm{loc}}$, so its normal form is 0. Conversely, if $G_i = 0$, then $Y_i \in (F_1, \dots, F_r)K[X, Y]_{\mathrm{loc}} = \mathrm{Ker}\ (\sigma)$, so $f_i = 0$.

(3) We can write $G_i = -Y_iQ_i' + R_i$ with $R_i \in K[X, Y_1, \dots, Y_{i-1}, Y_{i+1}, \dots, Y_r]$ and $Q_i = U_i' + Q_i'$. Since $T_{\mathrm{u}}(G_i) > Y_i$, we have that $Q_i, R_i \in (X, Y)$. Since $T_{\mathrm{u}}(G_i) \in K[X]$, then $R_i \neq 0$, and $M_{\mathrm{u}}(R_i) = M_{\mathrm{u}}(G_i) = M(\sigma(Y_i)) = M(f_i)$ by Lemma 3.2.

(4) Since $<_{\mathrm{u}}$ is a uniform term ordering, the thesis follows by Lemma 3.1.

Finally, claim (a) is a direct consequence of (1), (2) and (3). As for (b), notice that, for any $H \in K[X, Y]$, we have that if $T_{\mathrm{u}}(H) \in \langle X \rangle$, then $\mathrm{in}_{\mathrm{u}}(H) \in K[X]$ (because a uniform term ordering satisfies condition (3) of Lemma 3.1) and, therefore, $\mathrm{in}_{\mathrm{u}}(H) = \mathrm{in}(\sigma(H))$. So $\mathrm{in}(f_i) = \mathrm{in}_{\mathrm{u}}(R_i)$. □

The above theorem shows how to write an algorithm to compute initial forms which is based on normal form algorithm for local rings. It is an alternative versus the direct methods described in Corollary 2.3, moreover, it will permit the further development of next sections.

Definition. We say that $\mathbf{F}$ is a *standard locally smooth system* (SLSS) with respect to an admissible term ordering $<$ on $\langle X, Y\rangle$ if:

(1) $\mathbf{F} = (F_1, \ldots, F_r)$ is an LSS for the functions $f_1, \ldots, f_r$,

(2) $f_i \neq 0\ \forall i$,

(3) $F_i = Y_i(1 + Q_i) - R_i$ with $Q_i, R_i \in (X, Y)$, $R_i \in K[X, Y_1, \ldots, Y_{i-1}, Y_{i+1}, \ldots, Y_r]$ and $M(R_i) = M(f_i) \in K[X]$,

(4) $\{F_1, \ldots, F_r\}$ is a standard basis for the ideal it generates in $K[X, Y]_{\mathrm{loc}}$ for $<$.

Proposition 3.4. *With the notations and hypotheses of Proposition* 3.3, *the set* $\{F_i' : f_i \neq 0\}$ *is an SLSS for* $\{f_i : f_i \neq 0\}$ *with respect to* $<_{\mathrm{u}}$.

Proof. By Proposition 3.3 and the above definition, we have just to remark that if $(F_1, \ldots, F_r)$ is a local smooth system for $f_1, \ldots, f_r$, $f_i = 0$, and $G_j \in K[X, Y_1, \ldots, Y_{i-1}, Y_{i+1}, \ldots, Y_r]$ denotes the evaluation of F_j at $Y_i = 0$, then $(G_1, \ldots, G_{i-1}, G_{i+1}, \ldots, G_r)$ is a local smooth system for $f_1, \ldots, f_{i-1}, f_{i+1}, \ldots, f_r$. $\square$

Example 3 (continued). We impose on $\langle X\rangle = \langle X_1, X_2, X_3\rangle$ the deg-rev-lex ordering with $X_1 < X_2 < X_3$ so that $L(X_i) = 1\ \forall i$. Then $K[X, \mathbf{F}]_{\mathrm{loc}} = K[X, Y_1]_{\mathrm{loc}}/(F_1)$, $f_1 = \sigma(Y_1)$, $g_1 = \sigma(X_1^2 + X_1^2 Y_1)$.

Now $G_1 = X_1^2 + X_1^2 Y_1$ is a normal form of itself; X_1^3 is a normal form of $Y_1(2 + Y_1 - X_1^3)$ in terms of (F_1); $X_1^2 = M_{\mathrm{u}}(G_1) = M(g_1)$; $X_1^3 = M(f_1)$, and $\mathbf{F}$ is an SLSS.

4. Standard bases in $K[[X]]_{\mathrm{alg}}$

The aim of this section is to show that $K[[X]]_{\mathrm{alg}}$ satisfies (NF) and that the Tangent Cone Algorithm for $K[X, Y]_{\mathrm{loc}}$ can be used to compute normal forms and standard bases in $K[[X]]_{\mathrm{alg}}$ for any ideal, if the input data are algebraic series in $K[X, \mathbf{F}]_{\mathrm{loc}}$ for an LSS $\mathbf{F}$.

Notation. Through this section, let $f_1, \ldots, f_r \in K[[X]]_{\mathrm{alg}}$ be given by a local smooth system $(F_1, \ldots, F_r)$ and let $<$ be an admissible term ordering on $\langle X\rangle$, and $<_{\mathrm{u}}$ an uniform extension.

As a consequence of Proposition 3.4 we may assume that $f_i \neq 0$ for each i, that $(F_1, \ldots, F_r)$ is an SLSS for the f_i's with respect to $<_{\mathrm{u}}$ and that $m_i := T(f_i)$ is known, $\forall i$.

Let $K[X, \mathbf{F}]_{\text{loc}}$ and $\sigma : K[X, Y_1, \dots, Y_r]_{\text{loc}} \to K[[X]]$ as in Section 3; let σ^* be the semigroup morphism $\langle X, Y\rangle \to \langle X\rangle$ defined in a natural way by the evaluation $\sigma : \sigma^*(Y_j) = m_j = T(f_j)$, $\sigma^*(X_i) = X_i$. We are going to construct a term-ordering extension $<_\sigma$ on $\langle X, Y\rangle$, which is compatible with the morphism σ^*.

Let us fix any admissible term ordering $<_Y$ on $\langle Y\rangle$ with $Y_1 > \cdots > Y_r$.

For $m_X, m'_X \in \langle X\rangle$, $m_Y, m'_Y \in \langle Y\rangle$, we then define: $m_X m_Y <_\sigma m'_X m'_Y$ iff

$$\begin{aligned} & m_X\sigma^*(m_Y) < m'_X\sigma^*(m'_Y) \\ \text{or}\quad & (m_X\sigma^*(m_Y) = m'_X\sigma^*(m'_Y) \text{ and } m_X < m'_X) \\ \text{or}\quad & (m_X\sigma^*(m_Y) = m'_X\sigma^*(m'_Y) \text{ and } m_X = m'_X \text{ and } m_Y <_Y m'_Y)\,. \end{aligned}$$

We remark that $<_\sigma$ has weight L_σ with $L_\sigma(X_i) = L(X_i)$ and $L_\sigma(Y_j) = L(m_j)$.

Definition. We call $<_\sigma$ the *σ-extension* (or the natural extension) of $<$ (constructed over $<_Y$); it is an admissible term ordering on $\langle X, Y\rangle$ such that

(1) its restriction to $\langle X\rangle$ is $<$,
(2) if $\sigma^*(m) < \sigma^*(m')$, then $m <_\sigma m'$,
(3) if $\sigma^*(m) = \sigma^*(m')$, and $m \neq m'$ with $m' \in \langle X\rangle$, then $m <_\sigma m'$,
(4) if $\sigma^*(Y_i) = \sigma^*(Y_j)$, $i > j$, then $Y_i > Y_j$.

We notice that, as required, the ordering $<_\sigma$ induces the given term ordering $<$ on the monomials of $K[X, \mathbf{F}]$ in a natural way by means of the mapping

$$\sigma : K[X, Y]_{\text{loc}} \to \frac{K[X, Y]_{\text{loc}}}{(F)} \cong K[X, \mathbf{F}]_{\text{loc}}\,.$$

It will play an essential role in computing (local) normal forms and standard bases.

We also remark that to construct it we only need to know the $T(f_i)$'s and so we could either use the previously introduced uniform ordering $<_{\text{u}}$, or, as well, other methods to compute initial forms.

Let $<_\sigma$ be the ordering defined above and $<_{\text{u}}$ the uniform extension of $<$ (both constructed over the same ordering $<_Y$ on $\langle Y\rangle$). $T_{\text{u}}(F)$, $M_{\text{u}}(F)$, $T_\sigma(F)$, $M_\sigma(F)$, $\text{in}_{\text{u}}(F)$ and $\text{in}_\sigma(F)$ will then denote the leading term, the leading monomial and the initial form of $F \in K[[X, Y]]$ with respect to $<_{\text{u}}$ and $<_\sigma$ respectively.

Lemma 4.1. *Let $G \in K[X, Y]_{\text{loc}}$, $H \in K[X, Y]_{\text{loc}}$ be a normal form of G with respect to $(F_1, \dots, F_r)$ for $<_{\text{u}}$. Then if $\sigma(G) \neq 0$, $M(\sigma(G)) = M_\sigma(H)$.*

Proof. We are claiming, because of Lemma 3.2, that $m' := M_\sigma(H) = M_u(H) =: m$. Clearly $m \leq_{\text{u}} m'$, so $L_{\text{u}}(m) \leq L_{\text{u}}(m')$. Also, $m' \leq_\sigma m$ by definition; then $L_\sigma(m') \leq L_\sigma(m)$. Since $L_{\text{u}}(X_i) = L(X_i) = L_\sigma(X_i)$ $\forall i$, while $L_{\text{u}}(Y_j) = 1 \leq L_\sigma(Y_j)$ $\forall j$, necessarily $L_{\text{u}}(m') \leq L_\sigma(m') \leq L_\sigma(m) = L_{\text{u}}(m)$ (using that $m \in \langle X\rangle$), so that $L_{\text{u}}(m') = L_{\text{u}}(m)$. Then since $m \leq_{\text{u}} m'$ and $m \in \langle X\rangle$, by Lemma 3.1,

$m' \in \langle X \rangle$ too. Since both $<_u$ and $<_\sigma$ restrict to $<$ on $\langle X \rangle$, we obtain $m = m'$. $\square$

Corollary 4.2. *$(F_1, \ldots, F_r)$ is an SLSS for the f_i's with respect to $<_\sigma$.*

Proof. We only have to check conditions (3) and (4) of the definition. Following the notations of the definition of SLSS, by Lemma 4.1 we have that $M_\sigma(R_i) = M_u(R_i) = M(f_i)$, since R_i is a normal form of $Y_i(1 + Q_i)$. Since $Q_i \in (X, Y)$, $1 <_\sigma T_\sigma(Q_i)$; now we observe that $\sigma^*(Y_i) = T(f_i) = T_\sigma(R_i) = \sigma^*(T_\sigma(R_i))$ and that $T_\sigma(R_i) \in \langle X \rangle$, then $Y_i <_\sigma T_\sigma(R_i)$, so $T_\sigma(F_i) = Y_i$. Hence $\{F_1, \ldots, F_r\}$ is a standard base for $<_\sigma$ by the Buchberger criterion. $\square$

Definition. Let $g \in K[X, \mathbf{F}]_{\mathrm{loc}}$ and let $G \in K[X, Y]_{\mathrm{loc}}$ be such that $g = \sigma(G)$. We say that an element $H \in K[X, Y]_{\mathrm{loc}}$ is a *representation* of g if it is a normal form of G with respect to $(F_1, \ldots, F_r)$ for $<_\sigma$.

Let us remark that the representations of g, while they are not unique (since normal forms are not so), do not depend on the choice of G in the sense that the *set* of normal forms depends only on its class modulo σ, i.e. only on the algebraic power series g.

Notice further that if $M_\sigma(G) \in K[X]$, then G is a representation of g.

Moreover, for every $H \in K[X, Y]$ we have $T_\sigma(H) \leq T(\sigma(H))$ in the ordering $<_\sigma$.

Proposition 4.3. *Let $G \in K[X, Y]_{\mathrm{loc}}$, $g := \sigma(G)$, and let H be a representation of g, then:*

(i) $H = 0$ if and only if $g = 0$,

(ii) if $H \neq 0$, then $\sigma(H) = g$, $M_\sigma(H) \in K[X]$, and $M_\sigma(H) = M(g)$.

Moreover, representations can be computed and the initial form of g, $\mathrm{in}(g)$ can also be computed.

Proof. (i) is obvious. As for (ii) note that $(F_1, \ldots, F_r)$ is a standard basis for $\mathrm{Ker}(\sigma)$, so $G - H \in \mathrm{Ker}(\sigma)$ and $M_\sigma(H) \not\in (Y_1, \ldots, Y_r)$. Therefore, $\sigma(H) = \sigma(G) = g$ and $M_\sigma(H) = M(g)$.

As for the computability statements: by the Tangent Cone Algorithm on $K[X, Y]_{\mathrm{loc}}$ it is possible to compute a normal form H of G with respect to $(F_1, \ldots, F_r)$ for $<_\sigma$ which is a representation of g. For the computability of $\mathrm{in}(g)$, we cannot apply directly the proof of Proposition 3.3, since with respect to $<_\sigma$ there could be terms $m \in \langle X \rangle$, $m' \in \langle Y \rangle$ such that $L_\sigma(m) = L_\sigma(m')$, $m < m'$. Let $H', U' \in K[X, Y]$, $U' \in (X, Y)$ be such that $H = (1 + U')^{-1}H'$. By truncated Buchberger reduction of H' with respect to $(F_1, \ldots, F_r)$ (cf. auxiliary construction of Section 1 (p. 8)), we can compute $H'' \in K[X, Y]$ such that $\sigma(H') = \sigma(H'')$ and for each $t \in \mathrm{Supp}(H'')$, $L_\sigma(t) \leq L_\sigma(T(g))$ implies that $t \in \langle X \rangle$. Then $(1 + U')^{-1}H''$ is a normal form of G, $\mathrm{in}(g) = \mathrm{in}_\sigma((1 + U')^{-1}H'') = \mathrm{in}_\sigma(H'')$. $\square$

Proposition 4.4. *There is an algorithm which, given $g_0, g_1, \ldots, g_s \in K[X, \mathbf{F}]_{\mathrm{loc}}$, returns an $H \in K[X, Y]_{\mathrm{loc}}$ such that $\sigma(H) \in \mathrm{NF}(g_0, \{g_1, \ldots, g_s\}, K[X, \mathbf{F}]_{\mathrm{loc}})$ with respect to $<$.*

Proof. Let G_i be a representation of g_i $\forall i$. We distinguish two cases.

If $M(G_0) \notin (M_\sigma(G)_1), \ldots, M_\sigma(G_s))$, then $M_\sigma(G_0) = M(g_0) \notin (M(g_1), \ldots, M(g_s))$, so that $g_0 = \sigma(G_0)$ is a normal form of itself and we set $H = G_0$.

Otherwise, if $M(G_0) \in (M_\sigma(G_1), \ldots, M_\sigma(G_s))$, by the Tangent Cone Algorithm, let $H \in K[X, Y]_{\mathrm{loc}}$ be such that $H \in \mathrm{NF}(G_0, \{G_1, \ldots, G_s, F_1, \ldots, F_r\}, K[X, Y]_{\mathrm{loc}})$ with respect to $<_\sigma$. Then either $H = 0$ or $M_\sigma(H) \notin (Y_1, \ldots, Y_r, M_\sigma(G_1), \ldots, M_\sigma(G_s))$. Let $G_0 - H = \sum H_i G_i + \sum B_j F_j$ be a standard representation. Since $M_\sigma(G_0), M_\sigma(H) \in K[X]$, $M_\sigma(H) \notin (Y_1, \ldots, Y_r, M_\sigma(G_1), \ldots, M_\sigma(G_s))$ and $T_\sigma(G_0 - H) \leq T_\sigma(H_i G_i)$, we have that $T_\sigma(H) > T_\sigma(G_0)$. Hence $M_\sigma(G_0 - H) \in K[X]$ and $T(g_0 - \sigma(H)) = T_\sigma(G_0 - H) \leq T_\sigma(H_i G_i) \leq T(\sigma(H_i))T(g_i)$. Then $g_0 - \sigma(H) = \sum \sigma(H_i) g_i$ is a standard representation of $g_0 - \sigma(H)$ in terms of $\{g_1, \ldots, g_s\}$. $\square$

Proposition 4.5. *Let $g_1, \ldots, g_s \in K[X, \mathbf{F}]_{\mathrm{loc}}$ and let $G_1, \ldots, G_s \in K[X, Y]_{\mathrm{loc}}$ be a set of corresponding representatives.*

Let moreover $I = (g_1, \ldots, g_s)K[X, \mathbf{F}]_{\mathrm{loc}}$ and $J = \sigma^{-1}(I) = (G_1, \ldots, G_s, F_1, \ldots, F_r)K[X, Y]_{\mathrm{loc}}$. Then:

(1) *It is possible to compute a standard basis of I with respect to $<$.*

(2) *$\{G_1, \ldots, G_s, F_1, \ldots, F_r\}$ is a standard basis for J with respect to $<_\sigma$ if and only if $\{g_1, \ldots, g_s\}$ is a standard basis for I with respect to $<$.*

(3) *Given $g \in K[X, \mathbf{F}]_{\mathrm{loc}}$, it is possible to compute $H \in K[X, Y]$ such that H represents $\sigma(H)$ and $\sigma(H)$ is a normal form of g with respect to $\{g_1, \ldots, g_s\}$ in $K[X, \mathbf{F}]_{\mathrm{loc}}$.*

Proof. (1) We show that it is possible to compute $H_1, \ldots, H_t \in K[X, Y]$ such that H_i represents $h_i := \sigma(H_i)$ $\forall i$, and $\{H_1, \ldots, H_t, F_1, \ldots, F_r\}$ is a standard basis of J in $K[X, Y]_{\mathrm{loc}}$. Then $\{h_1, \ldots, h_t\}$ is a standard basis of I in $K[X, \mathbf{F}]_{\mathrm{loc}}$ with respect to $<$. (In fact: let $g \in I$, $g \neq 0$, G a representation of g. Then $G \in J$ and $T_\sigma(G) \in \langle X \rangle$. So there is H_i such that $M(h_i) = M_\sigma(H_i)$ divides $M_\sigma(G) = M(g)$.

Let $\mathbf{P} := \{P_1, \ldots, P_v\}$ be a standard basis of J in $K[X, Y]_{\mathrm{loc}}$, which can be computed by the Tangent Cone Algorithm. Let $\mathbf{Q} := \{P_i \in \mathbf{P}\colon T_\sigma(P_i) \in \langle X \rangle\}$. Then for each $P_i \in \mathbf{Q}$, P_i is a representation of $\sigma(P_i)$. Moreover, $\mathbf{Q} \cup \{F_1, \ldots, F_r\}$ is a standard basis for J. In fact, if $G \in J$, either $M_\sigma(G) \in (Y_1, \ldots, Y_r) = (M_\sigma(F_1), \ldots, M_\sigma(F_r))$, or $T_\sigma(G) \in \langle X \rangle$. In the latter case there is $P_i \in \mathbf{P}$, such that $M_\sigma(P_i)$ divides $M_\sigma(G)$; but then $T_\sigma(P_i) \in \langle X \rangle$ and $P_i \in \mathbf{Q}$.

(2) By the proof of (1) we are left to prove that if $\{g_1, \ldots, g_s\}$ is a standard basis for I in $K[X, \mathbf{F}]_{\mathrm{loc}}$ with respect to $<$, then $\{G_1, \ldots, G_s, F_1, \ldots, F_r\}$ is a standard basis for J in $K[X, Y]_{\mathrm{loc}}$. For this, let $H \in J$. If $M_\sigma(H) \notin K[X]$, then

$M_\sigma(H) \in (Y_1, \ldots, Y_r) = (M_\sigma(F_1), \ldots, M_\sigma(F_r))$. Otherwise, if $h := \sigma(H) \in I$, $M_\sigma(H) = M(h) \in (M(g_1), \ldots, M(g_s)) \subset (M_\sigma(G_1), \ldots, M_\sigma(G_s))$.

(3) Comes from Proposition 4.4. □

Theorem 4.6 (Finite Henselian Tangent Cone Theorem).

(1) *$K[X, \mathbf{F}]_{\mathrm{loc}}$ satisfies* (NF).

(2) *Let $I \subset K[X, \mathbf{F}]_{\mathrm{loc}}$ be an ideal. The following conditions are equivalent*:

(a) *$\{g_1, \ldots, g_s\} \subset I$ is a $K[X, \mathbf{F}]_{\mathrm{loc}}$-standard base of I.*

(b) *$\forall g \in K[X, \mathbf{F}]_{\mathrm{loc}}$: $g \in I$ iff g has a $K[X, \mathbf{F}]_{\mathrm{loc}}$-standard representation in terms of $\{g_1, \ldots, g_s\}$.*

(c) *$\forall g \in K[X, \mathbf{F}]_{\mathrm{loc}}$: $g \in I$ iff $0 \in \mathrm{NF}(g, \{g_1, \ldots, g_s\}, K[X, \mathbf{F}]_{\mathrm{loc}})$.*

(3) *Normal forms and standard bases in $K[X, \mathbf{F}]_{\mathrm{loc}}$ can be computed.*

(4) *It is possible to decide whether $g \in (g_1, \ldots, g_s)$.* □

Theorem 4.7 (Henselian Tangent Cone Theorem).

(1) *$K[[X]]_{\mathrm{alg}}$ satisfies* (NF).

(2) *Let $I \subset K[[X]]_{\mathrm{alg}}$ be an ideal. The following conditions are equivalent*:

(a) *$\{g_1, \ldots, gs\} \subset I$ is a $K[[X]]_{\mathrm{alg}}$-standard base of I.*

(b) *$\forall g \in K[[X]]_{\mathrm{alg}}$: $g \in I$ iff g has a $K[[X]]_{\mathrm{alg}}$-standard representation in terms of $\{g_1, \ldots, g_s\}$.*

(c) *$\forall g \in K[[X]]_{\mathrm{alg}}$: $g \in I$ iff $0 \in \mathrm{NF}(g, \{g_1, \ldots, g_s\}, K[[X]]_{\mathrm{alg}})$.*

(3) *Normal forms and standard bases in $K[[X]]_{\mathrm{alg}}$ can be computed.*

(4) *It is possible to decide whether $g \in (g_1, \ldots, g_s)$.*

Proof. Let $I = (h_1, \ldots, h_t)$, $g \in K[[X]]_{\mathrm{alg}}$. By the theorem in the Appendix, there is an LSS $\mathbf{F}$ such that $\{h_1, \ldots, h_t, g\} \in K[X, F]_{\mathrm{loc}}$; then the theoretical result is a consequence of Theorem 4.6.

If the series are given in our computational model, then also the computational part is immediate.

Otherwise, if they are given in the classical model, then by the algorithms in the Appendix, an LSS defining them can be explicitly computed. □

Remark 4.8. If $I \subset K[[X]]_{\mathrm{alg}}$ is an ideal, one can define the L-homogeneous ideal $\mathrm{in}(I) := (\mathrm{in}(f){:}\ f \in I)$ and the graded ring $K[X]/\mathrm{in}(I)$. By the method of associated graded rings, questions about the ideal I (such as its dimension or its Hilbert function) can be reduced to the same question about $\mathrm{in}(I) \subset K[X]$. If the latter is known by a Gröbner basis, such questions can be then effectively solved for it.

Proposition 4.9. *Let $(g_1, \ldots, g_s)$ be a standard basis of $I \subset K[[X]]_{\mathrm{alg}}$ with respect to an admissible ordering $<$ of weight L. Then $(\mathrm{in}(g_1), \ldots, \mathrm{in}(g_s))$ is a Gröbner basis of $\mathrm{in}(I) \subset K[X]$ with respect to the converse of $<$.*

Proof. Let $p \in \mathrm{in}(I)$ and let $g \in I$ be such that $\mathrm{in}(g) = p$. Then:

$$M(p) = M(g) \in (M(g_1), \ldots, M(g_s)) = (M(\mathrm{in}(g_1)), \ldots, M(\mathrm{in}(g_s))) .$$

□

Example 3 (continued). Let $I := (X_2^3 - g_1(X_1), X_1X_2 - X_3^3) \in K[X, \mathbf{F}]_{\mathrm{loc}}$; we want to compute a standard basis of I. We compute a standard basis of $(F_1, X_2^3 - X_1^2 - X_1^2Y_1, X_1X_2 - X_3^3)$ in $K[X, Y_1]_{\mathrm{loc}}$ by the Tangent Cone Algorithm, obtaining

$$\{X_1X_2 - X_3^3, X_1^2 + X_1^2Y_1 - X_2^3, F_1 ,$$
$$X_1X_3^3 - X_2^4 + Y_1X_1^2X_2, X_2^5 - X_3^6 - Y_1X_1^2X_2^2\}$$

so: $M(I) = (X_1X_2, X_1^2, X_1X_3^3, X_2^5)$ and $\mathrm{in}(I) = (X_1X_2, X_1^2, X_1X_3^3 - X_2^4, X_2^5)$ which, e.g., allows us to compute dimension, Poincaré series, Hilbert function:
dim$(I) = 1$,
poincare(in(I)) $= (1 + 2z + z^2 + z^3)/(1 - z)$,
hilbertfn(in(I)): $H(0) = 1$, $H(1) = 3$, $H(2) = 4$, for $z > 2$, $H(z) = 5$.

5. Weierstrass Preparation Theorem

In this section we give a computational version of the Weierstrass Preparation Theorem for algebraic series. More precisely, given a distinguished algebraic power series g in $K[X_1, \ldots, X_n, f_1, \ldots, f_r]$ we will construct a *new* LSS with one variable less, defining the coefficients of the Weierstrass polynomial of g with respect to that variable.

Notation. In the next two sections, we will denote $X' := (X_1, \ldots, X_{n-1})$, so that $X = (X', X_n) = (X_1, \ldots, X_{n-1}, X_n)$. Also, we denote by π the two projections of rings $\pi : K[[X_1, \ldots, X_n]] \to K[[X_n]]$ and $\pi : K[X_1, \ldots, X_n, Y_1, \ldots, Y_r] \to K[X_n, Y_1, \ldots, Y_r]$ defined by $\pi(X_i) = 0$ if $i < n$.

Let furthermore $\mathbf{F}_0 = (F_1, \ldots, F_r)$ be a given LSS defining $f_1, \ldots, f_r \in K[[X_1, \ldots, X_n]]_{\mathrm{alg}}$ and let $g \in K[X, \mathbf{F}_0]_{\mathrm{loc}}$.

The following lemma will permit us to check whether g is distinguished in X_n, i.e., whether $g(0, \ldots, 0, X_n) = \pi(g) = \lambda X_d^n +$ higher degree terms, with $\lambda \in K^*$ and some positive integer d; and it will permit us to construct a suitable ordering in the variables (X', X_n).

Lemma 5.1. (1) $\pi(\mathbf{F}_0) := (\pi(F_1), \ldots, \pi(F_r))$ *is a locally smooth system for* $\pi(f_1), \ldots, \pi(f_r)$.

(2) $$\pi(K[X,\mathbf{F}]_{\mathrm{loc}}) \approx K[X_n, \pi(f_1), \ldots, \pi(f_r)]_{\mathrm{loc}} = K[X_n, \pi(\mathbf{F}_0)]_{\mathrm{loc}} \approx \left(\frac{K[X_n, Y_1, \ldots, Y_r]}{(\pi(F_1), \ldots, \pi(F_r))}\right)_{\mathrm{loc}}.$$

(3) *It is possible to decide if* $\pi(g) = g(0, \ldots, 0, X_n) \neq 0$, *in which case to compute a positive integer d such that* $T(\pi(g)) = X_n^d$.

(4) *Let g be a distinguished polynomial in* X_n *of order d; then it is possible to compute an admissible ordering* $<$ *on* $\langle X \rangle$ *such that* $\mathrm{in}(g) = \lambda X_n^d$, $\lambda \in K^*$ (*i.e., any other term in* $\mathrm{Supp}(g)$ *has weight larger than the weight of* X_n^d).

(5) *By changing, if necessary, the LSS* $\mathbf{F}_0$ *we may assume that* $T(f_i) > X_n^d$ *for each i.*

Proof. (1) $F_i(X_1, \ldots, X_n, f_1, \ldots, f_r) = 0$ implies $F_i(0, \ldots, 0, X_n, f_1(0, \ldots, 0, X_n), \ldots, f_r(0, \ldots, 0, X_n)) = 0$, while the jacobian conditions are obviously preserved. Statement (2) is obvious and (3) is a consequence of Lemma 3.2 applied to $K[X_n, \pi(F_1), \ldots, \pi(F_r)]_{\mathrm{loc}}$.

To show (4) a default choice is obtained by assigning $L(X_n) = 1$, $L(X_i) = d + 1$ $\forall i < n$; better choices can be obtained by computing the truncation $\mathrm{Tr}(g)$ of g (and of f_i) at degree d and solving appropriate linear inequalities for force $\lambda X_n^d = \mathrm{in}(\mathrm{Tr}(g))$. As for (5), let $p_i \in K[X_1, \ldots, X_n]$ be such that $T(f_i - p_i) > X_n^d$. Then $(F_j(X_1, \ldots, X_n, Y_1, \ldots, Y_i - p_i, \ldots, Y_r), j = 1 \ldots n)$ is an LSS for $f_1, \ldots, f_i - p_i, \ldots, f_r$. □

Assumptions. From now on we assume that $<$ is an admissible ordering on $\langle X', X_n \rangle$ satisfying conditions (3), (4), and (5) of Lemma 5.1, whose weight we denote by L. Also, assume $\lambda = 1$. By the results of Section 3 we construct an SLSS $\mathbf{F}$ with respect to a σ-extension of $<$, defining the new f_i's. Moreover, assume that g is given by a representation G.

Let $(U) := (U_{10}, \ldots, U_{1,d-1}, \ldots, U_{r0}, \ldots, U_{r,d-1}, U_0, \ldots, U_{d-1})$ be a new set of indeterminates.

Let $P, P_i \in K[X, Y, U]$ be the polynomials

$$P := X_n^d - \sum_{j=0}^{d-1} U_j X_n^j,$$

$$P_i := Y_i - \sum_{j=0}^{d-1} U_{ij} X_n^j \quad \forall i = 1, \ldots, r.$$

Let L_0 be the weight on $\langle X, Y, U \rangle$ defined by

$$L_0(X_i) := L(X_i) \quad \forall i,$$

$$L_0(Y_i) := L(Y_i) \quad \forall i,$$

$$L_0(U_j) := (d-j)L(X_n),$$
$$L_0(U_{ij}) := L(Y_i) - jL(X_n).$$

Remark that $L(Y_i) > dL(X_n)$ $\forall i$ because we assume that $<$ satisfies condition (5) of Lemma 5.1; as a consequence $L_0(U_{ij}) > (d-j)L(X_n) \geq 0$, so that L_0 is actually a weight.

Let $<_U$ be any admissible term ordering on $\langle U \rangle$ such that

$$U_\alpha > U_{\beta\gamma} > U_{\delta\nu} > U_\mu \quad \Leftrightarrow \quad \alpha < \gamma < \mu \leq \nu \text{ or } \gamma = \mu \text{ and } \beta < \gamma .$$

Finally, let $<_0$ be the admissible term ordering on $\langle X, Y, U \rangle$ defined by: for each $m, m' \in \langle X, Y \rangle$, $m_U, m'_U \in \langle U \rangle$,

$$\begin{aligned} m\, m_U <_0 m'\, m'_U \quad \Leftrightarrow\ & L_0(m\, m_U) < L_0(m'\, m'_U) \\ & \text{or } (L_0(m\, m_U) = L_0(m'\, m'_U) \text{ and } m_U <_U m'_U) \\ & \text{or } (L_0(m\, m_U) = L_0(m'\, m'_U)\, , \\ & \qquad m_U = m'_U \text{ and } m < m')\, . \end{aligned}$$

As usual, $T_0(H)$, $M_0(H)$, $\mathrm{in}_0(H)$ will denote the leading term, the leading monomial and the initial form of $H \in K[[X, Y, U]]$ with respect to $<_0$.

Remark 5.2. (1) The ordering $<_0$ satisfies the following properties:

(1.1) its restriction to $\langle X, Y \rangle$ is $<$,

(1.2) if $L_0(m) = L_0(m')$, $m \in \langle X, Y \rangle$, $m' \in \langle U \rangle$, then $m <_0 m'$,

(1.3) generators of $\langle U \rangle$ of the same weight L_0 are ordered according to:

$$U_{ij} > U_{hj} > U_j \quad \text{for } i < h \text{ and for every } j\, ,$$
$$U_{ij} > U_{hk} \text{ and } U_j > U_k \quad \text{for } j < k \text{ and } \forall i,h,$$
$$U_h > U_{ij} \quad \text{for } h < j \text{ and } \forall i$$
$$\begin{aligned} (\text{or: } & U_{10} > U_{20} > \cdots > U_{r0} > U_0 > U_{11} > \cdots \\ & > U_1 > \cdots > U_{1,d-1} > \cdots > U_{r,d-1} > U_{d-1})\, . \end{aligned}$$

(2) The polynomials P and P_i's in $K[X, Y, U]$ are L_0-homogeneous; $T_0(P) = X_n^d$, $T_0(P_i) = Y_i$ $\forall i$.

(3) $\{P, P_1, \ldots, P_r\}$ is a Gröbner basis of the ideal it generates with respect to the converse of $<_0$.

(4) By Buchberger reduction, given any polynomial $F \in K[X, Y, U]$, we can compute a canonical form of F with respect to $\{P, P_1, \ldots, P_r\}$, i.e., a polynomial $\mathrm{Can}(F) = F' \in K[X, Y, U]$ such that

$$F - F' \in (P, P_1, \ldots, P_r)\,, \qquad \mathrm{Supp}(F') \cap (X_n^d, Y_1, \ldots, Y_r) = \emptyset\,.$$

Therefore, if we apply Buchberger reduction to $G, F_1, \ldots, F_r$, we obtain polynomials

$$H_0, \ldots, H_{d-1}, H_{1,0}, \ldots, H_{1,d-1}, \ldots, H_{r,0}, \ldots, H_{r,d-1}$$
$$\in (X_1, \ldots, X_{n-1}, U)K[X_1, \ldots, X_{n-1}, U] = K[X', U]$$

such that

$$(*) \qquad G - \sum_{j=0}^{d-1} H_j X_n^j \in (P, P_1, \ldots, P_r)\,,$$

$$(*)_i \qquad F_i - \sum_{j=0}^{d-1} H_{ij} X_n^j \in (P, P_1, \ldots, P_r) \quad \forall i\,.$$

Lemma 5.3. *(1) $U_\lambda \not\in \mathrm{Supp}(H_j)$ for $\lambda > j$ and $U_{\mu\lambda} \not\in \mathrm{Supp}(H_j)$ for $\lambda > j$ and $\forall \mu$. Moreover, $U_j \in \mathrm{Supp}(H_j)$.*

(2) $U_\lambda \not\in \mathrm{Supp}(H_{ij})$ $\forall \lambda \geq j$, $U_{\lambda k} \not\in \mathrm{Supp}(H_{ij})$ for $k > j$ or for $k = j$ and $\lambda > i$. Moreover, $U_{ij} \in \mathrm{Supp}(H_{ij})$.

Proof. (1) We can write

$$\begin{aligned} G &= X_n^d + \sum_{j=0}^{d-1} A_j(X', Y) X_n^j + X_n^d G_0(X, Y) \\ &= X_n^d + \sum_{j=0}^{d-1} \sum_{i=1}^{r} c_{ij} Y_i X_n^j + X_n^d \sum_{j=1}^{d-1} c_j X_n^j \\ &\quad + \sum_{j=0}^{d-1} B_j(X', Y) X_n^j + X_n^d(X_n^d G' + G''(X, Y))\,, \end{aligned}$$

with $B_j \in (X') + (Y)^2$ and $G'' \in (X', Y)$.

Let $\sum_{j=0}^{d-1} H_j''' X_n^j$ be the canonical form of

$$\sum_{j=0}^{d-1} B_j(X', Y) X_n^j + X_n^d(X_n^d G' + G''(X, Y))$$

with respect to $\{P, P_1, \ldots, P_r\}$. An easy direct computation shows that $U_\lambda \not\in \mathrm{Supp}(H_j''')$ $\forall \lambda$ and that $U_{\mu\lambda} \not\in \mathrm{Supp}(H_j''')$ $\forall \lambda, \mu$.

Let $\sum_{j=0}^{d-1} H_j' X_n^j$ be the canonical form of $\sum_{j=0}^{d-1} \sum_{i=1}^{r} c_{ij} Y_i X_n^j$ with respect to $\{P, P_1, \ldots, P_r\}$; since it is also the canonical form of $\sum_{j=0}^{d-1} \sum_{i=1}^{r} c_{ij} \sum_{k=0}^{d-1} U_{ik} X_n^{j+k}$, again a direct verification shows that $U_\lambda \not\in \mathrm{Supp}(H_j')$ $\forall \lambda$ and $U_{\mu\lambda} \not\in \mathrm{Supp}(H_j')$ for $\lambda > j$ and $\forall \mu$.

Finally, let $\sum_{j=0}^{d-1} H''_j X_n^j$ be the canonical form of $X_n^d \sum_{j=1}^{d-1} c_j X_n^j$ and also of $\sum_{j=1}^{d-1}\sum_{k=0}^{d-1} c_j U_k X_n^{j+k}$, again $U_\lambda \not\in \mathrm{Supp}(H''_j)$ $\forall\lambda \geq j$ and $U_{\mu\lambda} \not\in \mathrm{Supp}(H''_j)$ $\forall \lambda,\mu$.

Clearly, because of the uniqueness of canonical forms, one has

$$\sum_j H_j X_n^j = \sum_j U_j X_n^j + \sum_j H'_j X_n^j + \sum_j H''_j X_n^j + \sum_j H'''_j X_n^j .$$

Therefore, we obtain that

$$U_\lambda \not\in \mathrm{Supp}(H_j) \text{ for } \lambda > j \quad \text{and} \quad U_{\mu\lambda} \not\in \mathrm{Supp}(H_j) \text{ for } \lambda > j \text{ and } \forall \mu .$$

Also, $U_j \in \mathrm{Supp}(H_j)$.

(2) Recalling that $F_i = Y_i + \sum_{\lambda<i} b_{i\lambda} Y_\lambda + F'_i$, with $F'_i \in (X, Y^2)$ and that $L(Y_i) > L(X_n^d)$ (by assumption), we can write

$$F'_i = \sum_\mu \sum_{j=1}^{d-1} c_{i\mu j} Y_\mu X_n^j + \sum_{\mu=1}^{d-1} d_{i\mu} X_n^{d+\mu} + R_i(X', X_n, Y)$$

with $R_i \in (X') + (Y)^2 + X_n^d(X_n^d, Y)$. Again one has that,

denoting $\sum_j H'''_{ij} X_n^j$ the canonical form of $R_i(X', X_n, Y)$, $U_\lambda \not\in \mathrm{Supp}(H'''_{ij})$ $\forall\lambda$ and $U_{\mu\lambda} \not\in \mathrm{Supp}(H'''_{ij})$ $\forall\lambda,\mu$;

denoting $\sum_j H'_{ij} X_n^j$ the canonical form of $\sum_\mu \sum_{j=1}^{d-1} c_{i\mu j} Y_\mu X_n^j$, which is also the canonical form of $\sum_{j=1}^{d-1}\sum_\mu c_{i\mu j} \sum_{k=0}^{d-1} U_{\mu k} X_n^{j+k}$, $U_\lambda \not\in \mathrm{Supp}(H'_{ij})$ $\forall\lambda$ and $U_{\mu\lambda} \not\in \mathrm{Supp}(H'_{ij})$ for $\lambda \geq j$ and $\forall\mu$;

denoting $\sum_j H''_{ij} X_n^j$ the canonical form of $\sum_{\mu=1}^{d-1} d_{i\mu} X_n^{d+\mu}$ and also of $\sum_{\mu=1}^{d-1}\sum_{k=0}^{d-1} d_{i\mu} U_k X_n^{\mu+k}$, again $U_\lambda \not\in \mathrm{Supp}(H''_{ij})$ $\forall\lambda \geq j$ and $U_{\mu\lambda} \not\in \mathrm{Supp}(H_{ij})$ $\forall\lambda,\mu$.

Clearly, one has

$$\begin{aligned}\sum_j H_{ij} X_n^j &= \sum_j U_{ij} X_n^j + \sum_{\lambda<i} b_{i\lambda} \sum_j U_{\lambda_j} X_n^j \\ &\quad + \sum_j H'_{ij} X_n^j + \sum_j H''_{ij} X_n^j + \sum_j H'''_{ij} X_n^j .\end{aligned}$$

Therefore, we obtain that

$$U_\lambda \not\in \mathrm{Supp}(H_{ij}) \quad \forall\lambda \geq j ,$$

$$U_{\lambda k} \not\in \mathrm{Supp}(H_{ij}) \quad \text{for } k > j \text{ or for } k = j \text{ and } \lambda > i .$$

Also, by the same argument, $U_{ij} \in \mathrm{Supp}(H_{ij})$. □

Proposition 5.4. (1) *The system* $\mathbf{H} := (H_{1,0}, \ldots, H_{r,0}, H_0, H_{1,1}, \ldots, H_{r,1}, H_1, \ldots, H_{1,d-1}, \ldots, H_{r,d-1}, H_{d-1})$ *is an LSS, defining algebraic series*

$$h_{1,0},\ldots,h_{r,0},h_0,h_{1,1},\ldots,h_{r,1},h_1,\ldots,h_{1,d-1},\ldots,h_{r,d-1},h_{d-1}$$
$$\in K[[X']]_{\mathrm{alg}}.$$

(2) $\mathbf{W}:=(\mathbf{H},\mathbf{F})=(H_{1,0},\ldots,H_{r,0}, \quad H_0, \quad H_{1,1},\ldots,H_{r,1}, \quad H_1,\ldots,H_{1,d-1},\ldots, H_{r,d-1}, H_{d-1}, F_1,\ldots,F_r)$ *is an LSS.*

(3) *The polynomial* $\sum_{j=0}^{d-1} h_jX_n^j \in K[[X']]_{\mathrm{alg}}[X_n]$ (*resp.* $\forall i$: $\sum_{j=0}^{d-1} h_{ij}X_n^j$) *is* the *canonical form of* X_n^d (*resp. of* Y_i) *with respect to* $\{G, F_1,\ldots,F_r\}$ *in the power series ring* $K[[X,Y]]$.

(4) $\sigma_{\mathbf{W}}(P)$ *and* $\sigma_{\mathbf{W}}(P_i)\in(g)K[[X]]$.

Proof. Because of Lemma 5.3 the linear part of the Jacobian of $\mathbf{H}$ is a lower triangular nonsingular matrix, after reordering the U-variables and, consequently, the polynomials H_j's and H_{ij}'s, according to the uniform term ordering defined in the construction (i.e. $U_\alpha > U_{\beta\gamma} > U_{\delta\nu} > U_\mu \Leftrightarrow a<\gamma<\mu\le\nu$ or $\gamma=\mu$ and $\beta<\gamma$).

(2) It is then clear that the same holds for the Jacobian of $\mathbf{W}$.

(3) We first remark that $\{G, F_1,\ldots,F_r\}$ is a standard basis of the ideal I it generates in $K[X,Y]_{\mathrm{loc}}$ and therefore of $IK[[X,Y]]$ too. By Galligo's theorem (cf. [7]) there are unique $g_0,\ldots,g_{d-1}, g_{10},\ldots,g_{1,d-1},\ldots,g_{r0},\ldots,g_{r,d-1}\in K[[X']]$ such that

$$\mathrm{Can}(X_n^d,\{G,F_i\},K[[X,Y]])=\sum_{j=0}^{d-1} g_jX_n^j\,,$$

$$\mathrm{Can}(Y_i,\{G,F_i\},K[[X,Y]])=\sum_{j=0}^{d-1} g_{ij}X_n^j\,.$$

Let $\tau: K[U,X,Y]\to K[[X,Y]]$ denote the evaluation such that $\tau(U_j)=g_j$, $\tau(U_{ij})=g_{ij}$, we obtain

$$\tau(P)=X_n^d-\sum_{j=0}^{d-1} g_j\,X_n^j\,,$$

$$\tau(P_i)=Y_i-\sum_{j=0}^{d-1} g_{ij}X_n^j\,;$$

moreover, we remark that $X_n^d<T(g_j)X_n^j$ so $1<T(g_j)$, and therefore $g_j(0)=0$, and, in the same way, $g_{ij}(0)=0$, so that we can conclude that $\{\tau(P), \tau(P_1),\ldots,\tau(P_r)\}$ is a standard basis of $IK[[X,Y]]$. Because of the equations $(*)$, $(*)_i$ we have:

$$\sum_{j=0}^{d-1} \tau(H_j)X_n^j\in IK[[X,Y]]\,,$$

$$\sum_{j=0}^{d-1} \tau(H_{ij})X_n^j\in IK[[X,Y]]\,.$$

Since $M(I)=(X_n^d, Y_1, \ldots, Y_r)$ and $\mathrm{Supp}(\sum_{j=0}^{d-1} \tau(H_j)X_n^j) \cap (X_n^d, Y_1, \ldots, Y_r)=\emptyset$, we can conclude that $\sum_{j=0}^{d-1} \tau(H_j)X_n^j=0$, i.e., $\tau(H_j)=0\ \forall j$; and, in the same way, that $\tau(H_{ij})=0$, too. This means that the $\{g_j, g_{ij}\}$ are a solution of the system $\{H_j=H_{ij}=0\}$.

Therefore, by the uniqueness of the solutions of the Implicit Function Theorem, we conclude that $g_j=h_j$ and $g_{ij}=h_{ij}$.

(4) It is a consequence of (the proof of) (3), since $\tau=\sigma_{\mathbf{H}}$ and $\sigma_{\mathbf{W}}(I)=(g)K[[X]]$. $\square$

Theorem 5.5 (Effective Weierstrass Preparation Theorem). *Given a local smooth system $\mathbf{F}_0 \subset K[X, Y]$, a polynomial $G_0 \in K[X, Y]_{\mathrm{loc}}$ such that, denoting $g=\sigma_{\mathbf{F}_0}(G_0)$, g is regular of order d in X_n ($g(0, \ldots, 0, X_n) \neq 0$), it is possible to compute*:

(1) *an admissible term ordering $<$ on $\langle X, Y\rangle$ such that $T(g)=X_n^d$, an SLSS (with respect to $<$) $\mathbf{F}=(F_1, \ldots, F_r)$ defining $f_1, \ldots, f_r \in K[[X]]_{\mathrm{alg}}$ such that $K[X, \mathbf{F}]_{\mathrm{loc}}=K[X, \mathbf{F}_0]_{\mathrm{loc}}$ and a representation $G \in K[X, Y]_{\mathrm{loc}}$ of g verifying the conditions of the above assumptions.*

(2) *A locally smooth system $\mathbf{H} \subset K[X', U]=K[X_1, \ldots, X_{n-1}, U]$ defining algebraic series $h_0, \ldots, h_{d-1}, h_{10}, \ldots, h_{1d-1}, \ldots, h_{r0}, \ldots, h_{rd-1} \in K[[X']]_{\mathrm{alg}}$ which is an SLSS with respect to a σ_H-extension of $<$, and such that $\mathbf{W}:=(\mathbf{H}, \mathbf{F})$ is an SLSS with respect to a $\sigma_{\mathbf{W}}$-extension of $<$.*

(3) *$V, V_i \in K[X, Y, U]_{\mathrm{loc}}$, V a unit such that*

$$g\sigma_{\mathbf{W}}(V)=X_n^d-\sum_{j=0}^{d-1} h_jX_n^j=X_n^d-\sum_{j=0}^{d-1} \sigma_H(U_j)X_n^j \in K[X', \mathbf{H}]_{\mathrm{loc}}[X_n]$$

and

$$f_i=\sigma_{\mathbf{W}}(V_i)g+\sum_{j=0}^{d-1} h_{ij}X_n^j \quad \forall i\,.$$

Proof. (1) This has been already obtained by means of Lemma 5.1.

(2) By Proposition 5.4 we obtain an LSS $\mathbf{H}$ and by Proposition 3.4 we get the required SLSS, again called $\mathbf{H}$ by abuse of notation.

(3) Since $\{g\}$ is a standard basis in $K[X, \mathbf{W}]_{\mathrm{loc}}$ of the ideal it generates, $\{G, \mathbf{W}\}$ is a standard basis in $K[X, Y, U]_{\mathrm{loc}}$ of the ideal it generates. Also $P, P_i \in (G, \mathbf{W})$ by Proposition 5.4(4). Therefore, we have computable standard representations:

$$(\circ) \qquad X_n^d-\sum_{j=0}^{d-1} U_jX_n^j=\sum A_jF_j+\sum B_jH_j+\sum B_{\lambda j}H_{\lambda j}+VG\,,$$

$$(\circ)_i \qquad Y_i-\sum_{j=0}^{d-1} U_{ij}X_n^j=\sum A_{ij}F_j+\sum B_{ij}H_j+\sum B_{i\lambda j}H_{\lambda j}+V_iG\,,$$

where V is a unit in $K[X, Y]_{\mathrm{loc}}$.

So, applying $\sigma_{\mathbf{W}}$ to both sides of $(\circ)$ and $(\circ)_i$:

$$X_n^d - \sum_{j=0}^{d-1} h_j X_n^j = \sigma_{\mathbf{W}}(V)g\,,$$

$$f_i - \sum_{j=0}^{d-1} h_{ij} X_n^j = \sigma_{\mathbf{W}}(V_i)g\,. \qquad \square$$

Definition. We will denote

$$\mathrm{Wei}(g) := \sigma_{\mathbf{W}}(V)g = X_n^d - \sum_{j=0}^{d-1} h_j X_n^j \in K[X', \mathbf{H}]_{\mathrm{loc}}[X_n]$$

the *Weierstrass form* of g.

Algorithm. Let us resume the construction which given an LSS $\mathbf{F}_0 \subset K[X, Y]$ and $G \in K[X, Y]$ decides whether $g = \sigma_{\mathbf{F}_0}(G_0)$ is distinguished in X_n and in this case computes an LSS $\mathbf{H} \subset K[X', U]$ and $W \in K[X', U][X_n]$ such that $\sigma_{\mathbf{H}}(W) = \mathrm{Wei}(g)$.

(1) We compute $\pi(\mathbf{F}) = \{F(0, \ldots, 0, X_n, Y_1, \ldots, Y_r): F \in \mathbf{F}\}$, which is an LSS for $\pi(f_1), \ldots, \pi(f_r)$; we modify it into an SLSS $\mathbf{F}_1$ for $(\pi(f_i): \pi(f_i) \neq 0)$ with respect to a uniform term ordering.

(2) We compute a normal form G_1 of $\pi(G) = G(0, \ldots, 0, X_n, Y_1, \ldots, Y_r)$ with respect to $\pi(\mathbf{F}_1)$. If $G_1 = 0$, then g is not distinguished and the computation halts.

(3) Otherwise we obtain d such that $T(G_1) = X_n^d$ and we can compute a weight L such that $\mathrm{in}(g) = X_n^d$ (e.g., by setting $L(X_n) = 1$, $L(X_i) = d + 1$ for $i \neq n$) and an admissible term ordering $<$ on $\langle X \rangle$ of weight L.

(4) We compute, by truncated Buchberger reduction with respect to $\mathbf{F}_0$, polynomials $p_i \in K[X]$ such that $T(f_i - p_i) > X_n^d$. Then $\mathbf{F}_2 = (F_j(X_1, \ldots, X_n, Y_1 - p_1, \ldots, Y_r - p_r): j = 1 \ldots r)$ is an LSS for $f_i - p_i$.

We set $f_i := f_i - p_i$ and we compute an SLSS (with respect to a σ-ordering) for $f_1, \ldots, f_r$; which we denote by $\mathbf{F}$.

(5) We set U, P, P_i, L_0, $<_0$ as specified in the above construction (after the assumption).

(6) By Buchberger reduction with respect to the Gröbner basis (P, P_i) we obtain $H_0, \ldots, H_{d-1}, H_{10}, \ldots, H_{1,d-1}, \ldots, H_{r0}, \ldots, H_{r,d-1} \in K[X', U]$ such that $\sum_{j=0}^{d-1} H_j X_n^j$ is the canonical form of G and $\sum_{j=0}^{d-1} H_{ij} X_n^j$ of F_i with respect to: (P, P_i).

(7) We then set $\mathbf{H} := (H_{1,0}, \ldots, H_{r,0}, H_0, H_{1,1}, \ldots, H_{r,1}, H_1, \ldots, H_{1,d-1}, \ldots, H_{r,d-1}, H_{d-1})$ and $W := \sum_{j=0}^{d-1} U_j X_n^j$.

Under the same assumptions and notations of Theorem 5.5, we have, moreover, the following:

Theorem 5.6 (Effective Weierstrass Division Theorem). *Let* $B \in K[X, Y]$, *so that* $0 \neq b := \sigma_{\mathbf{F}_0}(B) \in K[X, \mathbf{F}] \subset K[X, \mathbf{W}]_{\mathrm{loc}}$. *Then*:

(1) *it is possible to compute* $A \in K[X, Y, U]_{\mathrm{loc}}$, *polynomials* $A_j \in K[X', U]$, $j = 0, \ldots, d-1$, *such that*

$$b = \sigma_{\mathbf{W}}(A)\mathrm{Wei}(g) + \sum_{j=0}^{d-1} \sigma_{\mathbf{H}}(A_j)X_n^j ,$$

(2) $\sum_{j=0}^{d-1} \sigma_{\mathbf{H}}(A_j)X_n^j = \mathrm{Can}(b, \{g\}, K[[X]])$,

(3) $\sigma_{\mathbf{W}}(A)$, $\sigma_{\mathbf{H}}(A_j)$ *are unique.*

Proof. We have: $\sigma_{\mathbf{F}}(B) = b \in K[X, \mathbf{F}] \subset K[X, \mathbf{W}]$. Since $B \not\in (F_1, \ldots, F_r)$, by truncated Buchberger reduction, one can compute a *polynomial* $B_1 \in K[X, Y, U]$, which is a representation of b. By Buchberger reduction with respect to (P, P_i) we can compute $A_j \in K[X', U]$, $j = 0, \ldots, d-1$ such that

$$B_1 - \sum A_j X_n^j \in (P, P_i) .$$

Then $\sigma_{\mathbf{W}}(B_1) - \sum \sigma_{\mathbf{W}}(A_j)X_n^j \in (\sigma_{\mathbf{W}}(P), \sigma_{\mathbf{W}}(P_i)) = (g)$, i.e., $B_1 - \sum A_j X_n^j \in (G, \mathbf{W})$. So we can compute a standard representation: $B_1 - \sum A_j X_n^j = A'G + \sum_{W_i \in \mathbf{W}} C_i W_i$. Since $\sigma_{\mathbf{W}}(W_i) = 0$, we have

$$b = \sigma_{\mathbf{W}}(B_1) = \sigma_{\mathbf{W}}(A')g + \sum_{j=0}^{d-1} \sigma_{\mathbf{W}}(A_j)X_n^j .$$

To complete the proof we set $A := V^{-1}A'$, where V is the unit given in Theorem 5.5; finally we have just to remark that, since $A_j \in K[X', U]$, $\sigma_{\mathbf{W}}(A_j) = \sigma_{\mathbf{H}}(A_j)$.

The claims (2) and (3) are then obvious. □

Remark 5.7. We want to point out explicitly a weakness of our approach: the nonzero coefficients in $K[[X_1, \ldots, X_{n-1}]]$ of the Weierstrass polynomial of G are treated as they were polynomially independent, requiring each a new variable and a generator in a standard local smooth system. This is an obviously inefficient approach, especially in view of repeated applications as in the next paragraph. However, in particular cases, we do not need all the construction given above, e.g., if the polynomial G does not depend on the Y variables, we do not need to introduce the U_{ij}'s and therefore the procedure is greatly simplified. It is moreover possible, using Proposition 2.4, to check, at least, whether these coefficients are polynomials, and, eventually, to reduce in this way the size of the LSS's.

Example 3 (continued). Let $g := g_1 - X_2^3$ and remark that $T(g(X_1, 0, 0)) \neq 0$. We can therefore apply the Weierstrass Preparation Theorem to obtain $\mathrm{Wei}(g) \in K[[X_2, X_3]]_{\mathrm{alg}}[X_1]$.

We introduce the new variables T_0, T_1, V_0, V_1 and the ideal $(X_1^2 - X_1T_1 - T_0, Y_1 - X_1V_1 - V_0)$.

The canonical form of F_1 with respect to it is $H_1X_1 + H_0$; the one of $X_1^2 + X_1^2Y_1 - X_2^3$ is $H_3X_1 + H_4$, where

$$H_1 = 2V_0 - T_1T_0 + T_0V_1^2 + V_0^2 - T_1^2T_0V_1 - T_1T_0V_0 - T_0^2V_1 ,$$

$$H_2 = T_0 - X_2^3 + T_1T_0V_1 + T_0V_0 ,$$

$$H_3 = 2V_1 - T_1^2 - T_0 + T_1V_1^2 + 2V_1V_0 - T_1^3V_1 - T_1^2V_0 - 2T_1T_0V_1 - T_0V_0 ,$$

$$H_4 = T_1 + T_1^2V_1 + T_1V_0 + T_0V_1 .$$

$\mathbf{H} = (H_1, \ldots, H_4)$ is an LSS defining $h_1, \ldots, h_4 \in K[[X_2]]_{\mathrm{alg}}$.

As in Section 3, we compute: $\mathrm{in}(h_1) = (-1/8)X_2^9$, $\mathrm{in}(h_2) = X_2^3$, $\mathrm{in}(h_3) = (1/2)X_2^3$, $\mathrm{in}(h_4) = (-1/2)X_2^6$. Finally, we have: $\mathrm{Wei}(X_1^2 + X_1^2f_1 - X_2^3) = X_1^2 - h_4X_1 - h_2$.

6. Noether Normalization Lemma

We are giving now two main consequences of the Weierstrass Preparation Theorem: the Noether Normalization Theorem and the elimination theory for algebraic series. For this we need some generalities from commutative algebra.

Let us fix the following notations:

Definition. Let $(A, \mathbf{m})$ be a local ring and U an indeterminate, we say that a polynomial $g \in A[U]$ is a *Weierstrass polynomial* if it is of the form

$$g = U^d + \sum_{i=0}^{d-1} a_iU^i , \quad \text{with } a_i \in \mathbf{m} .$$

Given a set $U = (U_1, \ldots, U_s)$ of indeterminates, we say that a set $\{g_1, \ldots, g_s\} \subset A[U]$, is a *Weierstrass sequence* if:

$g_s \in A[U_1]$ is a Weierstrass polynomial (in U_1),

for k, $1 \leq k < s$, $g_k \in A[U_1, \ldots, U_{s-k+1}]$ has the form:

$$g_k = U_{s-k+1}^d + \sum_{i=0}^{d-1} a_iU_{s-k+1}^i$$

with $a_i \in (\mathbf{m}, U_1, \ldots, U_{s-k})A[U_1, \ldots, U_{s-k}]$.

Lemma 6.1. *Let $(A, \mathbf{m})$ be a local ring and let $I \subset A[U_1, \ldots, U_s]$ be an ideal containing a Weierstrass sequence $\{g_1, \ldots, g_s\}$; then $IA[U]_{\mathrm{loc}} \cap A[U] = I$.*

Proof. We first observe that out contention is equivalent to the fact that every associated prime ideal of I is contained in $\mathbf{n} = (\mathbf{m}, U_1, \ldots, U_s)A[U_1, \ldots, U_s]$, and, therefore, it is enough to show that the only maximal ideal of $A[U_1, \ldots, U_s]$ which contains I is $\mathbf{n}$.

Let $\mathbf{n}^*$ be such an ideal; since $(g_1, \ldots, g_s) \subset \mathbf{n}^*$, the natural map

$$\frac{A}{\mathbf{n}^* \cap A} \to \frac{A[U]}{\mathbf{n}^*}$$

is an integral extension and, hence

$$\frac{A}{\mathbf{n}^* \cap A}$$

is a field and so $\mathbf{n}^* \cap A = \mathbf{m}$. Using the definition of Weierstrass sequence we obtain that $\mathbf{n}^*$ contains also the U_j's. □

Lemma 6.2. *Let A be a noetherian local normal domain, let B denote its henselization and let $I \subset A[U]$ be an ideal; then $IB[U] \cap B = (I \cap A)B$.*

Proof. We only have to show '$\subset$', which is straightforward if B were a free A-module.

Let $IB[U] \cap B = (b_1, \ldots, b_r)B$; then we will reduce to the preceding case by finding a suitable finite flat (hence free since A is local) extension C of A, contained in B, such that $b_i \in IC[U] \cap C$ for every i. For this let C be an étale-standard A-algera containing the b_i's (cf. [12, Chapter VIII]); then C is a flat and finitely generated A-module (cf. [12, Chapter V]). □

Let us return to the situation of algebraic series.

We first state a general lemma, in which $T = (T_1, \ldots, T_s)$ is a new set of variables.

Lemma 6.3. *Let $\mathbf{F} \subset K[X, Y]$ be an LSS defining $h_1, \ldots, h_t$; let I be an ideal in $K[X, \mathbf{F}]_{\mathrm{loc}}[T_1, \ldots, T_s]$. Then it is possible to compute a basis of $I \cap K[X, \mathbf{F}]_{\mathrm{loc}}$, consisting of elements in $K[X, \mathbf{F}]$.*

Proof. Let us denote by σ both the evaluation map $\sigma_{\mathbf{F}}$ and its polynomial natural extension $K[X, Y]_{\mathrm{loc}}[T] \to K[X, \mathbf{F}]_{\mathrm{loc}}[T]$. Let $J := \sigma^{-1}(I) \subset K[X, Y]_{\mathrm{loc}}[T]$. Clearly,

$$I \cap K[X, \mathbf{F}]_{\mathrm{loc}} = \sigma(J \cap K[X, Y]_{\mathrm{loc}}) .$$

Then by an application of the Tangent Cone Algorithm (cf. [10, Proposition 12]) it is possible to compute a basis G of J such that $G \cap K[X, Y]_{\mathrm{loc}}$ is a basis of $J \cap K[X, Y]_{\mathrm{loc}}$. □

Lemma 6.4. *Let* $\mathbf{H}_j$ *be an LSS defining series in* $K[[X_1,\ldots,X_{n-j}]]_{\mathrm{alg}}$, $A_j := K[X_1,\ldots,X_{n-j},\mathbf{H}_j]_{\mathrm{loc}}$. *Let* $B_j := \{b_{1j},\ldots,b_{jj}\}$ *be a Weierstrass sequence in* $A_j[X_{n-j+1},\ldots,X_n]$,

$$g_{1j},\ldots,g_{sj} \in A_j[X_{n-j+1},\ldots,X_n]\,,$$
$$I_j := (b_{1j},\ldots,b_{jj},g_{1j},\ldots,g_{sj})A_j[X_{n-j+1},\ldots,X_n]\,.$$

Then:

(1)

$$I_jK[[X_1,\ldots,X_n]]_{\mathrm{alg}} \cap K[[X_1,\ldots,X_{n-j}]]_{\mathrm{alg}} = (0)$$
$$\Leftrightarrow I_jA_j[X_{n-j+1},\ldots,X_n] \cap A_j = (0)\,.$$

(2) *It is possible to test whether* $I_jK[[X_1,\ldots,X_n]]_{\mathrm{alg}} \cap K[[X_1,\ldots,X_{n-j}]]_{\mathrm{alg}} = (0)$.

Proof. (1) Notice that '$\Rightarrow$' is obvious.

To show the converse, let $\mathbf{a}$ be the left-hand ideal and suppose $\mathbf{a} \neq 0$.

Since it is a nonzero ideal of $K[[X_1,\ldots,X_{n-j}]]_{\mathrm{alg}}$ which is the henselization of the local ring A_j, one has $\mathbf{a} \cap A_j \neq 0$ (cf. [12, Chapter V]). Moreover,

$$\begin{aligned}\mathbf{a} \cap A_j &= I_jK[[X_1,\ldots,X_n]]_{\mathrm{alg}} \cap A_j[X_{n-j+1},\ldots,X_n]_{\mathrm{loc}} \cap A_j\\ &= I_jA_j[X_{n-j+1},\ldots,X_n]_{\mathrm{loc}} \cap A_j = I_jA_j[X_{n-j+1},\ldots,X_n] \cap A_j\,,\end{aligned}$$

where the second equality comes from the faithfully flatness of the henselization, and the third one by Lemma 6.1.

(2) Because of Lemma 6.3 one can compute a basis of $I_jA_j[X_{n-j+1},\ldots,X_n] \cap A_j$ and so test whether it is (0). Because of (1), this gives a test whether $I_jK[[X_1,\ldots,X_n]]_{\mathrm{alg}} \cap K[[X_1,\ldots,X_{n-j}]]_{\mathrm{alg}} = (0)$. $\square$

Lemma 6.5. *With the same notation as in Lemma* 6.4, *assume that*

$$I_jK[[X_1,\ldots,X_n]]_{\mathrm{alg}} \cap K[[X_1,\ldots,X_{n-j}]]_{\mathrm{alg}} \neq (0)\,.$$

Let $h \in I_jA_j[X_{n-j+1},\ldots,X_n] \cap A_j$, $h \neq 0$.

Let γ *be a linear change of the coordinates* $X_1,\ldots,X_{n-j}$, *such that* $\gamma(h)$ *is a distinguished series.*

Let $\mathbf{H}_{j+1}$ *be an LSS such that* $b_{j+1,j+1} := \mathrm{Wei}(\gamma(h)) \in K[X_1,\ldots,X_{n-j-1},\mathbf{H}_{j+1}]_{\mathrm{loc}}$; *for each* i, *let*

$$b_{i,j+1} := \mathrm{Can}(\gamma(b_{ij}),\,b_{j+1,j+1},\,K[[X_1,\ldots,X_n]])\,,$$

$$A_{j+1} := K[X_1,\ldots,X_{n-j-1},\mathbf{H}_{j+1}]_{\mathrm{loc}}\,.$$

Then:

(1) *for each* i, $b_{i,j+1} \in A_{j+1}[X_{n-j}, \ldots, X_n]$

(2) $(b_{i,j+1}, \ldots, b_{j+1,j+1})$ *is a Weierstrass sequence.*

Proof. (1) is a consequence of the Weierstrass Division Theorem.

(2) $(b_{1j}, \ldots, b_{jj})$ is a Weierstrass sequence; since γ leaves fixed $X_{n-j}, \ldots, X_n$, $(\gamma(b_{1j}), \ldots, \gamma(b_{jj}))$ is a Weierstrass sequence; since $b_{i,j+1} = \mathrm{Can}(\gamma(b_{ij}), b_{j+1,j+1}, K[[X_1, \ldots, X_n]])$ is obtained by substituting each coefficient in A_{j+1} of $\gamma(b_{ij})$ by its canonical form, $(b_{1,j+1}, \ldots, b_{j+1,j+1})$ is a Weierstrass sequence. □

Theorem 6.6 (Effective Noether Normalization Lemma). *Let* $I = (g_1, \ldots, g_s)$ *be an ideal of* $K[[X]]_{\mathrm{alg}} = K[[X_1, \ldots, X_n]]_{\mathrm{alg}}$ *generated by polynomials* g_j *in* $K[X, \mathbf{F}]$, *where* $\mathbf{F}$ *is an LSS defining the algebraic series* $f_1, \ldots, f_r$.

Then there exist, and can be calculated

(a) *a linear change of coordinates* $C : K[[X]]_{\mathrm{alg}} \to K[[X]]_{\mathrm{alg}}$,

(b)

$$p := \dim \frac{K[[X]]_{\mathrm{alg}}}{I},$$

(c) *an LSS* $\mathbf{H}$ *with respect to the variables* $X_1, \ldots, X_p$,

(d) *a Weierstrass sequence*

$$B := (b_1, \ldots, b_{n-p}) \subset C(I) K[X_1, \ldots, X_p, \mathbf{H}]_{\mathrm{loc}}[X_{p+1}, \ldots, X_n],$$

(e) *elements* $h_1, \ldots, h_s \in K[X_1, \ldots, X_p, \mathbf{H}]_{\mathrm{loc}}[X_{p+1}, \ldots, X_n]$ *such that* $C(I) = (b_1, \ldots, b_{n-p}, h_1, \ldots, h_s)$.

As a consequence:

(i) $C(I) \cap K[[X_1, \ldots, X_p]]_{\mathrm{alg}} = (0)$,

(ii)

$$K[[X_1, \ldots, X_p]]_{\mathrm{alg}} \to \frac{K[[X_1, \ldots, X_p, X_{p+1}, \ldots, X_n]]_{\mathrm{alg}}}{C(I)}$$

is an integral extension.

Proof. If the data (a)–(e) have been obtained, then (i) and (ii) hold, since

$$p = \dim \frac{K[[X]]_{\mathrm{alg}}}{I}$$

and the elements in B give integral algebraic relations satisfied by $X_{p+1}, \ldots, X_n$ mod $C(I)$.

So let us show how to construct the data (a)–(e).

If $I = (0)$, which can be checked by Proposition 4.3, then $p = n$ and there is nothing to prove. So we assume $I \neq 0$.

We are going to construct inductively the following data:

(a) a linear change of coordinates $C_j : K[[X]]_{\mathrm{alg}} \to K[[X]]_{\mathrm{alg}}$,

(b) an LSS $\mathbf{H}_j$ defining series in $K[[X_1, \ldots, X_{n-j}]]_{\mathrm{alg}}$,
(c) the ring $A_j := K[X_1, \ldots, X_{n-j}, \mathbf{H}_j]_{\mathrm{loc}}$,
(d) a Weierstrass sequence $B_j := \{b_{1,j}, \ldots, b_{j,j}\}$ in $A_j[X_{n-j+1}, \ldots, X_n]$,
(e) elements $g_{1,j}, \ldots, g_{s,j} \in A_j[X_{n-j+1}, \ldots, X_n]$,

such that denoting $I_j = (b_{1,j}, \ldots, b_{j,j}, g_{1,j}, \ldots, g_{s,j})A_j[X_{n-j+1}, \ldots, X_n]$, it holds that:

$$I_j K[[X]]_{\mathrm{alg}} = C_j(I)$$

for $j = 0, 1, \ldots,$ until $I_j \cap A_j = (0)$.

We start by setting C_0 to be the identity, $\mathbf{H}_0 := \mathbf{F}$, $B_0 := \emptyset$, $g_{i0} = g_i$ for $i = 1, \ldots, s$, so that $A_0 = K[X_1, \ldots, X_n, \mathbf{F}]_{\mathrm{loc}}$, $I_0 = I$ and $I_0 \cap A_0 \neq (0)$.

Assume we have constructed C_j, $\mathbf{H}_j$, A_j, B_j, $g_{1,j}, \ldots, g_{s,j}$.

By Lemma 6.4, we can test whether $I_j K[[X_1, \ldots, X_n]]_{\mathrm{alg}} \cap K[[X_1, \ldots, X_{n-j}]]_{\mathrm{alg}} = (0)$.

If such is the case, then we set $C := C_j$, $p := n - j$, $\mathbf{H} := \mathbf{H}_j$, $B := B_j$; a basis of $C(I)$ in A_j is given by $B_j \cup \{g_{1,j}, \ldots, g_{s,j}\}$.

Otherwise, we choose $h \in I_j A_j[X_{n-j+1}, \ldots, X_n] \cap A_j$, $h \neq 0$ (which is possible, since we have a basis of $I_j A_j[X_{n-j+1}, \ldots, X_n] \cap A_j$).

Then we perform a random linear change γ of the coordinates $X_1, \ldots, X_{n-j}$ and we check whether $\gamma(h)$ is distinguished (cf. Lemma 5.1(3)). Since for almost all γ, $\gamma(h)$ is distinguished, we therefore obtain a probabilistic algorithm to compute such a γ. We then set $C_{j+1} := \gamma C_j$.

By the Effective Weierstrass Preparation Theorem we obtain an LSS $\mathbf{H}_{j+1}$ defining series in $K[[X_1, \ldots, X_{n-j-1}]]_{\mathrm{alg}}$ such that $\mathrm{Wei}(\gamma(h)) \in K[X_1, \ldots, X_{n-j-1}, \mathbf{H}_{j+1}]_{\mathrm{loc}}[X_{n-j}]$ and the ring $A_{j+1} := K[X_1, \ldots, X_{n-j-1}, \mathbf{H}_{j+1}]_{\mathrm{loc}}$.

We set $b_{j+1,j+1} := \mathrm{Wei}(\gamma(h))$ (obtained by the Effective Weierstrass Preparation Theorem); for each i, we set $b_{i,j+1} := \mathrm{Can}(\gamma(b_{ij}), b_{j+1,j+1}, K[[X_1, \ldots, X_n]])$, which is obtained by substituting each coefficient in A_{j+1} of $\gamma(b_{i,j})$ by its canonical form. By Lemma 6.5, $B_{j+1} := (b_{1,j+1}, \ldots, b_{j+1,j+1})$ is a Weierstrass sequence in $A_{j+1}[X_{n-j}, \ldots, X_n]$.

Also, by the Effective Weierstrass Division Theorem we compute $\mathrm{Can}(\gamma(g_{i,j}), b_{j+1,j+1}, K[[X]])$.

It is clear that, denoting $I_{j+1} = (b_{1,j+1}, \ldots, b_{j+1,j+1}, g_{1,j+1}, \ldots, g_{s,j+1})A_{j+1}[X_{n-j}, \ldots, X_n]$, it holds that:

$$I_{j+1} K[[X]]_{\mathrm{alg}} = C_{j+1}(I)\,. \qquad \square$$

Corollary 6.7 (Elimination for algebraic series). *Let I be an ideal in $K[[X_1, \ldots, X_n]]_{\mathrm{alg}}$ generated as in the above theorem. Then, given $\delta < n$:*

(1) *it is possible to decide whether $\delta > \dim(I)$,*

(2) *if this is the case it is possible to compute:*

a linear change of coordinates C on $K[[X]]_{\mathrm{alg}}$,

an LSS $\mathbf{H}$ *defining series in* $K[[X_1, \ldots, X_\delta]]_{\mathrm{alg}}$,
an ideal $I^* \subset K[X_1, \ldots, X_\delta, \mathbf{H}]$ *such that*

$$I^* K[[X_1, \ldots, X_\delta]_{\mathrm{alg}} = C(I) K[[X]]_{\mathrm{alg}} \cap K[[X_1, \ldots, X_\delta]]_{\mathrm{alg}} .$$

Proof. We iteratively compute (as in Theorem 6.6) C_j, $\mathbf{H}_j$, A_j, B_j, $g_{1j}, \ldots, g_{sj}$, for $j \geq 0$, until either $I_j A_j[X_{n-j+1}, \ldots, X_n] \cap A_j = (0)$ or $j = n - \delta$.

In the first case we can conclude that $\delta \leq \dim(I)$.

In the second case, we set $C := C_j$, $\mathbf{H} := \mathbf{H}_j$.

$B_j \cup \{g_{1,j}, \ldots, g_{s,j}\}$ is a basis of I_j consisting of elements in $K[X_1, \ldots, X_\delta, \mathbf{H}]_{\mathrm{loc}}[X_{\delta+1}, \ldots, X_n]$.

Let $X' := (X_1, \ldots, X_\delta)$, $X'' := (X_{\delta+1}, \ldots, X_n)$.

By Lemma 6.3, we can then compute a basis in $K[X', \mathbf{H}]$ of

$$I^* := I_j \cap K[X', \mathbf{H}]_{\mathrm{loc}}.$$

We have:

$$\begin{aligned}
&C(I) K[[X]]_{\mathrm{alg}} \cap K[[X']]_{\mathrm{alg}} \\
&\quad = I_j K[[X]]_{\mathrm{alg}} \cap K[[X']]_{\mathrm{alg}} \\
&\quad = I_j K[[X']]_{\mathrm{alg}}[X'']_{\mathrm{loc}} \cap K[[X']]_{\mathrm{alg}} \\
&\quad = I_j K[[X']]_{\mathrm{alg}}[X''] \cap K[[X']]_{\mathrm{alg}} \\
&\quad = (I_j K[X', \mathbf{H}]_{\mathrm{loc}}[X''] \cap K[X', \mathbf{H}]_{\mathrm{loc}}) K[[X']]_{\mathrm{alg}} \\
&\quad = I^* K[[X']]_{\mathrm{alg}} ,
\end{aligned}$$

where:

the first equality holds since $I_j K[[X]]_{\mathrm{alg}} = C(I)$,

the second equality comes from faithfully flatness,

the third one holds by Lemma 6.1 applied to the ring $A = K[[X']]_{\mathrm{alg}}$,

the fourth one holds by Lemma 6.2 with $A = K[X', \mathbf{H}]_{\mathrm{loc}}$ and $B = K[[X']]_{\mathrm{alg}}$. □

Example 3 (continued). Starting with $I = (X_2^3 - g_1(X_1),\ X_1X_2 - X_3^3)$, we now compute $I^* \subset K[X_2, X_3, \mathbf{H}']$ such that $I^* K[[X_1, \ldots, X_n]]_{\mathrm{alg}} = IK[[X]]_{\mathrm{alg}} \cap K[[X_2, X_3]]_{\mathrm{alg}}$, where $\mathbf{H}' = (H_1', H_2', H_3', H_4')$ is an SLSS defining h_1, h_2, h_3, h_4.

We apply Lemma 6.3 to

$$\begin{aligned}
&(X_1^2 - X_1T_1 - T_0, H_1', H_2', H_3', H_4', X_1X_2 - X_3^3) \\
&\quad \subset K[X_2, X_3, T_0, T_1, V_0, V_1]_{\mathrm{loc}}[X_1]
\end{aligned}$$

obtaining a basis G such that

$$G \cap K[X_2, X_3, T_0, T_1, V_0, V_1]_{\mathrm{loc}} = (H_1', \ldots, H_4', F_0) ,$$

where

$$F_0 = X_2^5 - X_3^6 + T_1X_2X_3^3 - T_0V_0X_2^2 - T_1T_0V_1X_2^2$$

so $IK[[X]]_{\mathrm{alg}} \cap K[[X_2, X_3]]_{\mathrm{alg}}$ is generated by

$$X_2^5 - X_3^6 + h_4X_2X_3^3 - h_1h_2X_2^2 - h_2h_3h_4X_2^2 .$$

Appendix. Constructive Artin–Mazur Theorem

In this section we show how it is possible to reduce to our computational model in the case that the given algebraic function f is represented in a more classical way, i.e. if it is given by a polynomial $G(X_1, \ldots, X_n, T)$ such that $G(X_1, \ldots, X_n, f(X_1, \ldots, X_n)) = 0$. However, in this case, one must give also an algorithm to compute the Taylor expansion of f at least up to some order d, which is enough to distinguish f from the other eventual roots of G.

To do this, we will use a well-known result, due to Artin and Mazur (cf. [2, 4]), which permits us to give an LSS defining the required f. We propose here a constructive version of it, using the Traverso Normalization Algorithm (cf. [13]).

We note that in this case we require a stronger notion of computable field, i.e. we require the availability of factorization algorithms for polynomials with coefficients in K.

Theorem (Constructive Artin–Mazur Theorem). *Let $f \in K[[X]]_{\mathrm{alg}}$, $G \in K[X, T]$ such that $G(X, f(X)) = 0$ and assume that an algorithm to compute the Taylor expansion of f up to order d, $\forall d$, is given. Then it is possible to compute a locally smooth system $(F_1, \ldots, F_r)$ defining algebraic series $f_1, \ldots, f_r$, with $f_1 = f$.*

Proof. We follow the proof given in [4] to which we refer for further details.

We can without loss of generality assume that G is irreducible. Otherwise we factorize and, since we know arbitrary Taylor expansions of f, we can check at which irreducible factor of G, the series f vanishes. (To do this, by the Bezout theorem, it is enough to verify which of the factors F_i's is such that $F_i(f(X))$ has order greater than the square of the degree of F (see Remark 2.6(4)).)

Let $R := K[X, T_1]/(G)$ and let $R' := K[X, T_1, T_2, \ldots, T_r]/(G_1, G_2, \ldots, G_s)$ be its normalization; then, by the universal property of the integral closure, the evaluation map $\sigma : R \to K[[X]]$ given by $\sigma(T_1) = f$, can be extended to $\sigma' : R' \to K[[X]]$. Let $f_2 = \sigma'(T_2), \ldots, f_r = \sigma'(T_r)$; by substituting T_i with $T_i - f_i(0)$, we can assume $f_i(0) = 0$ $\forall i$. Then by the Zariski Main Theorem, the localization of R' at the origin, R'_{loc}, is analytically irreducible and therefore an étale extension of $K[X]_{\mathrm{loc}}$, so that it is nonsingular and the Jacobian of the G_i's at the origin with respect to $T_1, T_2, \ldots, T_r$ has rank r. Therefore, there are

$F_1, \ldots, F_r$, linear combinations of the $G_1, \ldots, G_s$ such that $(F_1, \ldots, F_r)$ is a locally smooth system (cf. Lemma 2.1); since $F_j \in (G_1, \ldots, G_s)$ and $G_i(X, f_1, \ldots, f_r) = 0$, $F_j(X, f_1, \ldots, f_r) = 0$ too.

This gives the existence of a locally smooth system satisfying the requirements of the theorem. In order to obtain a constructive procedure to give the F_i's, all we need is to show how to compute $G_1, \ldots, G_s$ and $f_i(0)$ $\forall i$.

Now we recall that the Normalization Algorithm proposed by Traverso (cf. [13]) allows to compute:

(1) G_1, $G_2, \ldots, G_s \in P[T_1, T_2, \ldots, T_s]$ such that $R' = K[X, T]/(G_1, G_2, \ldots, G_s)$,

(2) polynomials $D \in K[X]$, $H_i \in K[X, T_1, \ldots, T_{i-1}]$ $\forall i$, such that

$$f_i(X) = \frac{H_i(X, f_1(X), \ldots, f_{i-1}(X))}{D(X)} \neq 0 .$$

Then, since we are able to compute the Taylor expansion of f_1 u to any order d, we can do the same for each f_i; in particular, we are able to compute $f_i(0)$. □

We remark that, while the normalization algorithms seem to be not very feasible, we do not need to have a complete normalization of R, but just an extension $R'' = K[X, T]/(G_1, G_2, \ldots, G_s)$ such that (assuming $f_i(0) = 0$) the Jacobian of the G_i's at the origin with respect to $T_1, T_2, \ldots, T_r$ has rank r.

Example. We remark that in Example 3 which we followed throughout the paper, the algebraic series f could be obtained by means of the normalization of the ring

$$R = \frac{K[X_1, T_1]}{(T_1^2 - X_1^4 - X_1^5 T_1)} ,$$

obtaining

$$R' = \frac{K[X_1, T_1, T_2]}{(T_1 - X_1^2 - X_1^2 T_2, 2T_2 + T_2^2 - X_1^3 - X_1^3 T_2)} \cong \frac{K[X_1, Y_1]}{(2Y_1 + Y_1^2 - X_1^3 - X_1^3 Y_1)} .$$

This is of course what we did by hand, and, also, in this case the normalization algorithm goes very well since the ring R has dimension one.

Acknowledgment

The authors thank Professor I. Luengo for several useful discussions on the geometrical aspects of the problem.

The paper was done while M.E. Alonso was guest of the Mathematics Department of Genova; she likes to thank the people who made this stay possible and pleasant.

The computations needed to derive Example 3 were done in the system CoCoA by A. Giovini and G. Niesi.

References

[1] M.E. Alonso, I. Luengo and M. Raimondo, An algorithm on quasi-ordinary polynomials, in: Proceedings AAECC 6, Lecture Notes in Computer Science (Springer, Berlin, 1989) 59–73.

[2] M. Artin and B. Mazur, On periodic points, Ann. of Math. 81 (1965) 82–99.

[3] E. Bierstone and P. Milman, The Local Geometry of Analytic Mappings (Pisa, 1988).

[4] J. Bochnak, M. Coste and M.F. Roy, Géométrie algébrique réelle, Ergebnisse Math. Grenzgeb. 12 (1987).

[5] B. Buchberger, A criterion for detecting unnecessary reductions in the construction of Gröbner bases, in: Proceedings EUROSAM 79, Lecture Notes in Computer Science 72 (Springer, Berlin, 1979) 3–21.

[6] B. Buchberger, Gröbner bases: an algorithmic method in polynomial ideal theory, in: N.K. Bose, ed., Recent Trends in Multidimensional System Theory (Reidel, Dordrecht, 1985).

[7] A. Galligo, A propos du theoreme de preparation de Weierstrass, Lecture Notes in Mathematics 409 (Springer, Berlin, 1974) 543–579.

[8] H. Hironaka, Idealistic exponents of singularity, Algebraic Geometry, The Johns Hopkins Centennial Lectures (1977) 52–125.

[9] F. Mora, An algorithm to compute the equations of tangent cones, in: Proceedings EUROCAM 82, Lecture Notes in Computer Science 144 (Springer, Berlin, 1982) 158–165.

[10] T. Mora, G. Pfister and C. Traverso, An introduction to the Tangent Cone Algorithm, in: C. Hoffman, ed., Issues in Nonlinear Geometry and Robotics (JAI Press, Greenwich, CT), to appear.

[11] M. Nagata, Local Rings (Interscience, New York, 1962).

[12] M. Raynaud, Anneaux Locaux Henséliens, Lecture Notes in Mathematics 169 (Springer, Berlin, 1970).

[13] C. Traverso, A study on algebraic algorithms: the normalization, Rend. Sem. Mat. Univ. Politec. Torino (1986) 111–130.